Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
By email and webform: legcon.sen@aph.gov.au

Monday November 7, 2022

Dear Committee Chair,

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the draft *The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (the Bill).

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, eBay, Google, Linktree, Meta, TikTok, Twitter, Snap and Yahoo, and its associate members are Change.org, Gofundme, ProductReview.com.au and Redbubble. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI and its members share and support the Government's strong commitment to privacy. We are supportive of the Bill's strengthened penalties for serious breaches, and its facilitation of greater regulatory cooperation.

In this submission, we seek more clarity on the extraterritorial scope of the Bill and the definition of 'serious' and 'repeated' interference with privacy, and we encourage an economy-wide approach to regulatory cooperation. DIGI fully supports modernising the Privacy Act for a digital era, and has engaged with the Privacy Act Review (the Review); this submission offers brief high level considerations in relation to the Review that we consider relevant to our understanding of the Bill's intent.

We thank you for your consideration of the matters raised in this submission. Should you have any questions, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director, DIGI
sunita@digi.org.au

DIGI

Table of contents

1. Scope of extraterritoriality

1.1. We are generally supportive of changes to clarify the extra-territorial operation of the Privacy Act. We understand that the Bill requires entities to meet the obligations of the Privacy Act if they 'carry on business' in Australia. Under the current Privacy Act, entities are also required to demonstrate that they collect or hold Australians' information directly from a source in Australia; however we understand that the Bill proposes to remove this requirement, and we believe the implications of this amendment must be closely examined.

1.2. DIGI is of the view that data localisation does not increase data security, and we recognise that data will not always be held in Australia; therefore, we accept that the *holding* of data within Australia should not constitute the basis for an Australian link.

1.3. However, we are concerned that the removal of the requirement in paragraph 5B(3)(c) 'that an organisation or operator that is not described in subsection 5B(2) must collect or hold personal information in Australia or an external Territory either before or at the time of the act or practice in order to have an Australian link' serves to also remove the requirement that data be *collected* in Australia.

1.4. The effect of the removal of this paragraph is that if an offshore corporation carries on business in Australia through providing services to Australian end users, then the Australian Privacy Act would also apply to that corporation's handling of information about users in any other jurisdiction where its services are available. DIGI would like to understand if the intention in removing this paragraph is that offshore businesses carrying on business in Australia must handle all the personal information they collect from *everywhere* (not from Australia or relating to Australians) in accordance with the Australian Privacy Act.

1.5. With paragraph 5B(3)(c) removed, what is retained is the requirement that entities 'carry on business' in Australia; however, as the OAIC notes in its explanation of key concepts, 'The phrase 'carries on business in Australia' in s 5B(3)(c) is not defined in the Privacy Act'[1].

1.6. The Explanatory Memorandum provides the following justification for the removal of this paragraph: 'when a breach of the Privacy Act occurs, it may be difficult to establish that these foreign organisations collect or hold personal information from a source in

[1]OAIC, *Chapter B: Key concepts*, accessed at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts

Australia'. DIGI considers that if the impact on Australians cannot be established, then this raises the question of whether the action falls within the jurisdiction of the Australian Information Commissioner. It is not clear why Australian laws seek to regulate the management of personal information that has no direct connection with Australia or with Australians. Ensuring a stronger connection with Australia is especially important when the well-established resource limitations of the Office of the Australian Information Commissioner (OAIC) are taken into consideration.

1.7. DIGI is concerned that these extraterritoriality provisions of the Bill exceed the provisions in the European Union's General Data Protection Regulation (GDPR). When introduced in 2018, the GDPR expanded the extraterritoriality of the EU's regulation such that it applies to (1) individuals that are EU residents, (2) organisations that are based in the EU, or (3) organisations based outside the EU that monitor the behaviour of EU citizens[2]. This still enables compliance from foreign entities, while still requiring a connection to the EU. This is important as it provides foreign companies with a degree of clarity as to which organisation is the responsible international regulator.

1.8. An additional challenge with open-ended extraterritoriality provisions is that they create uncertainty for international companies in situations where a conflict of laws between applicable privacy regulation may be present. In general, DIGI is of the view that refinement of the scope and application of the Privacy Act will provide a clarity of expectations of corporations that will ultimately assist compliance.

2. Definition of 'serious' and 'repeated' interference with privacy

2.1. DIGI understands that the Bill will increase maximum penalties that can be applied under the Privacy Act 1988 for *serious or repeated* privacy breaches from the current $2.22 million penalty to whichever is the greater of $50 million, three times the value of any benefit obtained through the misuse of information; or 30 percent of a company's adjusted turnover in the relevant period. DIGI has no objections to the increasing of penalties. Penalties play an important deterrence role in a modernised privacy regime, and need to form part of other pro-privacy consumer and organisational practices in the reform of the Act.

2.2. However, if the penalties are being raised so substantially, their scope and application need to be exceedingly clear, and greater clarity will ultimately assist APP entities' compliance efforts. We are concerned that the Act does not define a 'serious' or 'repeated' interference with privacy, creating uncertainty as to the circumstances in which this civil penalty provision may apply. To provide APP entities with greater clarity as to the potential application of the amended penalty provision, we submit that the Bill be amended to include a definition of both a 'serious' and 'repeated' interference with privacy that covers only the most egregious breaches of the Act (e.g. breaches involving deliberate or reckless conduct on the part of an APP entity).

2.3. We note that the most recent Privacy Act Review Discussion Paper, released in October 2021 (the Discussion Paper), proposes to 'clarify what constitutes a repeat or serious

[2]OAIC, *Australian entities and the EU General Data Protection Regulation (GDPR)*, accessed at https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation

interference with privacy'. As noted in our submission to the Discussion Paper, DIGI believes such clarification would be helpful; given these concepts are included in the Bill, clarification needs to occur prior to these being legislated.

2.4. Including a definition is also important when we consider the Bill's proposed penalties in the context of other enforcement recommendations contemplated in the Review (as reflected in the Discussion Paper) such as the proposal for a tiered civil penalties infringements that are not serious or repeated. DIGI broadly supports this proposal, and considers it sensible to have a tiered approach, however the effectiveness of such a scheme hinges on the definitional clarity of 'serious' and 'repeated'.

3. Regulatory cooperation

3.1. Recent large-scale data breaches in the telecommunications and insurance sectors have underscored the critical importance of data privacy and cyber security economy-wide, and the serious impact that any such event can have on Austalians.

3.2. The Bill amends the ACMA Act to expand the ACMA's ability to share information to any non-corporate Commonwealth entity responsible for enforcing a Commonwealth law where the information will enable or assist the entity to perform or exercise any of its functions or powers. Assuming that this provision is intended to facilitate better cooperation between the Commissioner and ACMA, DIGI is very supportive of this and other cooperation mechanisms between regulators.

3.3. However, the precise intent of the provision is not explicit in the Bill nor the Explanatory Memorandum. If the intent is that any concerns that the ACMA may find in its regulation of the communications and media sector can be referred to the OAIC, while we have no objections to this, we encourage parity in the allowance of such referrals from other regulators. For example, if not already in place, the same powers should exist in the regulation administered by the Australian Prudential Regulation Authority (APRA) that supervises institutions across banking, insurance and superannuation sectors.

3.4. Additionally, we note that subsection 50(1) (after paragraph b) lists the eSafety Commissioner as an alternative complaint body, in order to ensure that the Information Commissioner is able to transfer complaints and share information with the eSafety Commissioner. Again, DIGI supports cooperation mechanisms between regulators and we have no objections to this, but again call for a wider view in ensuring other sector-specific regulators are afforded such powers to reflect the economy-wide nature of privacy concerns.

3.5. Ensuring parity across sectors is especially important when we take into consideration that the Bill's provides the OAIC with power to make confidential information publicly available if the Commissioner considers it to be in the public interest, which arguably exceeds existing powers of the Office of the eSafety Commissioner and the ACCC.

3.6. In the OAIC's reporting on the Notifiable Data Breaches (NDB) scheme, it is important to note that the industries that consistently make the top five for experiencing data breaches include health service providers, finance organisations, legal accounting and

management services, educational institutions and insurance companies[3]. In order to reflect this data and the economy-wide nature of data privacy concerns, the Bill should consider a more comprehensive view of relevant enforcement and regulatory authorities and entities. This would also reflect the Explanatory Memorandum stated intent that 'The Bill will facilitate better cooperation between the Commissioner and ACMA, and other enforcement and regulatory authorities and entities'.

4. Situating the Bill within Privacy Act reform

4.1. DIGI believes that well-defined and proportionate penalties play an important deterrence role in a modernised privacy regime**.** However, penalties need to form part of other pro-privacy consumer and organisational practices in the reform of the Privacy Act. DIGI's members believe that pro-privacy practices go beyond merely providing privacy policies and notices, and extend to strong accountability-based practices and user controls. They continue to make extensive investments in the privacy of their users, including: having cross-functional privacy experts and teams who ensure that privacy is built into their products and services ('privacy by design'); providing information and tools to provide people with transparency, choices and control in relation to their personal data; and recognising their customers' rights to access, delete, correct and control personal data as part of global data protection frameworks including the Australian Privacy Act 1988, and the European Union's General Data Protection Regulation (GDPR).

4.2. DIGI fully supports modernising of the Privacy Act for a digital era, and sees the Review as a key opportunity to afford consumers choice, control and transparency while encouraging organisational accountability and best practice across the wide range of entities that collect personal information. DIGI recognises that "digital first" social media platforms and large online platforms are often in the spotlight when it comes to questions of data privacy, and are rightly held to a high level of public scrutiny. As a result of that and their depth of technical expertise with data governance, we posit that the privacy, safety and cyber security investments made in the digital industry may exceed those in other sectors that equally use personal information, but do not have as much experience nor the same levels of public scrutiny.

4.3. We also believe that recent data breach events have underscored the importance of data minimisation, as the more information that is required to be collected and retained by companies can increase the severity of a potential breach. Data minimisation requires goods or service providers to not seek to collect data beyond what is reasonably needed to provide the good or service, or to employ adequate measures to anonymise data using proven techniques such as differential privacy. We believe that privacy risks – such as inappropriate use or disclosure or poor security – can be reduced by resolving the tension between data retention requirements and data minimisation best practices. DIGI welcomes the fact that the universally accepted privacy best practice of data minimisation forms part of the existing APPs under the Privacy Act 1988 (Cth). We urge that the Review retain and refresh the data minimisation principle in the reformed Act from a protective viewpoint.

[3] OAIC, *Notifiable data breaches statistics*, accessed at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics