INTERNET ASSOCIATION OF AUSTRALIA
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

7 November 2022

To: Committee Secretary
Senate Legal and Constitutional Affairs Committee

PO Box 6100
Parliament House
Canberra ACT 2600

By submission:
https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/PrivacyEnforcement2022

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

Thank you for the opportunity to express the Internet Association of Australia's (**IAA**) perspective on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (**Bill**). IAA is a member-based association representing the Australian Internet community. Our membership is largely comprised of small to medium Internet Service Providers (**ISPs**). This response is written primarily in representation of our members' perspective, as well as in support of the general well-being of the Internet and telecommunications industry.

In light of the recent data breach incidents that have occurred in Australia, including those involving large corporations such as Optus, Medibank, and MyDeal, IAA recognises and appreciates the efforts to uplift Australia's data protection laws by the Bill. In particular, in today's data-driven Internet economy, IAA and our members are sincerely committed to the role we should play in the protection of Australians' data. As such, we agree in sentiment with the proposed Bill which purports to enhance enforcement measures and increase information sharing between relevant bodies to foster a culture where corporations take their data security obligations seriously, and allow the Australian Information Commissioner to function effectively.

However, we are concerned about the efficacy of some key aspects of the Bill. In particular, we believe that the government's focus and effort should be targeted more at prevention and mitigation of the potential for serious harm to individuals in the unfortunate occasion of a data breach. The Optus data breach in particular, brought to light data retention laws desperately in need of review to ensure companies are not holding data where it is not necessary to do so.

With the ever increasing scourge of sophisticated scams and cybersecurity attacks, it is widely accepted that data breaches may be inevitable, regardless of the security measures in place by an organisation. As such, while we understand that more a comprehensive response to privacy and data breach issues will be effected via the ongoing Privacy Act review and that this Bill does not intend to be the full extent of privacy reforms to better protect Australia's data security, we still believe that the immediate government focus should be to mitigate the negative impacts to Australians by ensuring only necessary personal information is being held in the first place, and encouraging compliance by

balancing the incentives for improved security and privacy practice with the penalties available. It is our view that the emphasis should be on better adherence to the privacy principles, better redress and response mechanisms, and shifting the culture away from unnecessary data collection and retention to a more privacy respectful one.

Ultimately, in a time where an immediate government response is required to the recent wave of data breaches affecting millions of Australians, there should be a clear consideration of what is the genuine purpose of legislative reforms, and what outcomes will such reforms actually serve?

INCREASED PENALTIES

The increased penalties proposed by the Bill suggest that organisations are wilfully negligent and/or ignore good security and privacy practice, implying that the cost of current penalties for non-compliance are simply the lesser and easier payment. While we acknowledge that serious fines and penalties can serve as a strong and effective incentive, and that there may well be entities who are so wilfully non-compliant, we don't believe this to be the majority case. Even without increased fines, the reputational harm and consequences of suffering and poor management of a data breach is a genuine deterrence for companies to ensure the protection of their data. It is our view that the fines proposed are excessive, despite an increase to the current regimen being warranted. It is our view also that such penalties be directed towards consumer redress and industry training through the work of the OAIC rather than simply general revenue to government.

Moreover, we are concerned that the penalties will affect smaller businesses – including our members – disproportionately. In its proposed current form, the increased penalties are likely to have a disproportionately punitive effect on smaller entities who are often struggling with compliance due to the complexity of privacy laws and regulation, rather than being wilfully negligent.

We strongly recommend a tiered approach to the penalties that takes into consideration a number of factors including, but not limited to:

- The size of the entity;
- The type of personal information held by the entity;
- The nature and type of business the entity operates; and
- Whether the entity had security measures in place.

Again, rather than taking a punitive approach, we believe greater education and guidance is necessary to ensure compliance, especially when it comes to smaller entities, who are already at risk of data breaches due to their inability to afford complex cyber security protections. While enforcement measures deal with the aftermath, we propose that addressing preventative and mitigation of serious harm measures is a more pressing concern to protect Australians.

AUSTRALIAN INFORMATION COMMISSIONER POWERS

In general, IAA supports providing the Commissioner with increased powers to carry out its function and investigate data breaches to ensure entities are complying with privacy laws. However, we believe that effective and best practice laws are measured and practicable and thus should balance the burdens placed on industry. As such, we recommend limitations to be placed on the proposed s 26WU(4) in terms of the minimum period given to entities to answer questions or produce documents in response to a notice given by the Commissioner. We propose that entities be given no less than 10 business days to respond, and that the place or manner of response not be unreasonable.

OTHER CONSIDERATIONS

IAA is concerned that the OAIC does not receive adequate funding to effectively carry out its functions. In order for these legislative amendments to be effective, the OAIC must be properly resourced. In addition, more so than enforcement, IAA reiterates the need for greater education and guidance provided particularly to smaller businesses to ensure privacy compliance. Thus, the OAIC must receive sufficient funding to engage in genuinely effective outreach and awareness building campaigns and education.

In the spirit of making compliance easier for companies, we believe that greater legislative clarity should be provided. In particular, "serious harm" with respect to the Notifiable Data Breach Scheme (**NDB Scheme**) should be properly defined or at least clarified. As notification of eligible data breach to affected individuals and the Commissioner can play a major role in mitigating the potential harm of a data breach, as well as the penalties involved for not complying with the NDB Scheme, it is necessary to make things as clear as possible.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. We reiterate our commitment to uplifting Australians' data security and protection and recognise effective legislation as an important way through which this can be achieved. As such, we believe that legislative reforms must be thoroughly reviewed and considered in terms of its purpose, and likely outcomes and consequences. As Australia continues to navigate through ever increasing threats to our data security, we sincerely look forward to working with government, industry and other stakeholders to ensure a fit for purpose privacy and data security framework.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.
IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia