Tech Council of Australia
www.techcouncil.com.au

07 November 2022

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

Thank you for the opportunity to respond to the Inquiry into the **Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022.** The Tech Council of Australia takes cybersecurity and privacy extremely seriously. We are grateful for the opportunity to provide a submission on the Bill.

About the Tech Council of Australia (TCA)

The TCA is Australia's peak industry body for the tech sector. The Australian tech sector is a key pillar of the Australian economy, contributing $167 billion to GDP per annum, and employing over 860,000 people. This makes the tech sector equivalent to Australia's third largest industry, behind mining and banking, and Australia's seventh largest employing sector.

The TCA represents over 160 member companies from a diverse cross-section of Australia's technology sector, including leading Australian software as a service and platform companies, fintech companies, venture capital and investment advisory firms, and multinational tech companies with a significant Australian presence. In light of the current cyber and data security crisis facing Australia, the TCA has brought together a "tiger team" of multi-disciplinary experts from across the tech sector to support the Government's response and provide advice on proposed reform initiatives.

The imperative to improve cyber and data security in Australia

Recent high-profile cyber attacks and data breaches have demonstrated the need for governments and industry to work together to meaningfully improve cyber security and privacy across Australia.

The Tech Council supports a comprehensive response to these incidents, including a modernised regulatory and legislative framework that aims to achieve the following outcomes in our shared interests:

- Making Australia more cyber resilient and rebuilding community confidence in our ability to deter, detect, withstand and manage cyber attacks and incidents.
- Incentivising effective disclosure, coordination and communication following a cyber attack or breach to make sure incidents are managed professionally and effectively, and impacted citizens and businesses can access the help they need as swiftly and seamlessly as possible.
- Ensuring regulatory consistency across Australian legislation and interoperability with international legislation, to lift the standard of Australia's privacy and data laws and improve industry compliance.

- Enabling the growth of Australia's digital economy, which will underpin our future prosperity and security (including our cyber security), and ensuring Australian citizens and businesses are capable and confident of engaging digitally.

Key issues, questions, and recommendations for the Inquiry

The Tech Council welcomes the decision to refer the *Privacy legislation Amendment (Enforcement and Other Measures) Bill 2022* for inquiry.

We are not opposed to increased penalties or changes to the Information Commissioner's powers. However, we recommend that the Bill is amended to ensure that the legislation achieves the cyber security and privacy outcomes it is aimed at addressing

There are also broader actions that are needed beyond the direct scope of the legislation that we recommend are considered by the Committee. Our full suite of recommendations are summarised in Attachment A.

1. **Scope of the legislation**: Penalty increases alone do not address the many drivers of cyber vulnerability and data breaches in Australia, such as skill shortages, regulatory gaps, and lack of investment in more secure technology and practices. A more comprehensive response is urgently needed to address the current cyber crisis, which should be underpinned by close collaboration between the Government and industry.

    1.1. The TCA supports the Government's decision to develop a new cyber security strategy and we are closely engaged in the broader review of the Privacy Act. Both of these initiatives will be critical to our national cyber response and we look forward to continuing to work closely with the Government on them.

    1.2. We believe that cyber security skills and talent is an area in need of far greater attention. Australia does not have enough cyber security professionals. In 2021, the vacancy rate for cyber security roles was over double the economy-wide vacancy rate, according to TCA research. The skills shortages are concentrated in roles with 3+ years' experience, and which require University degrees. That means they cannot be solved in the short-term by labour market adjustments or training. If businesses cannot hire experienced cyber security and tech talent, their capacity to prevent and manage incidents is far lower.

    1.3. One of the key solutions to the skills shortage is prioritising these skills via Australia's skilled migration program. Experienced and high-paid skilled migrants can help fill shortages, while also supervising and upskilling local staff. However, currently, Australia is one of the slowest governments in the world at processing visas for skilled cyber and tech workers, taking up to an average of 90 days[1] to process them, compared to 10 days in Canada[2], 15 in the UK,[3] and 20 in New Zealand[4]. Australia could very simply address these delays by directing the Department of Home Affairs to prioritise these roles for visa processing, and by setting a deadline for processing times, as it has recently done for Health and Education occupations, which are now being processed in 2 days. Other markets such as New Zealand, Canada, the UK, Singapore, France and Israel have prioritised

[1] Median processing time (3 months) for TSS (subclass 482), short-term stream. Source: Australian Department of Home Affairs.
[2] Service standard committed to by the Canadian Government. Source: Canadian Government
[3] Typical processing time for Global Talent visa for digital technology leaders. Source: UK Government
[4] Median processing time for Accredited Employer Work Visas (AEWV), Source: New Zealand Government

tech and cyber skills in their migration systems and set deadlines. Australia's failure to do this means an Australian business must wait more than 4 times as long to fill a vacant role as a comparable business in New Zealand. Increasing penalties does not change a business' capacity to hire workers, if the issue is that there is a skills shortage and a delay in skilled migrants entering Australia.

1.4. Technological solutions can also play a key role in the national response. One immediate action that could be taken is to legislate to support the expansion of the trusted digital identity model across the broader economy (noting it is currently restricted to Australian Government applications). This would enable consumers to establish a digital identity once and use it repeatedly to prove their identity for a range of online services, saving businesses and consumers time and money, while avoiding the need for organisations to collect and store sensitive personal information. Greater use of digital credentials, 2FA technology and encryption can also help.

Recommendation 1: We recommend the Committee notes the importance of developing a more substantive and comprehensive set of measures to improve Australia's cyber security environment and reduce the number and severity of data breaches, including:

a) an updated national cybersecurity strategy, supported by an improved system for disclosing, coordinating and communicating data and cyber breaches;
b) modernising the broader regulatory framework (including the Privacy Act);
c) addressing urgent skills shortages in tech and cyber workers (including by ensuring these skills are prioritised for processing in 10 days in skilled migration system) and improving cyber capability and awareness in the broader community; and,
d) deploying new technology solutions (including the expansion of the trusted digital identity model across the broader economy).

2. **Tiered Penalty Regime**: We note that the increased maximum penalties will apply to serious or repeated offences under the Act, covering a range of organisations, including in some cases small businesses. We also note that the proposed penalties, if adopted by the Parliament, will be amongst the most significant penalties for privacy breaches globally. While we are not opposed to increased penalties, our firm view is that penalties should be proportionately applied. While courts will be the ultimate arbiter of this, the legislation could be amended to provide for lower maximum penalties for less severe infringements.

2.1. For example, the GDPR adopts a tiered approach to maximum penalties, with a smaller maximum penalty for less severe infringements, and larger maximum penalties reserved only for the most severe infringements.

2.2. Introducing a tiered model would also provide more legal clarity for smaller businesses about their potential risk levels and exposure to the increased penalties.

Recommendation 2: Amend the Bill to introduce a two-tiered model for maximum penalties, proportionate to the seriousness of breaches. Under this model, the current proposed maximum penalties would be used for the most severe infringements under the Privacy Act, while a new tier of smaller maximum penalties (also adjusted to Australian domestic turnover) would apply to less severe infringements.

3. **OAIC guidance**: There is uncertainty regarding the application of privacy and cyber related laws and associated penalties, particularly when it comes to the actions expected of businesses to prevent or respond to data breaches, and the potential overlap between penalties under different pieces of legislation (e.g. between the Privacy Act and the Security of Critical Infrastructure Act). This uncertainty will be exacerbated by the increased penalties. Clear guidance is important to avoid creating unnecessary anxiety for businesses, including smaller businesses, about the penalties they may be liable for, and to avoid creating a disincentive for businesses to disclose data breaches.

   3.1. An example of guidance for assessing penalties for data breaches is provided in the EU GDPR scheme which outlines 11 criteria such as the gravity and nature of the breach, steps for mitigation, precautionary measures, history of previous infringements, cooperation with supervisory and regulatory bodies, type of data, and adherence to codes of cyber conduct.

> **Recommendation 3:** The OAIC (working in consultation with relevant stakeholders) should issue revised guidance on how penalties will be applied for by the OAIC to the courts, what behaviour will trigger them, and provide clarity on the factors that determine the assessment of the severity of breaches.
>
> **Recommendation 4**: The OAIC should play a greater role in assisting and guiding businesses to understand their privacy and cyber compliance obligations, and how to address and handle a data breach resulting from a cyber attack. This could, for example, take the form of a decision tree for organisations experiencing a potential or actual breach (acting as a nationally agreed tool to aid organisations dealing with these incidents).

4. **Information Commissioner powers**: The TCA supports expedited, secure information sharing following an incident where it ensures citizens can get the help they need to minimise harm to them from a breach (e.g. where ID documents must be reissued, or fraud prevention triggered). However, care needs to be taken in the design of the Information Commissioner's increased information gathering, sharing and public statement powers where it interacts with ongoing investigations or other legal action, such as class actions.

   4.1. For example, the capacity of the Commissioner to make public statements before an investigation has concluded, or to share information with law enforcement that effectively bypasses proper judicial process, could be prejudicial to these investigations or cases.

   4.2. This could also force companies to be more circumspect in the information they share with the Commissioner, and go through a more thorough legal review of any information disclosed, which would potentially lead to less information being disclosed in a timely manner.

   4.3. This is the opposite outcome sought by the new rules. This is particularly important in situations where the breach is a result of a malicious act (e.g. by cyber criminals, or an act of cyber espionage) and it may take time for a company and government agencies to investigate the situation and establish the facts.

   4.4. Companies may rightly be cautious in disclosing incorrect or unsubstantiated information to regulators. The design of disclosure, information sharing, and publishing powers need to bear this dynamic in mind.

Recommendation 5: Clarify in the Explanatory Memorandum that the Information Commissioner's information sharing powers are for the purposes of an emergency response to a data breach (not for prosecutions by law enforcement), and that the Commissioner should obtain the consent of an organisation subject to a data breach before sharing information with law enforcement agencies.

Recommendation 6: Amend the Bill or Explanatory Memorandum to require the Information Commissioner to seek the agreement of the Australian Signals Directorate, Australian Cyber Security Centre and Department of Home Affairs, and consult with the organisation subject to the data breach, as part of determining whether releasing information on a cyber attack or data breach is in the "public interest." Early release of this information may hinder law enforcement's ability to track and monitor state sponsored and criminal infrastructure which would contribute to larger law enforcement operations, arrests and takedowns.

Recommendation 7: The Government should increase resourcing for the OAIC commensurate to the increased powers and the increased risk of data breaches across the economy.

5. **Clarity over "reasonable steps" to improve certainty and incentivise disclosure**: At present, it is not clear in the Act on what grounds a company could be found liable for a data breach, particularly where they are the victim of a cyber attack. Clarity is not just important for industry certainty, it can also help incentivise good cyber and privacy practices, and encourage disclosure of data breaches which is a positive behaviour that helps keep the community safe by ensuring there is an effective response to incidents as they are unfolding, and by learning from them once they are concluded.

   5.1. With the proposed penalty increases comes the need for increased certainty over what constitutes "reasonable steps" to protect personal information under the Privacy Act, particularly with regards to a data breach.

   5.2. Unauthorised breaches of personal information as a result of criminal activity do not necessarily give rise to a breach of privacy law, where a company has taken all reasonable steps (e.g. a company could theoretically collect and store data in line with its Privacy Act obligations and comply with relevant data security standards, but still be subject to a data breach as a result of a sophisticated cyber attack).

   5.3. A safe harbour model could provide more balance to the legislation by retaining the large "stick" of increased penalties, while also providing organisations with a "carrot" to avoid the worst of these penalties if they meet certain conditions. For example, making an early disclosure, cooperating with relevant regulatory and law enforcement bodies, and complying with relevant security standards.

Recommendation 8: Amend the Bill to include a safe harbour regime for data breaches for organisations that make an early disclosure, can demonstrate that they are compliant with relevant standards, working in cooperation with relevant bodies, and that the breach was not a result of reckless or negligent behaviour. This would assist organisations with understanding what constitutes taking "reasonable steps" and would help encourage disclosure of data breaches and security incidents.

a) The details of the safe harbour could alternatively be determined via legislative instrument, rather than in the primary legislation. This would allow more time to get the details right and flexibility to make future changes.

6. **Overlapping regulatory, disclosure and reporting arrangements**: There are overlapping and duplicative disclosure and reporting requirements for data breaches across the federal government, as well as different levels of government, which hampers coordination efforts between government and industry, slows down the disclosure process, and creates unnecessary administrative burdens for companies that have been breached. Several agencies have similar, though not identical information requirements and therefore separate reporting processes must be undertaken for each entity.

6.1. Further work is needed to identify how disclosure and reporting requirements can be streamlined as well as to ensure that coordination, communication and support for consumers affected by a breach is able to be activated as quickly, consistently and seamlessly as possible.

6.2. Further consideration is also needed regarding the overlapping investigation and enforcement powers across different regulators with regards to privacy-related incidents (e.g. ACCC, ACMA, OAIC). This creates uncertainty for businesses who are unsure of what laws they must first comply with when suffering a privacy incident. It increases the cost for both Government and businesses when addressing a privacy incident as numerous government agencies may investigate and take action against a business in relation to a single privacy incident. It also creates confusion for consumers who don't know which agency to go to when raising a privacy complaint or concern.

Recommendation 9: The Government should commission a wide-ranging review of reporting and disclosure requirements for data breaches to streamline coordination and communication models across different regulators, and improve timeliness and quality of disclosure and investigation following a breach. The review could also consider the consistency of reporting and disclosure requirements with international schemes that many businesses are already complying with, such as the EU GDPR and the UK Data Protection Act.

Recommendation 10: The Government should commission a review of overlapping investigation and enforcement powers across different regulators with regards to privacy-related incidents.

7. **Extraterritoriality**: The proposed extraterritorial application of the Privacy Act would benefit from further clarification to avoid unintended consequences. In particular, the outright removal of subsection 5B(3)(c) relating to personal information collected or held in Australia could mean that foreign companies carrying on business in Australia would be subject to the Privacy Act even in respect of activities that do not relate to their business in Australia or to Australian individuals.

Recommendation 11: That the Bill be amended so that subsection 5B(3)(c) of the Act instead clarifies that the personal information collected or held must relate to an individual located in Australia (or similar).

8. **Review of Data Regulation**: Federal and state government laws often require private sector and non-profit organisations to collect and retain personal and sensitive data about Australians. Many of these laws have been in place for decades, without review, raising questions about whether businesses are unnecessarily collecting sensitive personal information due to outdated legal requirements.

   8.1. The TCA is also of the view that a more robust and independent process should be put in place to assess new laws that seek to expand requirements for sensitive and personal data collection. This would ensure that regulatory design balances privacy, data governance and cybersecurity considerations with the other policy outcomes sought by the proposed laws.

> **Recommendation 12**: The Government should commission a review of laws requiring data collection and retention to determine whether their provisions are reasonable (e.g. must all data be collected and retained, and for the specified period), and if there are now alternatives to data collection and retention requirements, such as the use of digital identity or digital credentials.
>
> **Recommendation 13:** As part of the Privacy Act Review, the Government should consider establishing an enhanced, proactive review process for new legislation proposing to mandate or undertake data collection and retention of personal and sensitive information by government agencies or the private sector, including how the design of the program will take into account privacy and security considerations, and the governance and assurance program for the design and implementation of the scheme. The Sharing Economy Reporting Regime (Treasury Laws Amendment (2022 Measures No. 2) Bill) is a good case study in new legislation requiring additional data collection and retention, without an associated governance and assurance program.

We appreciate the opportunity to contribute feedback to these proposed amendments to legislation and look forward to an ongoing dialogue.

Yours sincerely,

Kate Pounder
CEO, Tech Council of Australia

e:
m:

Attachment A – Summary of Tech Council Recommendations

Recommendations to Amend the Bill	
Recommendation 2:	Amend the Bill to introduce a two-tiered model for maximum penalties, proportionate to the seriousness of breaches. Under this model, the current proposed maximum penalties would be used for the most severe infringements under the Privacy Act, while a new tier of smaller maximum penalties (also adjusted to Australian domestic turnover) would apply to less severe infringements.
Recommendation 5:	Clarify in the Explanatory Memorandum that the Information Commissioner's information sharing powers are for the purposes of an emergency response to a data breach (not for prosecutions by law enforcement), and that the Commissioner should obtain the consent of an organisation subject to a data breach before sharing information with law enforcement agencies.
Recommendation 6:	Amend the Bill or Explanatory Memorandum to require the Information Commissioner to seek the agreement of the Australian Signals Directorate, Australian Cyber Security Centre and Department of Home Affairs, and consult with the organisation subject to the data breach, as part of determining whether releasing information on a cyber attack or data breach is in the "public interest." Early release of this information may hinder law enforcement's ability to track and monitor state sponsored and criminal infrastructure which would contribute to larger law enforcement operations, arrests and takedowns.
Recommendation 8:	Amend the Bill to include a safe harbour regime for data breaches for organisations that make an early disclosure, can demonstrate that they are compliant with relevant standards, working in cooperation with relevant bodies, and that the breach was not a result of reckless or negligent behaviour. This would assist organisations with understanding what constitutes taking "reasonable steps" and would help encourage disclosure of data breaches and security incidents. a) The details of the safe harbour could alternatively be determined via legislative instrument, rather than in the primary legislation. This would allow more time to get the details right and flexibility to make future changes.
Recommendation 11:	That the Bill be amended so that subsection 5B(3)(c) of the Act instead clarifies that the personal information collected or held must relate to an individual located in Australia (or similar).
Recommendations for other actions necessary to achieve policy objectives	
Recommendation 1:	We recommend the Committee notes the importance of developing a more substantive and comprehensive set of

	measures to improve Australia's cyber security environment and reduce the number and severity of data breaches, including: a) an updated national cybersecurity strategy, supported by an improved system for disclosing, coordinating and communicating data and cyber breaches; b) modernising the broader regulatory framework (including the Privacy Act); c) addressing urgent skills shortages in tech and cyber workers (including by ensuring these skills are prioritised for processing in 10 days in skilled migration system) and improving cyber capability and awareness in the broader community; and, d) deploying new technology solutions (including the expansion of the trusted digital identity model across the broader economy).
Recommendation 3:	The OAIC (working in consultation with relevant stakeholders) should issue revised guidance on how penalties will be applied for by the OAIC to the courts, what behaviour will trigger them, and provide clarity on the factors that determine the assessment of the severity of breaches.
Recommendation 4:	The OAIC should play a greater role in assisting and guiding businesses to understand their privacy and cyber compliance obligations, and how to address and handle a data breach resulting from a cyber attack. This could, for example, take the form of a decision tree for organisations experiencing a potential or actual breach (acting as a nationally agreed tool to aid organisations dealing with these incidents).
Recommendation 7:	The Government should increase resourcing for the OAIC commensurate to the increased powers and the increased risk of data breaches across the economy.
Recommendation 9:	The Government should commission a wide-ranging review of reporting and disclosure requirements for data breaches to streamline coordination and communication models across different regulators, and improve timeliness and quality of disclosure and investigation following a breach. The review could also consider the consistency of reporting and disclosure requirements with international schemes that many businesses are already complying with, such as the EU GDPR and the UK Data Protection Act.
Recommendation 10:	The Government should commission a review of overlapping investigation and enforcement powers across different regulators with regards to privacy-related incidents.
Recommendation 12:	The Government should commission a review of laws requiring data collection and retention to determine whether their provisions are reasonable (e.g. must all data be collected and retained, and for the specified period), and if there are now

	alternatives to data collection and retention requirements, such as the use of digital identity or digital credentials.
Recommendation 13:	As part of the Privacy Act Review, the Government should consider establishing an enhanced, proactive review process for new legislation proposing to mandate or undertake data collection and retention of personal and sensitive information by government agencies or the private sector, including how the design of the program will take into account privacy and security considerations, and the governance and assurance program for the design and implementation of the scheme. The Sharing Economy Reporting Regime (Treasury Laws Amendment (2022 Measures No. 2) Bill) is a good case study in new legislation requiring additional data collection and retention, without an associated governance and assurance program.