4 December 2020

To: Australian Attorney-General's Department.
By email: PrivacyActReview@ag.gov.au

Privacy Act Review 2020

Thank you for undertaking this consultation on whether the scope of the Privacy Act 1988 (the Act) and its enforcement mechanisms remain fit for purpose. The Digital Industry Group Inc[1] appreciates the opportunity to provide a submission on the questions raised in the Privacy Act Issues Paper of October 2020.

DIGI advocates for policies that enable a growing Australian technology sector that supports businesses and internet users, in partnership with industry, governments and the community. In this submission we have addressed the following issues raised by the Issues Paper:

A. The approach of the review
B. Objectives of the Privacy Act
C. Definition of personal information
D. Consent to collection of personal information
E. Notice of collection of personal information
F. Control and Security of personal information
G. Overseas data flows
H. Regulation and Enforcement (direct right of action/ tort for serious invasions of privacy)

DIGI fully supports the need for consumers to be informed about the use of their data, and the need for comprehensive measures to inform and enable users to both better understand and manage their data use. More can and should be done to ensure that consumers have confidence that their personal information is being used responsibly and that there are appropriate accountability frameworks in place for entities that use Australian's personal information. At the same time, it is critical to have a clear evidence-informed rationale for any significant change to the objectives of the Act which unduly restricts the ability of data-driven industries to innovate and grow, thereby contributing to Australia's economic recovery and future commercial prosperity. This review provides an opportunity for the Australian Government to adopt

[1] The Digital Industry Group Inc. (DIGI) is a non-profit industry association that advocates for the interests of the digital industry in Australia, with Google, Facebook, Twitter, and Verizon Media as its founding members. DIGI also has an associate membership program for smaller digital companies, such as Redbubble and GoFundMe.

privacy policies that can serve as an international exemplar at a critical juncture in Australia's social and economic development. Our response to the Issues Paper reflects our vision of 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.

A. Approach of Review

Economic and Social Context: Now and in the Future

The overall aim of this review is to consider whether the Privacy Act remains 'fit for purpose. We agree that this is a priority issue in the context of the economic and social changes that have accompanied the COVID-19 pandemic, as well as recent transformative developments in the adoption of digital technology by Australians. How the Government responds to recommendations made by the Attorney General's Department in response to these questions will be critical to the economic recovery of Australia and for the future development and prosperity of our society.We ask that consideration of these developments should be factored into the review process, so that recommendations in areas such consent do not inadvertently undermine the outcomes it is trying to achieve.

The benefits of digitisation to consumers were outlined in a major report about Australia's technology sector 'Australia's Digital Opportunity' produced by AlphaBeta and commissioned by DIGI in 2019. For example, that report identified that digital technologies unlock new consumer benefits:

> *'Platforms like Redbubble are allowing customers to access a wider variety of goods and services by linking independent local artists with a global marketplace. Point of sale technologies like Square enable customers to use more convenient, cashless payment methods in previously cash-only in situations like markets and festivals. Video streaming and online education platforms are improving consumers' access to new knowledge, skills, and qualifications. In addition, tools like mobile banking, digital government services and telehealth have made it more convenient for consumers to access these services, saving them time and improving productivity'*[2]

These consumer benefits should be front of mind given the experience of 2020. Digital products and services have enabled Australian's to cope with a highly uncertain 'new normal,' including by delivering critical news and healthcare information via the internet; facilitating business continuity through digital advertising and online customer and supply channels, supporting our education system and helping Australians to maintain their social connections. The Australian Broadband Advisory Council recently reported to Government that the accelerated adoption of digital technology during the pandemic has not only enabled Australian businesses to 'ride the wave' of the pandemic but has also created opportunities to improve productivity and increase the online participation of Australian businesses. 'The task now is to support Australians as they take advantage of the opportunities of broadband and continue to adopt digital applications.[3]' We agree that this task is vital to Australia's economic recovery.

[2]Alpha Beta, *Australia's Digital Opportunity: Growing a $120 billion tech industry*, 2019, 20

[3] Australian Broadband Advisory Council, *Riding the Digital Wave; Report on Covid-19 Trends and Forward Work Program*, November 2020

The experience of 2020 suggests the trend towards accelerated digitisation will play an increasingly critical role in shaping domestic commerce, and international trade. This past year has seen a global transformation of government and businesses practices and consumer behaviours, accompanied by an unprecedented uptake in digital technology over a matter of weeks. A recent survey by McKinsey of 800 executives representing a full range of industries in eight countries reflects the importance of digital and automated technologies in facilitating contactless interactions at a time of social distancing and heightened awareness of hygiene, as well as cost pressures that have arisen in wake of the economic slowdown caused by COVID-19. 85 % of respondents to the survey said their businesses had accelerated the implementation of technologies that digitally enable employee interaction and collaboration, such as video conferencing. Around half of those surveyed reported increasing digitisation of customer channels, for example, via ecommerce, mobile apps, or chatbots. Some 35 % had further digitised their supply chains, for example, by connecting their suppliers with digital platforms.[4]

The Australian experience of the pandemic shows that the flow of digital data both within and across our borders is vital to businesses across all sectors of the economy to produce, transport, market, and sell their products and services in increasingly competitive, globalised marketplaces. In this context, interoperability of the Australian framework for privacy law with the regulations of other major economies' legal regimes is vital. Privacy legislation that requires businesses to apply different obligations in different regimes is costly and unwieldy. There is a high risk that overly complex regulations will result in global companies and start-ups withdrawing or not developing products and services for the Australian market. While in the context of the DPI inquiry, the ACCC said that it 'considers that strengthened privacy safeguards have the potential to encourage growth and innovation in the digital platforms market'[5] the DPI report provided no evidence of how specific recommendations they have made will produce that result. We think it is important that Department's review of what is 'fit for purpose' privacy regulation takes into account the need for pragmatic, stream-lined regulations that support the critical role of digitally enabled products and services in meeting the growing complexity of consumer needs, and the social and economic challenges that will likely endure for Australia years after the pandemic.

Consumer Trust

In setting up the context for the review of the existing Act the Issues Paper invites consideration of research from the Office of the Australian Information Commissioner that shows Australia's trust in the ability of entities to protect their data is declining.'[6] The perspective of the OAIC is consistent with recommendations made in the ACCC's Digital Platforms Inquiry report that the Government consider whether the objectives of the Privacy Act should place a greater emphasis on privacy protections for consumers, to empower them to make informed choices[7].

While the OAIC survey provides important data about shifts in the privacy landscape in the twelve months leading up to the pandemic, Australian's attitudes towards the tradeoff between technological innovation

[4]McKinsey Global Institute, 'What 800 Executives envision for the post pandemic workforce', 20 September 2020. https://www.mckinsey.com/featured-insights/future-of-work/what-800-executives-envision-for-the-postpandemic-workforce.

[5] ACCC (July 2019), *Digital Platforms Inquiry Final Report*, 443.

[6] OAIC, *Australian Community Attitudes to Privacy Survey*, 2020.

[7] ACCC, *Digital Platforms Inquiry Final Report*, 439, 477

and privacy is a contested space. According to cultural anthropologist Genevieve Bell, how Australian's view privacy after this period of rapid technological change is likely to be highly polarized 'They don't enter a neutral landscape', she says. 'Many people say 'I gave up my privacy a long time ago, I don't care' and then there are other people who say 'I do care, I do a lot to protect my privacy and that of my family.'[8] The findings of the OAIC about attitudes over the initial the lockdown period suggest that this assessment is accurate – half (50%) of Australians surveyed considered that their privacy is 'more at risk' in a COVID-19 environment than usual with (48%) being more concerned about the protection of their location information than they were before the outbreak.[9] The way the OAIC presents this data clearly favours the argument that stronger privacy regulation is needed to improve consumer trust. Framed in the alternative the survey results suggest that half of the Australians surveyed were comfortable that the pandemic had *not* increased their privacy risk.

DIGI agrees that consumer trust is an important issue, not the least because it is an essential ingredient of a thriving digital economy. Trust is an essential part of a user's willingness to disclose information or do business with a website.[10]The challenge is to identify what are the key concerns of consumers and what measures are likely to best address those concerns without jeopardizing the task of supporting the further development of Australia's digital capability. We should not assume that Australians all share the same concerns about privacy – for example some may be more concerned about account security, and the risk of fraud, others may be more concerned about the use which is being made of personal data. Any regulatory changes made to enable users make an 'informed choice' should focus on consumer's key concerns, rather than attempting to allay all consumer concerns at the expense of businesses' use of data. Lastly, it is worth noting that a further challenge for designing policy that 'empowers users' is that there is not a lot of research which shows the effectiveness of different kinds of regulatory intervention (including the more prescriptive choice based approach discussed in the Issues Paper) in increasing consumer trust levels in entities that collect their data.

B. Objectives of the Privacy Act

1. *Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?*

The Issues Paper asks that we reconsider the tradeoff in the current Act between the value of individuals' privacy against the value of entities (both commercial and public) carrying out their functions or activities. While acknowledging the importance of data as an economic resource and the extent to which data is

[8] '"We are all interconnected': Coronavirus is reshaping our relationship with technology (smh.com.au) 19 April 2020

[9] https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/

[10] See Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, (2016) 19 *Stanford. Technology. Law. Review*. 431 Ari Ezra Waldman, Privacy, Sharing, and Trust: The Facebook Study, (2016) 67 *Case Western Reserve. Law Review*,193. See also Timothy Morey, Theodore Forbath and Allison Schoop,' Customer Data: Designing for Transparency and Trust', (2015) *Harvard. Business. Review*. https://hbr.org/2015/05/customer-data-designingfor-transparency-and-trust

integrated into business practices , the Paper argues that this balance can be difficult to achieve, particularly for businesses whose core activity is acquiring and dealing in personal information.[11]

The DPI report recommended considering whether changing the objectives of the Act, which currently require that the protection of privacy to be balanced with the interests of business in carrying out their functions or activities. In our view, the DPI report over-indexes the potential consumer harm of digital services. For example, the ACCC states:

> A lack of privacy and control over data-sharing can give a data holder economic leverage over the data subject (for example, by allowing a seller to use their knowledge of consumers to target vulnerable consumers or discriminate against customers on the basis of gender, race or sexual orientation).[12]

Yet the only evidence that the DPI report provides of such harmful consumer practices occurring is in the following example, where the company in question is not a digital platform:

> For example, insurance provider MLC had requested access to the medical records of a consumer indicating that she had accessed mental health services for sexual abuse she suffered as a child in the 1980s, which led to MLC excluding her from mental health coverage in her life insurance.[13]

The Issues Paper does not provide any additional evidence of the types of businesses that are not achieving an appropriate balance between their data collection activities and user privacy.

Given the critical importance of digital technology to Australia's future development, we do not think there is currently a strong case for changing the objectives in section 2A save that it is worth considering whether the Act include two additional objectives;

1) incentivising regulated entities to use less-identified data when reasonably practicable; and
2) the need to facilitate the interoperability of privacy regulation in Australia with global regulations, particularly with relevant provisions of the GDPR regarding cross-border data transfer.

C. Definition of personal information

2. *What approaches should be considered to ensure the Act protects an appropriate range of technical information?*

   Recommendation 16(a) of the DPI report proposed that:

   > *The definition of personal information in the Act be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual*[14].

[11] Issues Paper, 15.
[12] ACCC (July 2019), *Digital platforms Inquiry Final Report* 435
[13] Ibid.
[14] Ibid, 34.

IP addresses and device identifiers are collected by websites for basic and essential functions. Almost every website requires the collection of this essential information to meet basic consumer expectations in relation to the services they access, and the services cannot be provided without such processing. As a result, we do not think that this kind data should be classified as personal data unless they are used, or combined with other data, to identify an individual.

We suggest the scope of the protection provided by the Privacy Act should substantially follow the model of the GDPR. Keeping definitions of concepts such as personal information clear and consistent with other prominent legal regimes such as GDPR is desirable to support the development of digital products and services including by enabling vital cross-border data flows. The GDPR makes clear that technical data are only personal data if they can be used to indirectly identify an individual when combined with other data. Recital 30 relevantly provides that:

> Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.
>
> This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Aligning the scope of data protection offered by the Privacy Act with the EU will benefit consumers and business. Consumers will be reassured that their data has consistent protection across multiple jurisdictions. Businesses operating offshore will be able to standardise their approach to compliance, enabling them to conduct their data processing operations as consistently as possible in different jurisdictions.This approach will also assist national regulators align their views and expectations of data privacy compliance activities as they observe and work with consistent international accountability frameworks.

3. *Should the definition of personal information be updated to expressly include inferred personal information?*

The Issues Paper defines 'inferred personal information as information collated from a number of sources which reveals something new about an individual'. This kind of data is substantially different to the kinds of data generally undertood to be 'personal' to the individual since it is not created by an action of the individual but by entities. We do not think that it is appropriate to include inferred data within the definition of personal information under the Act since, as the Paper acknowledges regulated entities may find it exceedingly difficult to define what kinds of data fall within that concept, creating considerable uncertainty around when requirements around notice and consent are triggered.

The key issue with inferred data, is not about users privacy but around the potential for such data to be processed in ways that amplify bias and inaccuracies via positive feedback loops, that have harmful consequences for data subjects.[15] Understandably, there is concern about the extent discrimination or

[15] See Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops'

bias are introduced through the aggregation and processing of inferred data, especially when it is used for the purpose of profiling. While this is an important issue, we think it is best addressed within another forum.

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

In our view, anonymised, pseudonymous, and aggregated data should not constitute personal information under the Privacy Act. We support an approach in which encourages entities to anonymise, de-identify, or pseudonymise personal data, while allowing them flexibility to make a balanced assessment of the merits of these alternative approaches, based on relevant factors such as the risk of re-identification.

D. Consent to collection and use and disclosure of personal information

26. Is consent an effective way for people to manage their personal information?
28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

The Privacy Act is currently based on the principle of obtaining user agreement with notice in a limited set of cases. The question of whether consent is an effective method of data protection is associated with the question of notice discussed below. In general, we recommend that any changes to the current regulatory settings should focus less on strengthening consent requirements and more on incentivising regulated entities to be better caretakers of data. An approach to data protection which is entirely based on a consent-notice approach is problematic in a variety of ways:

- Consent places a burden on consumers to read and understand privacy notices and then act. Consumers regularly report experiencing "consent fatigue" in relation to an excessive number of consents.

- Consent is hard to get, particularly when there is no user interface, such as with IoT devices. For consent to be legally enforceable it must be freely given, unambiguous, specific, and informed. Meeting such standards requires consent interfaces that set out specific data uses in complex legalistic language which users struggle to read and comprehend.

- Consent that meets legal standards is hard to effectuate in an ecosystem in which data is exchanged, shared, or sold. The IAB EU companies have worked hard to develop the Transparency and Consent Framework v 2.0 but it has been and continues to be a challenge and is only as valuable as the number of companies that use it; and

in: Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum:.10 Years of Profiling the European Citizen*, (2018, Amsterdam University Press)., 112-115

- Consent is a rigid tool for protecting privacy that can impede the development and use of digital products and services. Many publishers support their content with advertising. Acceptance of ads is thus part of the value proposition for consumers -- free content on an ad supported internet.

Ultimately, digital services primarily collect data to provide better services for consumers, with the understanding that better services will both meet consumer demand *and* support business growth We do not support changes to the Act that would require individuals to separately consent to each purpose for which an entity collects, uses and discloses information but we would support changes to the model that would bring the Act in line with the GDPR's balanced approach to the use and disclosure of personal information.

The GDPR provides data controllers with six lawful bases with which they can justify their collection of information of users, summarised as consent, performance of a contract, vital interest, legal obligation, public task, and legitimate interest. We recommend that legitimate interest is included as a basis for data processing., enabling uses of data that presents a reasonable risk to users, or which are compatible with user's expectations, to process data without the need for consent. The UK Information Commissioner's Office explains, this test includes:

- Purpose test ‐ is there a legitimate interest behind the processing?
- Necessity test ‐ is the processing necessary for that purpose?
- Balancing test ‐ is the legitimate interest overridden by the individual's interests, rights or freedoms?

...This means it is not sufficient for you to simply decide that it is in your legitimate interests and start processing the data. You must be able to satisfy all three parts of the test prior to commencing your processing[16].

The advantage of the GDPR approach is that it provides a pragmatic alternative to burdening users with consent in almost every instance of personal information collection, while allowing consent to be more narrowly focused on priority areas such as sensitive data and data collected from children. The large fines associated with GDPR disincentivise companies from not applying this balancing test correctly.

Issues concerning targeted advertising

The DPI report noted that digital platforms may collect personal information without an individual's consent for wide-ranging purposes on the basis that such collection is necessary for the digital platform's functions or activities, even where such practices may not meet consumer expectations.[17] It cited the example of digital platforms collecting web-browsing data of users on third party websites for the platform's advertising related functions. The ACCC considered whether the Act could be strengthened by prohibiting entities from collecting, using, or disclosing personal information of Australians for targeted

[16] ICO 'What is the legitimate interests basis?'https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis

[17] ACCC (July 2019), *Digital platforms Inquiry Final Report 23*

advertising purposes unless consumers have provided express, opt-in consent. In Recommendation 18 the ACCC recommended the introduction of an enforceable Digital Platforms Code which would include requirements to give consumers the ability to select global opt-outs or opt- ins, such as collecting personal information for online profiling purposes or sharing of personal information with third parties for targeted advertising purposes[18]. Under such a proposal, consumers receiving advertising-funded services could still be required by the platform to consent to view advertisements but the user would not be required to consent to view targeted advertisements based on their user data or personal information in order to use the platform. In considering whether there is a need for more stringent regulation of targeted advertising it is important to consider the ACCC's concerns against consumers preferences for free content on an ad supported internet [19] as well as the future contribution of targeted advertising to the economy.

Targeted advertising has reduced the cost of advertising for Australian businesses and contributed to economic growth, especially in small businesses.[20]: A 2019 study of the advertising markets in four countries (Australia, the United States, France, and Germany) explains:

> Better targeting leads to higher returns on investment, while the lower cost of entry opens the door to smaller firms. Small businesses can grow more quickly and easily through digital advertising. Consumers benefit by the increased choice and access to more business.[21]

These benefits are also acknowledged in the ACCC's DPI report: in particular, digital platforms have provided a new advertising avenue for small to medium sized businesses that may not have been able to afford the advertising available on the high-reach traditional newspapers or commercial television and radio networks.[22]

Demand for targeted online advertising services is primarily driven by the number and type of internet users and is projected to grow over the next five years, as more businesses develop an online presence or channels through which their services can be accessed over the internet.[23] We note that the findings of the OAIC survey indicated that most Australians (58%) agree it is fair that they share some information if they want to use a digital service and, if they have to receive any ads, they would prefer that they are targeted (48%). Further, the level of comfort with targeted advertising varies widely across different demographics[24]. We think that in order to accommodate these varying preferences and retain the economic benefit of targeted advertising to the economy, it would be preferable if the Act is amended to codify current voluntary arrangements in the digital advertising industry for users to opt- out of targeted advertising.

---

[18] Ibid 36

[19] https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf

[20] Dr Michael Mandel, 'The Declining Cost of Advertising: Policy Implications', July 2019, https://www.progressivepolicy.org/issues/government-reform/the-declining-price-of-advertising-policy-implications-2/

[21] Ibid

[22] ACCC (July 2019), *Digital platforms Inquiry Final Report,* 92.

[23] IBISWorld, 'Online Advertising in Australia' *Industry Research Report* 26 August 2020.

[24] OAIC, *Australian Community Attitudes to Privacy Survey*, 2020, 32-33

E. Notice of collection of personal information

20. Does notice help people to understand and manage their personal information?
21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?
22. What sort of requirements should be put in place to ensure that notification is accessible; can be easily understood; and informs an individual of all relevant uses and disclosures?
24. What measures could be used to ensure individuals receive adequate notice without being subject to information overload?
The concept of informing people what information about them is held and how it used—is a foundational aspect of privacy law and regulation, not only because it assists people to make choices about their information, but also because it incentivises organisations to handle data responsibly. The ACCC DPI Report found that the current law affords regulated entities considerable discretion about whether they notify consumers about collection of their personal information and how that notice is provided. This, they suggest, creates 'information asymmetry' between the entity and the person whose information is being collected which impacts on individuals' ability to make informed choices about whether to engage with a business[25].

As noted above, we do not support changes to the Act that would require individuals to separately consent to each purpose for which an entity collects, uses, and discloses information or more prescriptive notice regimes for the digital industry. Many of the industries that collect and utilise considerable volumes of personal information do not have the same level of transparency or offer equivalent controls as the digital sector. Note that the Deloitte Privacy Index 2018 observed that digital companies provide greater transparency for their users than non-digital companies.[26]

The main way regulated entities currently inform users about the collection of their data is via privacy policies. The 2020 ACAP survey by the OAIC found that three quarters of surveyed Australians do not read most or all privacy policies, with one third of respondents reading few or no policies.[27]There is considerable research in the US which also shows that privacy policies are hard to read, read infrequently, and do not support rational decision making by internet users.[28] Arguably, a key part of the problem of notice is the design of privacy policies:

> Privacy policies today do not convey information in a way that reflects the embodied experience of internet users because they are designed without the needs of real people in mind. They are written by lawyers and for lawyers. Privacy law, for the most part, has exacerbated the problem. It primarily mandates the content of notice and ignores how that content is

[25] ACCC (July 2019), *Digital platforms Inquiry Final Report*,23.
[26] Deloitte, *Deloitte Australian Privacy Index 2018,* May 2018, https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html
[27] OAIC, *Australian Community Attitudes to Privacy Survey*, 2020,69
[28] See Carlos Jensen and *Colin Potts, Privacy policies as decision-making tools: an evaluation of online privacy notices* (Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vienna, Austria, April 24-29, 2004) 477; Alecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, (2008), 4 I/S:A Journal of . Law. and Policy for the Information Society 543, 563

conveyed: statutes insist that policies include a what-when-how of data use, and regulatory action is often triggered when companies violate the substantive terms of their policies[29].

The DPI report recommended that the notification requirements in the Privacy Act be strengthened. Recommendation 16(b) proposes that:

> • All collection of personal information (whether directly or indirectly) be accompanied by a notice from the APP entity collecting the personal information unless the individual already has the information or there is an overriding legal or public interest reason.
>
> • The notice must be concise, transparent, intelligible, and easily accessible and must clearly set out how the APP entity will collect, use and disclose the information. The notice should be able to be readily understood by persons of the minimum age of the permitted platform user; and
>
> • To reduce information burden, it may be appropriate to implement these requirements with measures such as layered notices or the use of standardised icons or phrases.[30]

The question of how notices can be optimally designed may not be one that is best achieved through prescriptive regulations but through best practice guidelines around the design of notices. For example, research by Ari Ezra Waldman .recommends several practical strategies for online platforms to improve the design of their privacy notices including increasing collaboration between privacy lawyers and technologists in the drafting of notices and committing to embedding privacy protection into the corporate ethos.[31]

F. Control of personal information

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

DIGI members allow their users to delete, access and correct their personal information. DIGI is supportive of measures that give people more meaningful control over their information in a digital world in relation to data erasure requests provided that provision is made for businesses to take a balanced approach to considering deletion requests which takes into account legitimate business purposes for retaining data.

G. Overseas data flows.

As noted in Section A we consider the interoperability of the Australian framework for privacy law with the regulations of other major economies legal regimes is vital to enable cross-border data flows that are

[29] Ari Ezra Waldman, *Privacy, Notice, and Design*, (2018) 21 Stanford. Technology. Law Review. 74, 77,
[30] ACCC (July 2019), *Digital platforms Inquiry Final Report*,35.
[31] Ibid

integral to developing the ecommerce capabilities of Australian business. The Privacy Act should encourage global interoperability, including by:

- Recognising the same or substantially similar grounds for transfer as the GDPR;
- Proactively acknowledging a role for interoperability frameworks like the APEC Cross Border Privacy Rules (CBPR) system where relevant.

We note that Australia has formally signed on to the CBPR but has yet to implement it. DIGI urges the Government to proceed with implementation as a matter of priority to provide more structure and certainty around cross border data flows.

H. Regulation and enforcement

DIGI is inherently sceptical of a direct right of action which incentivises regulated entities to produce highly legalistic disclaimers in privacy notices. and would undermine our preferred regulatory approach which provides clear and consistent requirements that will help create a bridge between Australia and other leading international regimes, thus supporting the digital transformation of society and the economy now, and into the future.

DIGI looks forward to further engaging with the consultation process in relation to the review and with the Government in relation to any related reform proposals.Should you have any questions about this submission, please do not hesitate to contact us.

Jennifer Duxbury
Acting Managing Director
4 December 2020.