ITI Promoting Innovation Worldwide

November 25, 2020

To: Australia Attorney-General's Department
PrivacyActReview@ag.gov.au

Subject: Australia Public Consultation on the Review of the Privacy Act 1988

The Information Technology Industry Council (ITI) is the premier global advocate and thought leader for the information and communications technology (ICT) industry. ITI's membership is comprised of more than 70 leading technology and innovation companies headquartered around the world from all corners of the information and communications technology (ICT) sector, including hardware, software, digital services, semiconductor, network equipment, and Internet companies.

We are writing regarding the review of the Privacy Act. Like the Australian government, we agree that privacy is essential for the protection of technology users, information, networks, and commerce. However, we believe that some proposals for the review of the Act could unintentionally constrain the ability of Australian and other companies to operate fully in the market, while in some cases offering limited incremental benefit to Australian citizens' privacy.

We believe our interests are fundamentally aligned with Australia regarding the importance of privacy protection, and we welcome the opportunity to provide our views on the review of the Privacy Act. The below recommendations are intended to help protect privacy while leveraging the benefits of data innovation and economic growth. We look forward to working closely with you and would be pleased to discuss further any of the below recommendations.

Recommendations

Add Controller/Processor Distinction

Australia's privacy legislation currently does not contain a controller/processor distinction. ITI believes that it would be important for Australia to consider incorporating such a distinction into its Privacy Act. The EU's General Data Protection Regulation (GDPR) and many other privacy laws around the world, such as in Brazil, Hong Kong, Singapore, and the draft law in India, all take into account the different responsibilities between data controllers/processors to better serve their respective purposes. A clear allocation of accountability between data controllers and processors is key to a successful data protection regime. Under the EU's GDPR, the data controllers, which determine the data processing, are primarily responsible for protecting the privacy of data subjects to ensure that they have one single point of contact for exercising their rights. The data processors should only act on the documented instructions of controllers to fulfill responsibilities. ITI encourages Australia to consider adding such distinction to align with global best practices.

Exempt Biometric Data Captured for Public Safety and Security Purposes

In response to question 2 of the issue paper, ITI suggests granting an exemption for biometric data captured for public safety and security purposes. This should also apply in commercial settings, such as a retail store. In such instances, a security exception would otherwise require consent to capture a person's image through a facial recognition camera. This would not be practical in

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

instances involving public safety and security, including retail. Suggested language for the exemption is below:

- "Nothing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose."
- "Security purpose" means “the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.”

Keep Inferred Data Out of the Scope of Personal Data Definition

In response to question 3 of the issue paper (“Should the definition of personal information be updated to expressly include inferred personal information?”), ITI suggests that Australia’s privacy legislation should maintain the current definition of personal information and should not extend it to include “inferred personal information.” First, inferences similar to economic trends or other analytics are often drawn using aggregated, anonymized, or otherwise de-identified information, meaning that inferences cannot always be assumed to include personal information. Because it may not be possible to identify individuals using this information, it is inaccurate to define all inferences as personal information. Second, to draw inferences businesses often use proprietary technology, advanced models, or other datasets, such that these inferences may also constitute proprietary information. To include inferred data in any right of data portability risks harming businesses if proprietary information could potentially form part of the inferred data. It is also important to note that individual rights, such as data portability, should not include an obligation for entities to transfer inferred data generated by these entities during the course of provision of services to the individual.

Avoid Additional Regulation Governing De-Identified, Anonymized and Pseudonymised Information

In response to question 4 of the issue paper (“Should there be additional protections in relation to de-identified, anonymized and pseudonymized information? If so, what should these be?”), ITI suggests that de-identified, anonymized and pseudonymized information do not need additional regulations governing their use because de-identification, anonymization, and/or pseudonymization are themselves essential privacy techniques and tools to minimize and to ensure that information is stored and processed in a secured manner. In practice, once these processes have been performed in line with existing guidelines, it should not be possible for an Australian Privacy Principles (APP) entity to distinguish personal data from non-personal data in a single dataset. Mandating additional protection on de-identified, anonymized and pseudonymized data with low or no risk of re-identification may discourage the use of those tools and result in more personal information remaining in its original form, which creates more privacy risks.

Include Careful Addition on Right to Erasure

In response to question 46 (“Should a ‘right to erasure’ be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?”), ITI supports the addition of a right to erasure, with important enumerated exceptions similar to those available under international best practices. These would include where processing of personal

information is necessary for one or more of the following: (i) to complete the transaction for which the personal information was provided or fulfill performance of a contract with a consumer; (ii) to exercise any right of freedom of expression or information; (iii) archival, research or statistical purposes; or (iv) to comply with a legal obligation. Furthermore, the APP entity having the primary relationship with an individual should bear the obligation to fulfill an individual's request for erasure (and to notify other entities processing the information), in order to validate or verify that the individual requesting the deletion of the information has a right to do so. This exemplifies one of the key reasons why it is important to introduce a distinction between a data controller and a data processor, primarily because processors can only operate as they are instructed by the controller.

Retain Accountability and Exception to Extraterritoriality

In response to questions 48-49 of the issue paper, ITI supports the current accountability approach and the exception to extraterritorial application. The current exception to extraterritoriality works well and such scope should be retained to minimize conflicts of laws where companies are faced with the choice of breaching one law or another. However, as the Australian government reviews and revises the Privacy Act's provisions on accountability, ITI would like to see a more defined scope for when companies can or cannot transfer personal data overseas. The current "accountability" language in Australia's law is overly broad, and often leads to disputes between cloud service providers acting as data processors and customers in Australia as to what the cloud service provider needs to put in place to protect the personal data in question. For example, it should be expressly clarified that data and server localization in Australia is not required for companies to meet their accountability obligations under the Privacy Act.

Advance International Data Transfers Mechanisms

In response to questions 51-52 of the issue paper, ITI encourages advancing privacy tools and mechanisms to facilitate more cross-border data flows, which underpin the global economy and ensure seamless consumer experiences, among other benefits. A domestic privacy certification scheme could provide companies with a mechanism for demonstrating their compliance with the local privacy laws. However, such a scheme needs to remain voluntary and linked with certification mechanisms supported by Australia, such as the APEC Cross-Border Privacy Rules (CBPR). Linking the domestic certification to international certifications (such as the CBPR) will ensure comprehensive compliance regimes without redundant compliance costs, as the more certifications a company is required to obtain, the more burdensome and costly it becomes for companies (both local and foreign) to meet their compliance obligations. The CPBR system should be fully implemented within Australia in a manner that is fully compatible with, and not duplicative of, any additional domestic certification scheme.

Promote Meaningful Enforcement Instead of Direct Right of Action

In response to question 56 of the issue paper, ITI cautions against the potential addition of a "direct right of action" and ITI supports enforcement by well-resourced and informed regulators. For example,in the United States, a strong and well-resourced Federal Trade Commission, with supplemental enforcement by state attorneys general, has worked well. Such meaningful enforcement is a far better alternative than private or direct rights of action, as this tends to result in frivolous litigation or the development of organizations that profit entirely from class action privacy suits that distract from good compliance work and incentives toward best practices. When

the threat of class action litigation looms, privacy notices become liability-reducing legal disclaimers, and any attempt at risk-based regulation that takes specific circumstances and diverse harms into account is undermined. Individual actions may also conflict with enforcement action already being undertaken by the Office of the Australian Information Commissioner or other bodies in response to complaints or breaches of the Act.

ITI encourages individuals to use the existing complaint handling processes contained within the Privacy Act, such as the right to be compensated via the complainants process, as well as existing statutory rights such as the right to seek injunctions. A further benefit to codifying certification regimes such as the CBPR into the Privacy Act will allow consumers to levy complaints with certification authorities (such as the CBPR System's Accountability Agent), which can be remedied through the CBPR system's existing protocols before rising to regulatory or judicial redress.

Carefully Evaluate Introduction of Statutory Tort

ITI requests further details to respond appropriately to questions 57-61 regarding the introduction of a "statutory tort" for serious invasions of privacy. Specifically, it is critical to understand what would be included within a definition of "serious invasion of privacy" in order to determine the appropriate course of action and provide recommendations. In addition, we would require further context as to the public interest factors the Australian government intends to consider when introducing a "statutory tort for invasion of privacy" (e.g., freedom of expression, right to a fair trial, freedom of the media, the proper administration of government, open justice, public health and safety, national security, and the prevention and detection of crime and fraud). Each of these carries a different level of importance and means of address. We note, however, that if a statutory tort for the invasion of privacy were created, it should be limited to intentional and reckless behavior rather than negligent acts or omissions.

Align Global Practices on Data Breach Notification

In response to questions 63-65 of the issue paper regarding Notifiable Data Breach (NDB) schemes, ITI suggests maintaining current Australian law of allowing 30 days to determine the issuance of a notice. ITI also suggests further clarification regarding the point at which the notification timeframe commences based on an entity's awareness of an eligible data breach (particularly in the case of multi-party breaches). We note that clarification has also been required on this point in applying the personal data breach guidelines under GDPR, with authorities having recognized that awareness depends on the circumstances of each breach. We also suggest, based on the recommendation to include a controller/processor distinction, that only entities classified as data controllers should be required to notify individuals (rather than entities which may not have direct relationships with those individuals). ITI also encourages the Australian government to retain the existing "serious harm" to individuals standard in the NDB scheme for breach notification. Alternatively, the Australian government could consider aligning the eligible breach notification standard to the GDPR standard that only requires notification to individuals where the "data breach is likely to result in a high risk to the rights and freedoms of natural persons". This reduces the need for notification of small breaches that do not present a high risk of individual harm, and avoids the problem of "notification fatigue."