Privacy Act Review
Information Law Branch, Integrity and Security Division
Attorney-General's Department
By email: PrivacyActReview@ag.gov.au

Tuesday April 4, 2023

Overview: DIGI's submission to the Privacy Act Review Report

Dear Privacy Act Review team,

The Digital Industry Group Inc. (DIGI) thanks you for the extended opportunity to provide our views on the Privacy Act Review Report, released on February 16, 2023 (the Report), and acknowledge this consultation as a milestone in an important reform process of the Privacy Act (the Act).

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, Spotify, Snap and Yahoo. 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.

At the outset, DIGI wishes to underscore that its members share and support the Government's strong commitment to privacy. DIGI's members believe that pro-privacy practices go well beyond providing privacy policies and user consent notices, but that they extend to strong accountability-based practices and user controls. Members continue to make industry leading 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 give people transparency, choices and control in relation to their personal data; recognising their customers' rights to access, delete, correct and control personal data, and specific protections for minors' privacy.

DIGI recognises that large technology companies are often in the spotlight when it comes to questions of data privacy, and are held to a high level of public scrutiny. However, we consider that there is a high level of technical experience with data governance in 'digital first' companies that may not exist to the same extent in other industries that are also using personal information. In an economy where arguably every company is digital, we believe that Australians should be given a clear expectation of their privacy rights no matter what service they are using.

DIGI therefore fully supports the need for reform of the Privacy Act, and sees the Privacy Act Review as a key opportunity to afford consumers choice, control and transparency while encouraging organisational accountability and best practice economy-wide, across a wide range of sectors.

In this submission, DIGI has provided a brief perspective on all of the Report's 116 proposals. While we acknowledge the comprehensiveness of the Report's evaluations of stakeholder input received on the Privacy Act Review Discussion Paper (the Discussion Paper), important questions remain regarding each recommendation's intended implementation, interconnection and relative Government prioritisation. Therefore, our response to each recommendation is at a principle level at this stage, and we hope to have

the opportunity to further engage with the legislative detail and OAIC guidance in future stakeholder consultations.

In advance of those perspectives on each recommendation, we advance in this covering letter several high-level considerations that we encourage the Privacy Act Review team to consider.

Key recommendations and approaches DIGI supports

1. Strengthened consumer rights

DIGI is extremely supportive of offering consumers strengthened consumer rights, such as the right to erasure, the right to access and the right to object, which mirror similar laws including EU General Data Protection Regulation (GDPR). When applied economy-wide, affording Australians with these consumer rights will empower people with a consistent level of choice, control and transparency over their personal information.

2. Strengthened organisational controls and guidance

However, consumer rights alone will not be sufficient in protecting Australians' privacy, and must be implemented in addition to strengthened organisational controls over the use of personal information. For example, we welcome the proposals aimed at improving the security, retention and destruction of personal information. We also welcome the reinforcement of the data minimisation principle in the Report, which we consider of critical importance, especially in relation to reducing the human impact of data breaches.

Effective organisational controls are contingent on entities subject to the Act (APP entities) being provided with actionable guidance on implementation. DIGI therefore welcomes proposals that both properly resource and empower the Office of the Australian Information Commissioner (OAIC) with the ability to develop guidance in relation to a range of recommendations. The practical success of this guidance will rely on consultation and co-design with industry in order to effectively address many of the implementation questions DIGI raises in this submission.

3. Strengthened minors' privacy, modelled on the UK Age Appropriate Design Code

While children's privacy rights have always been included within the Privacy Act, DIGI believes there is an important opportunity in this reform process to single out and improve privacy protections for Australian minors. DIGI is in principle supportive of the introduction of a children's online privacy code that draws on the UK's Age Appropriate Design Code and other similar models. We agree that the code developer, whether an industry code developer or the OAIC, should be required to consult broadly with relevant experts.

We welcome the acknowledgement in the report that the code developer should consider the relationship between the codes under the Online Safety Act and this proposed code in order to ensure consistency or requirements. DIGI has co-led the drafting of the Online Safety Act industry codes, along with Communications Alliance and a steering group of associations. Should a further discussion about DIGI's code development experiences assist the Government in its exploration of this and related recommendations on codes, we would welcome the opportunity to assist.

4. Harmonisation with the EU and UK GDPR through introduction of controller and processor distinction

DIGI supports interoperability between established international privacy regimes, such as the EU GDPR, in order to provide greater legal certainty to companies, and consistency of experience for consumers who regularly interact with services offered outside of Australia. DIGI welcomes the Report's recommendations that harmonise and interoperate with the GDPR, such as the adoption of the 'data controller' and 'data processor' designations to increase organisational accountability across complex digital supply chains.

The EU GDPR, introduced in 2018, was landmark legislation that has served as the new global model for privacy legislation. It has been implemented by many multinational companies present in Australia, though has also raised compliance burden questions particularly for smaller entities. It is worth the Government noting that the EU GDPR will be reviewed in 2024, and that proposed changes to the UK GDPR have been advanced through the Data Protection and Digital Information Bill, released on March 8, 2023 (after the Report's release). This bill aims to introduce practical changes that the UK Government has positioned as a 'common-sense-led UK version of the EU's GDPR'[1]. The Australian Government should closely consider both of these models and processes as it advances its reforms.

Key recommendations and approaches where we encourage further consideration

1. Lack of diverse legal bases

While DIGI acknowledges and welcomes the proposals that align with EU GDPR in the Report, we consider that there are many areas where closer alignment is needed. As the OECD notes, the significant increase in flows of personal data requires a globally coherent approach that includes national privacy strategies that can act to further privacy interoperability[2].

DIGI is concerned that the Report's proposed model does not interoperate with the six legal bases provided under the GDPR for the lawfulness of processing: consent; contract; legal obligation; vital interests; public task; or legitimate interests. DIGI understands that the current Act provides two legal bases for the processing of personal information: where appropriate notice has been provided to or made available to the data subject, and where the data subject has provided *consent* to the processing for the identified purposes[3]. We are concerned that the Report over-indexes on consent, and does not advance multiple legal bases that would better interoperate with other privacy regimes such as the EU GDPR.

Concerns with over-reliance on consent are well documented. For example, the Information and Privacy Commission NSW has said that 'consent as a legal mechanism is best applied to special cases: non-routine uses and disclosures, for purposes that are not directly related to the primary purpose of

---

[1] UK Department for Science, Innovation and Technology and The Rt Hon Michelle Donelan MP, Press release: *British Businesses to Save Billions Under New UK Version of GDPR*, available at https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr

[2] OECD, *Interoperability of privacy and data protection frameworks*, available at http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

[3] Baker McKenzie, *Global Data Privacy & Security Handbook*, 'Legal Bases for Processing of Personal Data', accessed at https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/australia/topics/legal-bases-for--processing-of-personal-data

collection and in circumstances where no other exemption applies.'[4] In that context, opt-out approaches are general preferable to approaches that compel frequent opt-in requests to consumers

2. Broad definitions and restrictions on targeting

DIGI is extremely concerned that the Report proposes long-term, micro-economic shifts in the viability of digital advertising as a medium for all small and large businesses, Government agencies and not-for-profit organisations, as well as the viability of ad-supported free digital services.

The proposed definition of 'targeting' is overly broad as proposed, encompassing any form of segmentation of a customer database into important groupings (e.g. state of residence), or based on interests and behaviours (e.g. sports), or any personalisation that occurs online, including the prioritisation and sorting of content that a consumer opts in to receiving. Disabling the functionality described as 'targeting' – through the proposed prohibitions and opt-outs – will remove the ability for advertisers and digital services to provide *relevant* information to customers, including the provision of age-appropriate content to protect minors or the restriction of inappropriate content which relies on the creation of exclusionary segments. The removal of relevance from advertising runs counter to consumer interest: An OAIC 2020 survey of Australians that asked 'If I have to receive ads, I'd prefer them to be targeted and relevant to me' found that 35% agreed, and 13% strongly agreed vs. 13% who disagreed and 10% who strongly disagreed.[5]

The economic ripple effect and social impact of fundamentally reducing the effectiveness of digital advertising has not been scoped, and we would foresee the proposals resulting in radical shifts over time in: the viability of businesses that cannot afford traditional advertising, particularly small businesses[6]; limitations in the ability of non-profits and Government agencies to reach key audiences with advocacy and public service announcements; and the potential for the increase in 'pay to play' subscription models to sustain otherwise free digital services, that impact the equality and inclusivity of digital spaces.

3. Uniform and proportionate application of the Privacy Act

DIGI considers this reform process to be an opportunity to provide Australians with protections that they can expect to receive across the wide range of services that process their personal information, and it is appropriate that the current exemptions under the Act be re-evaluated. 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. The reform of the Privacy Act is a critically important moment to improve Australians' choice, control, transparency and confidence in their data privacy, no matter what service they are using.

We hope that the Privacy Act Review team can closely consider DIGI's specific recommendations

---

[4]Information and Privacy Commission NSW, Fact Sheet - Consent and Bundled Consent, available at https://www.ipc.nsw.gov.au/fact-sheet-consent-and-bundled-consent

[5] OAIC (2020), *Australian Community Attitudes to Privacy Survey 2020*, available at https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

[6] The ACCC's Digital Platforms Inquiry report in 2019 acknowledged that "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 network. See ACCC July 2019, Digital platforms Inquiry Final Report, available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report, p. 132

enclosed in the remainder of this submission, along with the overarching considerations that DIGI has highlighted in this overview.

We thank you for your engagement with stakeholders to date and look forward to continuing to engage with the Australian Government on this important process to reform Australia's Privacy Act. Should you have any questions, please do not hesitate to contact me.

Best regards,

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

Table of contents

Responses to specific proposals

In this section, DIGI advances a preliminary response to each of the Report's proposals, along with considerations for the Government. For ease of review, we have endeavoured to categorise the proposals with those that we support in principle (marked as 'Y' for 'yes' in green), those where we are unsure or conditionally support (marked as 'M' for 'maybe' in yellow), and those where we urge further consideration (marked as 'N' for 'no' in red). While we acknowledge the comprehensiveness of the Report's evaluations of stakeholder input received on the Privacy Act Review Discussion Paper, important questions remain regarding each recommendation's intended implementation, interconnection and Government prioritisation. Therefore, our response to each recommendation is at a principle level at this stage, and we hope to have the opportunity to further engage with the legislative detail and OAIC guidance in future stakeholder consultations.

Report proposal	(Y/M/N)	DIGI's preliminary position
3. Objects of the Act		
Proposal 3.1 Amend the objects of the Act to clarify that the Act is about the protection of personal information.	Y	DIGI is supportive of this proposal in principle.
Proposal 3.2 Amend the objects of the Act to recognise the public interest in protecting privacy.	Y	DIGI is supportive of this proposal in principle. We believe this, along with a legal basis equivalent to the GDPR's 'legitimate interests', will assist the global interoperability of Australia's privacy regime.
4. Personal information, de-identification and sensitive information		

Proposal 4.1 Change the word ‘about’ in the definition of personal information to ‘relates to’. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.	Y	We support aligning the definition of 'personal information' under the Privacy Act to the GDPR definition of 'personal data', and encourage its adoption in full. Article 4 of the GDPR defines personal information as: ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’ We welcome the clarification that the connection between the information and the individual is not too tenuous or remote. Building upon that, it is important that IP addresses and device identifiers are not considered 'personal information'. IP addresses and device identifiers are often automatically collected by websites for the basic and essential functions such as providing an online service in the user’s language, based on their location, and to fit the user’s chosen web browser. Arguably, almost every website requires the collection of this essential information in order to meet basic consumer expectations in relation to the services they access, and the services cannot be provided without such processing. While DIGI is supportive of this proposal in principle, because of its potential for alignment with the GDPR, we note the flow-on impacts of this proposal on other proposals, alongside which we have noted our concerns.
Proposal 4.2 Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.	Y	DIGI is supportive of this recommendation in principle. Effective organisational controls are contingent on APP entities being provided with actionable guidance on implementation. DIGI welcomes proposals that both properly resource and empower the OAIC with the ability to develop guidance, and we encourage consultation and co-design with industry in the development of guidance. We would suggest also including a non-exhaustive list of information that is not considered to be personal information by the OAIC.

Proposal 4.3 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.	M	DIGI has some concerns about the interoperability of this proposal with the GDPR. While the Discussion Paper (where the proposal was first put forward) claims that this proposal is 'harmonising the Australian definition with GDPR', DIGI's understanding is otherwise. The GDPR's definition of 'personal data' means any information relating to an identified or identifiable natural person. The GDPR has a definition of 'processing' that encompasses 'collection, and separate to this it advances a definition of 'profiling' which encompasses 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'. It is our view that this proposal is not interoperable with GDPR, as it conflates the GDPR's concepts of *collection* and *profiling*. We see these as distinct acts that should be conceptually separate, and that collection should not by default cover profiling that infers information. Conflating these may be counterproductive to the review's intent, as it may encourage entities to undertake more profiling as this is considered a "baseline" expectation by being included in the definition of collection. Furthermore, DIGI is concerned that the proposal is so broadly scoped that it could capture crawling the web (for example, to train AI, or to develop an index for a search engine). We also suggest that collection in this context requires 'holding' the data in a 'record'. Currently APP entities do not 'hold' personal information under the Privacy Act unless the entity maintains possession and control of a 'record' containing the information. A 'record' does not include a 'generally available publication', which is defined in the Act as a publication which is generally available to members of the public. DIGI notes the flow-on impacts of this proposal on other proposals, alongside which we have noted our concerns.
Proposal 4.4 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.	Y	DIGI is supportive of this proposal in principle. While we consider guidance to be helpful, use cases will vary greatly so the guidance should not be overly prescriptive.

Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.	M	The Act should not be overly prescriptive because of the great variation of businesses that are APP entities, and therefore regulatory guidance developed by the OAIC may be a more appropriate avenue for this clarification. DIGI assumes that certain proposed obligations would not apply to de-identified data, such as consumer rights to access, object or erase. While we are supportive of these rights being afforded to consumers, it is illogical for these rights to extend to de-identified information, which by its very nature is no longer personal information since it does not relate to an identified or identifiable individual. Proposals around de-identification raise implementation questions for those consumer rights. For example, how would an APP entity de-identify data if it can not aggregate that data around a data point? How can they authenticate a consumer record for the purposes of actioning an erasure request without some sort of identification of the requesting consumer? Therefore, we consider the simplest pathway would be an approach which encourages entities to anonymise, de-identify, or pseudonymise personal data, while providing 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.
Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information: (a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure.	Y	DIGI is supportive of this proposal in principle.
(b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.	N	While DIGI understands and appreciates the intent behind this proposal, we consider that this would be difficult to implement in any multinational company. The requirement to ensure that the overseas recipient does not breach the Australian Privacy Principles puts an onus on the APP entity to oversee a level of extra-territorial application of Australian law that may be unrealistic.
(c) Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.	N	DIGI is concerned that the proposed definition of targeting to include de-identified information risks regulating non-personal information that is not tied to an identified person. It is also counter-intuitive and confusing to suggest that de-identified information can be used to target users. This is inconsistent with the policy intent behind privacy laws which is

		to protect information that is personally identifying. We discuss the implications of this in depth in our response to proposals in relation to targeting under Proposal 20.
Proposal 4.7 Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions.	M	DIGI questions the proportionality and appropriateness of criminal penalties in this area, unless 'malicious' relates to the use of the re-identified data for another criminal purpose and the offence is aimed at third parties that exfiltrate personal information from legitimate organisations that collected and processed it lawfully.
Proposal 4.8 Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where: (a) the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way. (b) the re-identification is conducted by a processor with the authority of an APP entity controller of the information.	M	DIGI is supportive in principle that de-identified data should not be re-identified if the re-identification goes against the wishes of the data subject. However, if the data subject has not requested the de-identification, then an APP entity should have the discretion to process its data to serve business needs as long as that processing is otherwise compliant with the Privacy Act.
Proposal 4.9 Sensitive Information (a) Amend the definition of sensitive information to include 'genomic' information, and other amendments as proposed.	Y	DIGI is supportive in principle of the expansion of sensitive data to include genomic information. DIGI suggests that the language in the GDPR definition of 'special categories of personal information' be adopted in relation to the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person.
(b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act. (c) Clarify that sensitive information can be inferred from information which is not sensitive information.	M	DIGI is concerned that 4.9 b) and c) may blur the lines as to what constitutes 'sensitive information' and could therefore be problematic in implementation. It is important to ensure that there is clarity as to what constitutes sensitive data for APP entities to ensure appropriate handling and processing. DIGI understands that Proposals 4.1 and 4.3 make it clear that inferred information can be personal information. DIGI notes related questions about the implications of the proposed prohibition of targeting individuals based on sensitive information (under Proposal 20.8b) for individuals proactively seeking advertising or other information based on their own sensitive data (e.g. ethnic origin or sexual orientation) in relation to Proposal 20.

Proposal 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.	Y	DIGI is supportive of this proposal in principle, however more granularity in the definitions is needed in order to help interoperate with GDPR. For example, the revised Act should adopt the GDPR distinction between precise and coarse location.
5. Flexibility of the APPs		
Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code. In developing an APP code, the Information Commissioner would: (a) be required to make the APP Code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.	M	DIGI is supportive in principle of the OAIC having code making ability and, drawing upon our direct experience developing digital industry codes, we see advantages in industry-led processes being explored in the first instance in order to ensure that codes are reflective of practitioners' experiences and future proofed as technology evolves. In that context, we raise questions about the conditions advanced in the proposal to inform a determination that the OAIC should develop the code instead of industry representatives. DIGI believes the condition of 'where in the public interest' is too broad and open to interpretation. We also believe in many instances it is often the case that no single industry association can act as 'an appropriate industry representative to develop the code'. For example, the Online Safety Act requires codes for eight industry sections, one of which encompasses 'Designated Internet Services' which includes all websites in Australia. This was a code making exercise where there is not a single association that can suitably cover the field. To address this challenge, a steering group was formed which includes the Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance, the Communications Alliance (CA), the Consumer Electronics Suppliers' Association (CESA), the Interactive Games & Entertainment Association (IGEA) and DIGI. The group assigned lead associations for the drafting of sections of the codes that best aligned with their membership, and they coordinated around other functions associated with the code development project. With this experience in mind, DIGI supports the current process whereby the OAIC undertakes a code developer identification process to identify and appoint the industry associations undertaking the code, recognising that a group of associations may be the most appropriate option. We ask that the time period for this process be in addition to the period assigned for code development. We also recommend that the period assigned for code development be a minimum of 12 months in duration, and should commence after detailed regulatory advice on the intended scope and approach of codes is publicly released by the OAIC.

Proposal 5.2 Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12 month period on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.	M	DIGI is concerned that 'in the public interest' does not provide a clear and objective framework to be made, and that this could be politicised. We prefer the threshold of 'in cases of emergency' that was advanced in the Discussion Paper.
Proposal 5.3 Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to: (a) entities, or classes of entity (b) classes of personal information, and (c) acts and practices, or types of acts and practices.	Y	DIGI is supportive of this proposal in principle. A clear definition of 'emergency' is required.
Proposal 5.4 Ensure the Emergency Declarations are able to be made in relation to ongoing emergencies.	Y	DIGI is supportive of this proposal in principle, subject to a clear definition of 'emergency'.
Proposal 5.5 Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.	Y	DIGI is supportive of this proposal in principle, subject to a clear definition of 'emergency'.
6. Small business exemption		
Proposal 6.1 Remove the small business exemption, but only after: (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and	M	DIGI believes that consumers should be afforded a baseline standard of privacy protection no matter what service they are using, and that all entities that use and disclose personal information should all have responsibilities in relation to their users' personal information. To the extent that small businesses do use personal information, particularly in the marketing of their services and other promotional or commercial functions, DIGI believes in the need for a defined set of whole-of-economy privacy requirements that take into account proportionality and public interest. These standards are extremely important, but the compliance burden could be onerous for small businesses. DIGI agrees that an impact analysis, support and consultation with small business will be important to ensure proportionality in their obligations under the Act. This should also include dedicated and ongoing support to small businesses to ensure they are aware of their compliance obligations, and the provision of resources and guidance to assist with their compliance.

(d) small businesses are in a position to comply with these obligations.		
Proposal 6.2 In the short term: (a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and (b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.	Y	DIGI is supportive of this proposal in principle, and higher thresholds of privacy protection for biometric information. We also highlight that there are benefits offered by the use of facial recognition and biometric technologies that mean a nuanced, risk-based approach to regulation is preferable.
7. Employee records exemption		
Proposal 7.1 Enhanced privacy protections should be extended to private sector employees, with the aim of: a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm. Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The	M	DIGI notes the varied stakeholder views in relation to the exemption, and encourages further consultations with expert stakeholder and analysis of how the proposals interact with workplace relations laws to 'stress test' the proposals against varied use cases from employees and employers.

possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.		
8. Political exemption		
Proposal 8.1 Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C.	N	DIGI understands that this proposal narrows the exemption for political parties, yet an exemption is still retained. We are concerned about the proposed exemption from the Privacy Act for registered political parties and political contractors relation to elections and referenda. DIGI has a particular interest in combating mis- and disinformation, having developed The Australian Code of Practice on Disinformation and Misinformation (ACPDM) which provides Australians with safeguards in relation to mis- and disinformation on digital platforms, including during elections. This technology industry code needs to form part of a wider multi-stakeholder approach, and it is possible that the inadvertent misuse of data collected by political parties can be used in organised disinformation and voter manipulation campaigns. We do not consider the removal of this exemption to have implications on the freedom of political communication, rather we consider that the Proposal 18.5d, that introduces the introduces the right to de-index online search results that are 'inaccurate, out-of-date, incomplete, irrelevant, or misleading' may have such impacts. DIGI believes that consumers should be afforded a baseline standard of privacy protection no matter what service they are using, and that all entities that use and disclose personal information should all have responsibilities in relation to their users' personal information.
Proposal 8.2 Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.	Y	DIGI is supportive of this proposal that political entities be required to publish a privacy policy, and we consider that this policy should be required to meet the requirements for privacy notices under the Privacy Act.
Proposal 8.3 The political exemption should be subject to the following requirements:	M	While DIGI welcomes the additions of these safeguards to the exemption, we believe a clearer and more consistent approach would be to remove the exemption.

(a) Political acts and practices covered by the exemption must be fair and reasonable. (b) Political entities must not engage in targeting based on sensitive information or traits which relates to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union. The political exemption should include a savings clause as per Recommendation 41-2 of ALRC Report 108.		
Proposal 8.4 The political exemption should be subject to a requirement that individuals must be provided with the means to: (a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and (b) opt-out of receiving targeted advertising from a political entity.	M	While DIGI welcomes the additions of these safeguards to the exemption, we believe a clearer and more consistent approach would be to remove the exemption.
Proposal 8.5 The political exemption should be subject to a requirement that political entities must: (a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure (b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and (c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption.	M	While DIGI welcomes the additions of these safeguards to the exemption, we believe a clearer and more consistent approach would be to remove the exemption.
Proposal 8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.	Y	DIGI welcomes OAIC guidance to assist all entities with their compliance.

9. Journalism exemption		
Proposal 9.1 To benefit from the journalism exemption a media organisation must be subject to: (a) privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC), or (b) standards that adequately deal with privacy.	M	DIGI considers that media organisations should be able to report on matters of public interest, and that the revised Privacy Act should not preclude them from undertaking their journalistic functions; we are therefore supportive of exemptions for journalistic functions. We understand that this exemption does not extend to the media and marketing functions of media organisations, and if this is the case we consider this to be appropriate. As noted, DIGI believes that consumers should be afforded a baseline standard of privacy protection no matter what service they are using, and that all entities that use and disclose personal information should all have responsibilities in relation to their users' personal information. To the extent that media organisations use personal information in the marketing of their services and other promotional or commercial functions, DIGI believes in the need for a defined set of whole-of-economy privacy requirements that take into account proportionality and public interest.
Proposal 9.2 In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt.	Y	DIGI welcomes OAIC guidance to assist all entities with their compliance.
Proposal 9.3 An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the journalism exemption come into force.	Y	DIGI welcomes periodic review of the journalism exemption.
Proposal 9.4 Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11.	Y	DIGI welcomes the addition of these safeguards to the exemption for journalistic functions, assuming other functions of media organisations are in scope of the Act.
Proposal 9.5 Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.	Y	While DIGI welcomes the additions of these safeguards to the exemption, we believe a clearer and more consistent approach would be to remove the exemption.

10. Privacy policies and collection notices		
Proposal 10.1 Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place.	Y	DIGI broadly supports this proposal in principle. We caution that an over-reliance on notice mechanisms could contribute to 'notice fatigue', much like 'consent fatigue', where users do not pay adequate attention to consent mechanisms. We also note that there can be a tension between the desire to create notices that are 'understandable' and also legally comprehensive. More broadly, DIGI is concerned that the Report over-indexes on consent and does not advance multiple legal bases in order to better interoperate with other regimes such as the GDPR. Further guidance should be provided to APP entities on appropriate accessibility measures.
Proposal 10.2 The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice.	Y	DIGI is supportive of the proposal to retain APP 5.2. Care needs to be taken to ensure that the collection notice is not so long as to discourage users from reading it.
The following new matters should be included in an APP 5 collection notice:		
(a) if the entity collects, uses or discloses personal information for a high privacy risk activity — the circumstances of that collection, use or disclosure		
(b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients.		

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.	M	DIGI agrees with the view put forward in the report that 'it is impractical to develop one standardised template, lexicon or icon for use across all APP entities due to the wide range of contexts in which the Act applies. We would further argue that this same argument holds with regard to the proposal to recommend sector-specific standardised notices, and caution against such an approach for the digital industry in particular which is highly diverse. To illustrate the diversity of the digital industry, under the Online Safety Act, the industry is divided into eight sections: providers of social media services (defined around online social interaction between 2 or more end-users), providers of relevant electronic services (includes any services with messaging, and gaming), providers of designated internet services (includes all websites), providers of internet search engine services, providers of app distribution services, providers of hosting services, providers of internet carriage services, and persons who manufacture, supply, maintain or install certain equipment (includes retailers). We believe that is an incredibly broad set of organisations that would have a multitude of data processing, and therefore question how standardised notices can be relevant across them all. There is a risk to consumers that standardised notices or icons may oversimplify the communication of different data practices. This is particularly important for an industry that is constantly evolving and innovating; we need to be mindful that standardisation applied rigidly to enforce specified formats can deter innovation, or the transparent communication about that innovation. We suggest this proposal be rephrased such that the OAIC may consider guidance or recommendations in relation to the content of notices, but notices and iconography should be tailored to the users of the service and the data collection to which the notice relates. DIGI also notes that this recommendation is not featured in the GDPR.
11. Consent and privacy default settings		

Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.	M	DIGI supports this definition for the most part, for its broad alignment with the features of GDPR and that it rests on affirmative action. DIGI is only concerned about areas where the definition of consent differs from that of the GDPR through its inclusion of 'current'. Under GDPR, 'consent' of the data subject 'means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Further rationale needs to be provided for the inclusion of 'current'. While we appreciate the intent of this is to ensure the data subject's continued permission, we are concerned that 'current' sets too high of a standard unless consent is continually being resought, which would result in considerable consent fatigue if data subjects had to regularly re-consent across the wide range of services that they utilise. We believe the issues underlying this proposal can be better addressed by affording consumer rights to withdraw consent at any time. More broadly, we are concerned that the Report over-indexes on consent and does not advance multiple legal bases in order to better interoperate with other privacy regimes such as the EU GDPR. Concerns with over-reliance on consent are well documented. For example, the Information and Privacy Commission NSW's fact sheet on consent and bundled consent advances five comparable elements required for consent, however concludes that 'The five elements required for a valid consent set a high standard for organisations seeking to rely on 'consent' to authorise their activities.... Consent as a legal mechanism is best applied to special cases: non-routine uses and disclosures, for purposes that are not directly related to the primary purpose of collection and in circumstances where no other exemption applies....Not all activities will be capable of meeting these five elements'[7].
Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.		In general, as noted, DIGI is very supportive of OAIC guidance. The next stage of the process should carefully consider the experience of other countries where regulatory guidance has been prescriptive and consumers have found the experience burdensome without enhancing levels of privacy protection. We caution against sectoral standardised consents, per our comments in relation to Proposal 11.1. Standardisation of consent requests may only work for small businesses with a single product offering, and could be considered in the context of supporting small business compliance efforts. This proposal will be far more challenging for large multinational businesses with multiple products, underscoring the importance of ensuring that the guidance is voluntary and co-designed with a range of industries and design experts.

[7] NSW Information Privacy Commission, *Fact Sheet - Consent and Bundled Consent*, available at https://www.ipc.nsw.gov.au/fact-sheet-consent-and-bundled-consent

Proposal 11.3 Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.	Y	DIGI supports this recommendation in principle, and notes that it is aligned with the GDPR. We note that withdrawal of consent will sometimes result in the inability to use a service, when a data subject withdraws consent for the privacy policy or fundamental data processing. Providers should not be prevented from this practice.
Proposal 11.4 Online privacy settings should reflect the privacy by default framework of the Act. APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.	M	DIGI supports 'privacy by design' where consumer choice is embedded, and we agree that privacy settings should be clear and easily accessible for service users. Depending on how it is defined, a privacy by default approach may not always allow a service to offer the best available version of their product to attract consumers; for example, it may restrict the customisation of a website to a particular locale. Depending on how 'privacy by default' is defined, requiring this could have a business impact on the provision of quality digital services that are in line with consumer expectations. 'Design' rather than 'default' ensures consumer choice and business flexibility, and should be considered alongside the provision of consumer rights of which DIGI is highly supportive.
12. Fair and reasonable personal information handling		
Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.	M	DIGI agrees in principle that personal information collection, usage and disclosure should be generally fair and reasonable in the eyes of a reasonable person. Currently, the Privacy Act requires entities to *collect* personal information by fair and lawful means, with no equivalent requirement for the *use* or *disclosure* of personal information. Our understanding is that Proposal 12.1 will require the collection, use and disclosure of personal information to be fair and reasonable in the circumstances *irrespective* of consent. The current Privacy Act does not define 'fair' but an amendment has defined a 'fair means' as one that 'does not involve intimidation or deception, and is not unreasonably intrusive'[8]. We recognise that the concepts of 'fair' and 'reasonable' exist in other areas of Australian federal law, and we understand the preference to incorporate Australian legal concepts in the updated Act. In Australia, the relatively new notion of fairness as a consumer protection standard has sat within the Australian Consumer Law (ACL) which provides a definition of an 'unfair contract'; however the ACL does not define what a proactive obligation to be *fair* looks like. DIGI notes that Article 5 of the GDPR references principles relating to processing of personal

[8] OAIC, *Chapter 3: Australian Privacy Principle 3 — Collection of solicited personal information*, available at https://www.oaic.gov.au/__data/assets/pdf_file/0010/1207/chapter-3-app-guidelines-v1.pdf

		data, which include that 'personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'. However, DIGI sees fundamental differences between Article 5 of the GDPR and Proposal 12.1 of the report; the former advances principles, and that the latter advances a more prescriptive 'fair and reasonable' test with consideration of very different factors. Other principles under Article 5 include purpose limitation, data minimisation and accuracy, whereas the test advanced under 12.1 refers to the nature of the personal information, the volume of it, and to whom it relates. DIGI considers these to be very different factors, and we therefore question the interoperability of Proposal 12.1 with Article 5 of the GDPR. As noted earlier, DIGI's understanding of the Report as a whole is that it over-indexes on 'consent' as a legal basis. As currently proposed in the Report, we are additionally concerned that the 'fair and reasonable' test is an overlay that is required in addition to, and irrespective of, consent. We consider that the most effective way to operationalise a 'fair and reasonable' standard would be through the creation of a 'fair and reasonable' legal basis, modelled on the 'legitimate interests' legal basis under GDPR. It is worth noting that the legitimate interests legal basis also advances a form of balancing test – including questions around purpose, necessity and data subject's interests – which should be aligned with an updated 'fair and reasonable' test, if reconfigured as a legal basis. Creating such a legal basis puts the onus on entities to ensure the legitimacy and fairness of their data processing, rather than putting the onus entirely on consumers though a model that only provides consent as a legal basis. We are concerned that the overlay approach will create confusion, as it will need to be applied in addition to obtaining consent; such an approach makes the 'fair and reasonable' overlay difficult to operationalise, in a manner that may compromise its intent and effectiveness. In the absence of additional legal bases, DIGI is concerned that overemphasis on consent models also creates 'consent fatigue' for Australian consumers, as well as raising questions around interoperability. The Report references Singapore as a jurdisdiction with a comparable standard. Section 11(1) of Singapore's Personal Data Protection Act 2012 (PDPA) requires consideration of 'what a reasonable person would consider appropriate in the circumstances' when they undertake any action that is subject to the Data Protection provisions. However, Singapore's PDPA has a number of provisions referencing the reasonableness standard *without* imposing a separate consent obligation. From the last PDPA amendments, consent is not the only legal basis for processing and this list has the potential legal bases for processing personal data[9]. It includes personal data necessary to fulfil a legitimate interest of the controller or third

[9] Baker McKenzie, *Legal Bases for Processing of Personal Data*, available at https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/singapore/topics/legal-bases-for--processing-of-personal-data

		party, provided the interest is not overridden by data subject's privacy interests or data subject has not exercised the right to object. Australia could also consider adopting Singapore's approach of introducing legal bases along with a 'fair and reasonable' principles that do not duplicate or confuse obligations. Clarity around obligations could be improved through OAIC guidance that assists APP entities in determining what categories of data processing be considered 'fair and reasonable'. For example, the UK GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests[10].
Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances (b) the kind, sensitivity and amount of personal information being collected, used or disclosed (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (d) the risk of unjustified adverse impact or harm (e) whether the impact on privacy is proportionate to the benefit (f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and (g) the objects of the Act. The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: (a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and	Y	Subject to our comments in relation to Proposal 12.1, DIGI agrees in principle that the matters identified are important considerations in determining standards of fairness and reasonableness. We would suggest interoperability with the balancing test advanced under the GDPR's legitimate interests, which will help operationally guide APP entities with their compliance. The list of factors to be taken into account should also include what is technically and economically feasible for a business. Any failure to agree to a request that is manifestly unfounded and excessive should not mean an APP entity is acting unfairly or unreasonably.

[10] UK Information Commissioner's Office, *Lawful basis for processing*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

(c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.		
Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.	M	In relation to this proposal, DIGI reiterates its comments in relation to Proposal 12.1. In short, DIGI considers that there should not be multiple layers requiring consent and the application of a 'fair and reasonable' test. As noted, DIGI's interpretation of the Report is that it over-indexes on *consent* as a legal basis, and that the 'fair and reasonable test' is a form of overlay, rather than a legal basis. However, the wording of the proposal here raises questions about that interpretation through its reference to 'irrespective of whether consent has been obtained', which works from an assumption that there may be use cases where consent is not obtained. This adds to the confusion of this model which would be simplified through the provision of other different legal bases for data processing. This would provide clarity to entities in circumstances where, as this proposal acknowledges, consent cannot be obtained. DIGI is concerned that this proposal does not account for advanced data processing functions that entities need to undertake to deliver aspects of their services which may involve sensitive data processing, for example, which may not meet the criteria of the fair and reasonable considerations (under Proposal 12.2) but that deliver upon the express wishes of the data subject obtained through specific consent. While Privacy Reform should serve to standardise expectations, the direction of the reform should not homogenise the extremely varied needs of users of the wide range of APP entities.
13. Additional protections		
Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. (a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity. (b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.	M	DIGI is supportive in principle of Privacy Impact Assessments, but we consider that they should be proportionate to the processing and the APP entity type. DIGI is concerned that the definition of high risk activity proposed ('likely to have a significant impact on the privacy of individuals') is vague. While guidance is welcome, having this indeterminate wording in the Act will create legal risk for APP entities and confusion as to when a Privacy Impact Assessment must be taken. DIGI considers this approach different to EU GDPR's rights based approach which frames the Privacy Impact Assessment as an early warning system to assess high risks impacts to rights and freedoms of individuals. Furthermore, if the

The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.		assessment is to provided to the OAIC, this should be undertaken on a confidential basis as the data and the nature of processing may contain proprietary information.
Proposal 13.2 Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by the government of the regulation of biometric technologies.	Y	DIGI agrees that risk assessment requirements for facial recognition technology should be considered, but we also consider that these technologies provide benefits, and we would support a risk-based approach that results in balanced outcomes for Australian consumers Consistent with Proposal 13.1, there should be a focus on higher privacy risk applications.
Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.	Y	OAIC guidance is generally welcome, and we encourage a consultative approach in developing the guidance with practitioners engaging in the development of these new technologies, along with a process to iteratively future proof the guidance as technology evolves.
Proposal 13.4 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.	Y	DIGI is supportive of this proposal in principle.
14. Research		
Proposal 14.1 Broad consent for research	Y	DIGI broadly supports this proposal in principle, though we raise questions about 'broad' and how it will be implemented. DIGI also interprets this to be equivalent to legitimate interests processing under GDPR, and therefore we consider this another reason for the Government to

Introduce a legislative provision that permits broad consent for the purposes of research: (a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply. (b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.		introduce a 'legitimate interest' equivalent legal basis whereby categories of activities are identified, which may include research.
Proposal 14.2 Consult further on broadening the scope of research permitted without consent for both agencies and organisations.	Y	DIGI is supportive of this proposal in principle.
Proposal 14.3 Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.	Y	DIGI is supportive of this proposal in principle.
15. Organisational Accountability		

Proposal 15.1 An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure.	M	DIGI broadly supports this proposal in principle, while noting that it could create an onerous reporting requirement and that compliance would be assisted through guidance on how to differentiate between primary and secondary purposes. For example, an APP entity might contract a third-party security partner as a data processing and it may be unclear to entities whether this would constitute a secondary or primary purpose. This again underscores the importance of a legal bases model, as well as a controllers and processors model, based on GDPR in providing entities with certainty and clarity around the legitimacy of different data usages. More broadly, we consider Proposal 15.1 is a relatively limited view of organisational accountability. Organisational accountability should feature prominently as a privacy and data protection principle enabling companies to demonstrate accountability for data in its custody, care and control. This is in accordance with the APEC Privacy Framework and many other existing and developing international standards (e.g. OECD Transborder data flows, Singapore PDPA's accountability approach, OECD government access to private sector data). In that context, DIGI also recommends a clear link to be made between proposal 15 and 23, in particular to recognise CBPR certification as one of the ways to achieve interoperability and meet the relevant expectations in Proposal 12.
Proposal 15.2 Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.	Y	DIGI broadly supports this principle. We consider this to be a more proportionate approach for different businesses than the designation of a distinct Data Protection Officer. However, it is important to clarify that this employee may be responsible for Australian privacy compliance, but that the employee does not need to be employed by an Australian entity or domiciled in Australia. In regional and multinational companies, primary responsibility for privacy compliance and expertise is often located in global or regional headquarters.
16. Children's privacy		

Proposal 16.1 Define a child as an individual who has not reached 18 years of age.	N	DIGI agrees that minors require additional privacy protections under the revised Act, and we support the introduction of a code that draws on the UK 's Age Appropriate Design Code and other comparable models. However, we consider the approach of using age 18 inconsistent with the established global laws on the digital age of consent. The first data protection law to set a digital age for users, below which parental consent is required, was the Children's Online Privacy Protection Act (COPPA) in the US, which set the minimum age at 13. In the EU, the GDPR set the age below which parental consent is required at 16, giving member states the option to lower this to age 13. In practice, the majority of EU member states have settled on age 13, with only a third opting to retain 16 as the appropriate age. These two laws have been influential in relation to why most globally-accessible digital services have age restrictions between 13 and 16 in place. From an implementation perspective, digital services which are generally globally accessible, require consistency and interoperability with the relevant laws in major markets such as the US and EU. Additionally, there are questions about the digital inclusion of young people that need to be further explored in discussion with experts in that area.
Proposal 16.2 Existing OAIC guidance on children and young people and capacity should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise. The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.' Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary to their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).	M	This Proposal appears to be consistent with Article 1 UNCRC which allows for the age of majority to be obtained earlier, and establishes minimum ages for certain purposes, including the changing capacities of children. DIGI posits that APP entities will not be able to make informed assessments as to the capacity of minors using their services, particularly as such assessments would require intrusive data collection practices. Taking into consideration the concerns raised in relation to Proposal 16.1, and recognising that Privacy Act defines a child by reference to Family Law Act 1975 as under 18, a more practical and globally consistent approach for the digital world would be to set the revised age of digital consent to 13, or no older than 15.

Proposal 16.3 Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child. In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.	Y	DIGI broadly supports this proposal for information addressed specifically to a child, while noting the varying reading levels of children of different ages, and the need for APP entities to accurately describe their data processing without oversimplification.
Proposal 16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.	M	DIGI agrees that specific privacy protections for minors should be expanded upon within the Privacy Act. DIGI supports an Australian code modelled on the UK Age Appropriate Design Code, which requires services to have regard to the best interests of the child. Having said that, our understanding of 'the best interests of the child' is that it concerns whatever is best for that individual child. In some instances it may be best to restrict a particular minor from a service, however in other instances it might be in the best interests of the child to have access to a digital service. Parents or guardians can make judgements on what is in the best interests of the child, not APP entities, because service providers rightly do not have that knowledge. More thinking needs to be done about how we apply this principle to children in a general sense in the digital world through OAIC guidance. For example, that guidance might determine that a risk based approach is to ensure that minors are not inadvertently excluded from essential online resources like search and news media.
Proposal 16.5 Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services. The code developer should be required to consult broadly with children, parents, child development experts, child welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted. The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.	Y	DIGI is supportive of the introduction of a Children's Online Privacy Code that considers effective practices from other markets and reflects the risks and benefits of different processing purposes to children. We agree that the code developer, whether an industry code developer or the OAIC, should be required to consult broadly with relevant experts in its development. Further consideration by the OAIC would need to be given to the threshold 'likely to be accessed by children', noting that organisations in the UK have found this vague and therefore difficult to operationalise. Consideration should be given instead to using US Children's Online Privacy Protection Rule (COPPA) language of 'targeted or directed towards' as it provides more clarity and would exclude general audience type sites, such as news. DIGI has considerable experience in relevant code development having co-led with Communications Alliance, alongside a steering group of associations, the development of industry codes under the Online Safety Act. We welcome the acknowledgement in the report that 'the code developer to consider the relationship between these and the children's online privacy code, to ensure that requirements are consistent.' Should a further discussion about

		DIGI's code development experiences assist the Government in its exploration of this and related recommendations on codes, we would welcome the opportunity to assist.
17. People experiencing vulnerability		
Proposal 17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.	Y	DIGI is supportive of this proposal in principle, and the need for OAIC guidance. There should be consideration given to how vulnerable people exercise expanded consumer rights (e.g. erasure) on APP entities, such as through nominated representatives. However, we note that the challenge for industry practitioners will be how to determine that someone is vulnerable without collecting more information.
Proposal 17.2 OAIC guidance on capacity and consent should be updated to reflect developments in supported decision making.	Y	DIGI is supportive of this proposal in principle, and the need for OAIC guidance. In relation to other relevant developments, the OAIC should ensure its approach guides the The NSW Department of Communities and Justice work to an interjurisdictional work program, endorsed by the Meeting of Attorneys-General (MAG) on 12 August 2022, to develop a nationally consistent scheme to access to digital records upon death or loss of decision-making capacity.
Proposal 17.3 Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.	Y	DIGI is supportive of this proposal in principle.
18. Rights of the Individual		
Access and Explanation		

Proposal 18.1 Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features:	Y	DIGI is extremely supportive of enabling Australians with the right of access, consistent with the EU GDPR and other jurisdictions. We note that the addition of 'explanation' under the proposal is a departure from GDPR, and we question its scalability as it will require human intervention for each access request if user-specific information is expected. We propose that this be clarified to an explanation of the data processing functions at a general summary level, rather than anything user-specific. It is also worth noting that the California Consumer Privacy Act of 2018 (CCPA) does not require businesses to disclose their trade secrets in response to consumers' requests for information .
(a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act)	Y	DIGI is supportive of this proposal in principle.
(b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual	Y	DIGI is supportive of this proposal in principle.
(c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual	Y	DIGI is supportive of this proposal in principle. As noted above in relation to Proposal 18.1, the provision of an explanation should be at a general summary level, rather than user-specific, so as to ensure the scalability and automation of this function.
(d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information	Y	DIGI is supportive of this proposal in principle.
(e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual	Y	DIGI is supportive of this proposal in principle.
Object		

Proposal 18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.	Y	DIGI supports the right to object under the GDPR, where a right to object is only available for data processed on the grounds of legitimate interests or public interest. In the development of a right to object, it will be important to ensure this proposal, and Proposal 20, do not impede advertising-supported business models, as consumers may object to advertising and expect an advertising-free version of their services that the provider will not be able to offer for both technical or budgetary reasons. Furthermore, if the consumer objects to processing that is fundamental to the provision of the service, the request may not be able to be honoured without the denial of the service altogether. Given these constraints, DIGI considers that the right to erasure provides a more actionable consumer right in general than the right to object.
Erasure		
Proposal 18.3 Introduce a right to erasure with the following features: (a) An individual may seek to exercise the right to erasure for any of their personal information. (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.	Y	DIGI is supportive in principle of this proposal, and our relevant members honour erasure requests from users under the GDPR and other laws. We agree that a 'right to erasure' should be introduced in the Act, compatible with GDPR. DIGI notes that the scope of this proposal may have expanded from the version proposed in the Discussion Paper, and we encourage analysis to encourage compatibility with GDPR and internationally recognised human rights such as the access to information.. Guidance will need to be provided on the scope of such erasure requests, after technical consultation with industry, once the Act's definitions are in final form. Consideration needs to be given to how the right to erasure will interact with forthcoming defamation reform, under the both Stage 2 law reform process of the Model Defamation Provisions. This should include guidance as to whether the right to erasure concerns the public posting of content, and whether this will be seen as an alternative pathway for defamation complainants to disassociate themselves with allegations in public content. Consideration may need to be given to whether an independent adjudicator can determine when objectionable content pertaining to an identified individual should be erased from the Internet.
Correction		

Proposal 18.4 Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control.	M	DIGI is supportive of the right of rectification, consistent with the EU GDPR which enables individuals to have inaccurate or incomplete data rectified by the data controller. DIGI considers that further consideration is needed on how the 'right to correction', if expanded to all generally available publications online, would interact with the journalistic exception. This could see the permission of 'uncorrected' information on journalistic sources, yet the obligation to correct this information when the journalistic information is republished or quoted on digital services.
De-indexing		
Proposal 18.5 Introduce a right to de-index online search results containing personal information which is:		DIGI is concerned about the implementation and implications of this proposal.
(a) sensitive information [e.g. medical history], or (b) information about a child, or	M	Our concerns are largely with C and D, and we note that we are broadly supportive of the proposals under A and B.
(c) excessively detailed [e.g. home address and personal phone number], or (d) inaccurate, out-of-date, incomplete, irrelevant, or misleading. The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.	N	However, we consider that the proposal under C would need to be limited to excessive personally identifiable information, such as that which may be used for doxxing. The definition of 'excessively detailed' is problematic and unclear, and the length or specificity of content should not provide grounds for removal, unless there is an invasion of privacy of the data subject. We are extremely concerned with the implications of D. While DIGI, as the code developer and administrator of the Australian Code of Practice on Mis- and Disinformation, is supportive of search engine efforts to address mis- and disinformation, the concepts of 'inaccurate, out-of-date, incomplete, irrelevant, or misleading' are highly broad, subjective and not able to be implemented at scale. The de-indexing of content that was subjectively considered to fall into these categories would have a major chilling impact on the availability of information that is accessible via search engines. Search engines are generally intended to reflect the lawful content available on the world wide web, although Google, for example, does already remove search results to protect limited categories of personal information. Paradoxically, the proposal would permit the original information to be available on the originating webpage, but the webpage would not be able to be found via a search engine. We consider this recommendation to have the potential to seriously impact freedom of expression and political communication in Australia, and we note that

		there are other proposals in the report -- such as the exemptions for political parties, and the journalistic exemption -- that are aimed at preserving these same ideals. The freedom of expression concerns with the EU's Right to be Forgotten are well documented, with this being used in relation to news articles with reputational impact[11]. DIGI is also concerned about the extraterritoriality of the provision, which does not appear to be jurisdictionally limited to Australia. On this point, we note that the EU's Court of Justice has limited the scope of the "right to be forgotten," so that websites can't be forced to censor content outside of the EU[12].
Exceptions		
Proposal 18.6 Introduce relevant exceptions to all rights of the individual based on the following categories: (a) Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities. (b) Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual. (c) Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.	Y	DIGI is supportive of this proposal in principle.
Response		
Proposal 18.7 Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.	Y	DIGI is supportive of this proposal in principle, assuming it equates to inclusion in the entity's privacy policy. It is worth noting that there is often limited space within privacy notices to accurately detail all privacy rights afforded to the data subject, alongside other consent requirements (such as in relation to seeking consent for direct marketing).

[11] Techdirt (11/10/2019), How A Right To Be Forgotten Stifles A Free Press And Free Expression, available at https://www.techdirt.com/2019/10/11/how-right-to-be-forgotten-stifles-free-press-free-expression/
[12] Techdirt (11/10/2019).

Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.		
Proposal 18.8 An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.	Y	DIGI is supportive of this proposal in principle, and considers that OAIC guidance on 'reasonable assistance' may be helpful in ensuring APP entities can implement the proposal.
Proposal 18.9 An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.	Y	DIGI is supportive of this proposal in principle.
Proposal 18.10 An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding.	Y	DIGI is supportive of this proposal in principle, assuming that it enables automated receipt of requests in order to ensure that APP entities can manage these requests at scale and large volumes.
An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.	Y	DIGI is supportive of this proposal in principle.
19. Automated decision making		
Proposal 19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.	M	DIGI is supportive of the disclosure of information used in automated decision-making in privacy policies. However, the threshold of 'legal or similarly significant effect on an individual's rights' is unclear as to which rights this relates. The Government might consider defining automated decision-making as involving 'no meaningful human involvement', consistent with the approach being considered to reform the UK GDPR, rather than 'substantially automated decisions'.
Proposal 19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.	M	OAIC guidance is welcome, and clarity is required as to what rights this encompasses. Some rights will have a higher importance, such as human rights in relation to non-discrimination. Such rights need to be clearly differentiated from user preferences, for example in areas such as advertising.

Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.	M	DIGI supports the provision of information in general terms, however balance is required in the transparency provided to respect the proprietary nature of automated technology. DIGI reiterates its comments made in relation to proposals 19.1 and 19.2 in relation to the threshold related to this right. Balance is also needed to recognise that providing information does not enable bad actors to 'game the system', and we would suggest an exemption from 'meaningful information' may be required where automated decision making is being utilised to assess provision of services and information may aid circumvention of controls. Additionally, we suggest that 'legal or similarly significant effect' should relate to rights, rather than preferences. Finally, as noted, the Australian Government may also consider the approach being considered to reform the UK GDPR that is focused on automated decision-making with 'no human involvement'.
20. Direct marketing, targeting and trading		
Proposal 20.1 Amend the Act to introduce definitions for:	M	We have no objection to the introduction of definitions, assuming the definitions will be subject to further consultation. Here we express some concerns with the preliminary concepts related to these definitions advanced in the report.
(a) Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material.	M	DIGI considers that this definition should advance the mediums that constitute 'direct marketing', and confine this to as email, mail or telephone marketing. The current definition advanced is quite broad and non-specific. In relation to the component of the definition that recommends a focus on 'promoting the aims and ideals of any organisation', it is worth noting that the bill intended to reform the UK GDPR expands the ability to rely on opt-out consent to noncommercial organisations that are furthering charitable, political or other noncommercial objectives, if the individual's contact details were obtained in the course of the individual expressing interest or offering support to the objective[13].
(b) Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).	N	DIGI is concerned that the proposed definition of targeting is overly broad as proposed. As drafted, we understand that this definition encompasses any form of segmentation of a customer database into groups, such as by state of residence, including for the purposes of contextual advertising (i.e.the practice of placing ads on web pages based on the content of those pages using an ad network, which involves segmenting ads based on parameters like keyword or website topic). We also understand that it encompasses any personalisation that occurs online, including the prioritisation and sorting of content that a consumer opts in to receiving.

[13] International Association of Privacy Professionals (IAPP), *The Privacy Advisor*, (8/3/2023), "Top ten takeaways from the draft UK GDPR reform", available at https://iapp.org/news/a/top-ten-takeaways-from-the-draft-uk-gdpr-reform/

		Businesses across the economy undertake list segmentation and personalisation in order to understand their customers, and to provide them with relevant content. The functionality described in targeting is the backbone of providing any sort of customer with relevant information. DIGI is extremely concerned that this well-intentioned privacy proposal will affect the business, advocacy and marketing functions of a wide range of small and large businesses, Government departments and non-profits, by restricting their ability to communicate with relevance to their customer base. For example, this definition would restrict the targeting of an offer or a campaign to residents in one state in Australia e.g. the ability to show an ad in NSW, in compliance with relevant state laws, instead of having a NSW-based offer displayed in other states. In particular, DIGI is concerned that the current definition risks regulating non-personal information that is not tied to an identified person. This is inconsistent with the policy intent behind privacy laws which is to protect information that is personally identifying. The inclusion of deidentified information and unidentified information in the definition of targeting is legally confusing and impractical as deidentifed information cannot by definition be used to tailor online services, as it cannot be used to diffrentiate users. Coupled with the expanded definition of personal information under Proposal 4.1, would also have significant unmeasured economic consequences in relation to proposals (such as 20.2) to restrict targeting. The result of this definition may be to include interests and behaviours in the definition of targeting (e.g. an interest in sports) that are key in ensuring advertising is relevant. Any restrictions on the use of interests and behaviours in targeting will have a material impact on the relevance of advertising that consumers experience online. It will have a detrimental impact on the ability of businesses, particularly small businesses, to connect with customers with interests and behaviours relevant to their services. An OAIC 2020 survey of Australians that asked 'If I have to receive ads, I'd prefer them to be targeted and relevant to me' found that 35% agreed, and 13% strongly agreed vs. 13% who disagreed and 10% who strongly disagreed[14]. Instead of 'targeting', DIGI instead recommends that the Act advance a definition of 'targeted advertising' that focuses on paid content, taking into account further industry consultation on the specifics of this definition.

[14] OAIC, (September 2020), *Australian Community Attitudes to Privacy Survey 2020*, available at https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

(c) Trading – capture the disclosure of personal information for a benefit, service or advantage.	M	DIGI disagrees with the need for a distinct definition of 'trading', noting that both the GDPR and the UK GDPR do not have a distinct definition of trading, rather encompassing this within the definition of processing. This serves to highlight the definitional challenges of this proposed concept. If a definition of trading is to be retained, it should be narrowed to capture financial benefit only. This has become a common definition in the US 'exchange of personal data for monetary consideration by the controller to a third party[15]'. For example, the definition could be linked to the sale of user information to third parties for direct marketing. There should not be a more expansive definition that encompasses the sharing of information to legitimate third parties for other data processing within a supply chain. DIGI is concerned that, as drafted, the definition could encompass the sharing of personal information to third-party fraud prevention services, because this would be captured in the definition of 'service'. An example of such a fraud prevention service is Sift Science[16], which requires personal information or a user identifier, which would now be defined as personal information under the Report's proposed expanded definition, in order to protect and secure transactions and other customer interactions[17].
Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.	M	DIGI is supportive of this recommendation in principle, however our position on this recommendation is contingent on the definition of 'direct marketing'. If the definition of 'direct marketing' is confined to email, telephone or postal marketing from the APP entity or third party advertisers, we support empowering customers to opt out of communications from specific entities. This would complement the provision of unbundled consent requirements that enable consumers to opt out of email marketing when signing up for a service. However, should the definition be scoped more broadly so as to include on-site advertising, this may also require an APP entity to provide an ad-free version of their services which may not be technically possible, nor financially sustainable. DIGI has heard that this approach has not been successful in the EU. As with all of the recommendations related to Proposal 20, consideration needs to be provided to the economic ripple effects that these proposals will have on the broader array of small, large, public and private organisations that rely upon digital advertising. In this context, it is worth noting that the reforms to the UK GDPR propose to allow narrowly-defined direct marketing as a 'legitimate interest', which goes some way to recognise the centrality of marketing to business functions.

[15] This phrase is used in Virginia (VCDPA), Utah (UCPA), Colorado (CPA), Connecticut, and California (CCPA) laws.
[16] Sift Science, available at https://sift.com/
[17] Sift Science, "Tracking Anonymous User Activity", available at https://sift.com/resources/tutorials/anonymous-users

Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising.	N	DIGI members understand the need for consumers to be informed about the use of their data in general including for targeted advertising, and relevant members have comprehensive resources in place to inform and enable users to both better understand and manage the specific advertising that they see. However, building upon the analysis provided in relation to Proposal 20.1b) in relation to the expansive definition of 'targeting', DIGI is concerned that this proposal is predicated on an assumption that targeted advertising is not valuable to consumers and businesses alike -- an assumption that we urge the Government to rigorously analyse and challenge. Advertising financially sustains free digital services and the wide range of freely available content available to consumers. Furthermore, consumers benefit from targeted advertising as it enables a personalised experience and the discoverability of relevant goods and services often from small businesses. DIGI is concerned that the adoption of Proposal 20.4 would see consumers object to targeted advertising when asked in the abstract, in the same way that they might also express a preference for television without commercials, or newspapers without advertorials, or streets without billboards; a choice that is not afforded to them in these other mediums. We encourage the Government to further examine the evidence base in its case for this preliminary recommendation, and conduct further analysis on the benefits that targeted advertising provides Australian consumers. For example, the Interactive Advertising Bureau found in 2021 that there was an $8.8 billion value to the Australian community from access to free ad-supported digital services and content, a $10.2 billion value from consumption being more closely matched to consumer preferences, and $36.5 billion decreased transaction costs via reduced time and cost savings; totalling a $55.5 billion total annual consumer benefit in 2021 in Australia[18]. This recommendation will seriously hamper the ability for a wide range of advertisers to deliver relevant advertising to consumers. The long-term impacts of reducing the viability of ad-supported digital services also needs to be scoped in consultation with the media and advertising industry. For example, a wide range of creators use audience analytics on digital services and provide targeted advertising services to advertisers in order to optimise the performance and commercial viability of their services. The long term impact could also see otherwise free digital services moving toward a paid subscription model to ensure financial sustainability, which has implications for the long term health and diversity of Australia's media and creative sector. Additionally, there are potential competition and social impacts. The ACCC's Digital Platforms Inquiry report in 2019 acknowledged that 'digital platforms have provided a new advertising

[18] Interactive Advertising Bureau (IAB), (21/11/2022), *Ad'ing Value: Impact Of Digital Advertising On The Australian Economy & Society*, available at https://iabaustralia.com.au/resource/ading-value-impact-of-digital-advertising-on-the-australian-economy-society/#:~:text=The%20report%20also%20found%20that,was%20%2455.5bn%20in%202021

		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 network". (ACCC July 2019, Digital platforms Inquiry Final Report, p. 132). Competition concerns could arise from systematically reducing the effectiveness of digital advertising to reach relevant audiences that will limit or negate the ability of organisations to advertise their services, if they are not able to afford alternative traditional forms of advertising. This could have a particularly negative impact on non-profits and charities that use personalisation to overcome 'compassion fatigue' and match people to relevant social causes and fundraising initiatives[19].
Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information.	M	DIGI is supportive of mechanisms that provide consumers with more information about the third parties with which personal information will be shared, and the types of personal information that will be disclosed. However, building upon the concerns articulated in relation to the definition of trading in Proposal 20.1c), the definition of 'trading' is unclear, and not reflected in established international privacy norms. If 'trading' is intended to just cover the trading of lists for financial benefit, and not wider processing activities, then DIGI is supportive of this proposal in principle. As the current proposed definition of 'trading' includes a range of data processors, requiring consent for this data processing is impractical and not interoperable with GDPR whereby consent for all data processing is not required; rather, DIGI understands that data processing types need to be disclosed in privacy policies. Using the example cited earlier, it is not practical nor effective for consent to be sought for fraud prevention services. Fraud prevention should be assumed to be in line with customer expectation; enabling the opt-out of such services could also see nefarious activity. It is also worth noting that recent efforts to simplify the UK GDPR have proposed a list of activities that may be regarded as in a data controller's legitimate interest to process data that include direct marketing, intraorganisational transmission of data and network and information systems security; that is to say, these activities would not require consent under proposed UK law[20]. As noted elsewhere in this submission, Australia must consider the more practical models of advancing different legal bases, modelled upon the GDPR and UK GDPR.

[19] C Green, 'What the next generation of personalisation means for charity marketing', Charity Digital, 19 August 2020, available at https://charitydigital.org.uk/topics/topics/what-the-next-generation-of-personalisation-means-for-charity-marketing-7831

[20] International Association of Privacy Professionals (IAPP), *The Privacy Advisor*, (8/3/2023), "Top ten takeaways from the draft UK GDPR reform", available at https://iapp.org/news/a/top-ten-takeaways-from-the-draft-uk-gdpr-reform/

Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests.		DIGI agrees that the Privacy Act reform provides an opportunity to improve privacy protections for minors. Subject to our recommendations in relation to the definition of 'direct marketing', DIGI is supportive of this recommendation in principle. DIGI notes the use cases contemplated in the Report that a person under the age of 18 should be able to sign up for a mailing list to receive information about new products and services, and that they should not received unsolicited direct marketing from third-party businesses i.e. ensuring the entity has sought the consent of the minor to send direct marketing is extremely important. While DIGI agrees in principle that there should be an exception for direct marketing that is in the child's best interests, such as educational materials for example, OAIC guidance is required for APP entities to determine the best interests of the child. Our understanding of 'the best interests of the child' is that it concerns whatever is best for that individual child. In some instances it may be best to restrict a particular minor from a service, however in other instances it might be in the best interests of the child to have access to a digital service. Parents or guardians can make judgements on what's in the best interests of the child, not APP entities, because service providers rightly do not have that knowledge. More thinking needs to be done about how we apply this principle to children in a general sense in the digital world.
Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.	M	DIGI agrees that the Privacy Act reform provides an opportunity to improve privacy protections for minors and, as noted, we agree in principle on restrictions in relation to direct marketing to children. We are also supportive of the introduction of a code modelled on the UK Age Appropriate Design Code (AADC) and note that it focuses on 'harmful' 'profiling'; Standard 12 of the AADC states that 'profiling' should only be permissible, 'if you have appropriate measures in place to prevent the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing). As currently conceptualised, the definition of 'targeting' is far wider and DIGI is concerned that prohibiting targeting for children may expose children to age inappropriate content if targeting is prohibited. While we note the exception for 'targeting that is in the child's best interests', the conceptual difficulty for APP entities in interpreting this (noting our comments above in relation to Proposal 20.5) may not go far enough to ensure that children have an appropriate experience online. One approach may be to limit this prohibition to commercial content, such that it does not apply to non-commercial recommendations (e.g. for music and educational information). However, DIGI notes that even this approach would see a lack of parity in the online world with 'targeted' advertising to children in other mediums such as children's television. DIGI's relevant members have a range of tools to protect the experience of minors online; we would be supportive of an approach that provides further guidance in age-appropriate advertising and prohibitions through the recommendation in Proposal 16.5, rather than a blanket prohibition which may have adverse and unintended consequences.

Proposal 20.7 Prohibit trading in the personal information of children.	M	DIGI is supportive of the principle behind this recommendation that children's data should not be sold for commercial purposes, without consent of a guardian, and we consider that this should be explored in the context of recommendation 16.5. However, we reiterate our comments in relation to Proposal 20.1c) in relation to the definition and concept of 'trading', which is currently broadly scoped to include data processing functions, including in online safety, that will be used to protect children. However, if 'trading' is intended to just cover the trading of lists for commercial purposes, and not wider data processing activities or partnerships, then DIGI is supportive of this proposal in principle. For example, a prohibition on trading may restrict the use of third party content scanning software services designed to address and report child sexual exploitation material. The discussion of this proposal in the Report focuses on the profiling through the 'combining of data points from multiple sources'; this focus appears different to the broader definition of trading earlier in the report and risks confusing overlap with the definition of 'targeting' as noted above. As noted, definitions of 'trading' information do not exist in the GDPR and the UK GDPR, and we consider that this concept risks confusion with other forms of legitimate processing.
Proposal 20.8 Amend the Act to introduce the following requirements: (a) Targeting individuals should be fair and reasonable in the circumstances. (b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political association or membership of a trade union), should be prohibited, with an exception for socially beneficial content.	M	DIGI agrees that targeting of individuals should be fair and reasonable in the circumstances, and that a way to ensure this is by creating a 'fair and reasonable' legal basis, as previously discussed. In relation to Proposal 20.8, DIGI agrees that it is not always appropriate to target based on categories of information considered sensitive, and services should restrict discrimination on these grounds. However, as sensitive information includes attributes such as 'sexual orientation or practices' or 'philosophical beliefs', it is unclear how an APP entity would cater for users of their services proactively seeking information in these categories, such as information relating to sexual identity. Similarly, it is unclear how advertisers seeking to connect with these audiences with relevant information and services would be able to do so. While we appreciate the intent of this recommendation, extreme care must be taken as the result of such blanket restrictions can be the removal of content for different audiences that they would find relevant, and can have an impact on the inclusivity of digital spaces.

Proposal 20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.	Y	DIGI is supportive in principle of further information about targeting and recommendations being provided to users of services. For example, in DIGI's 2022 review of the Australian Code of Practice on Dis- and Misinformation, we added additional commitments reflecting updates to the strengthened EU Code of Practice in relation to recommender systems, and deterring advertisers from repeatedly placing digital advertisements that propagate mis- and disinformation[21]. DIGI considers that this information should be included in privacy policies for APP entities that use targeting. To the extent that this proposal is modelled on the EU DSA, we note that the proposal there is limited to a smaller set of services, and that the transparency obligations are not yet fully defined or implemented, and are outside the scope of data protection regulation.
21. Security, retention and destruction		
Proposal 21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.	Y	DIGI supports this recommendation in principle, and welcomes its harmonisation with the GDPR which requires that personal data must be processed securely using appropriate technical and organisational measures
Proposal 21.2 Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.	Y	DIGI broadly supports this recommendation, subject to further consultation on the proposed baseline privacy outcomes. DIGI welcomes the inclusion of cyber security measures within the APPs, and considers this a more effective approach to ensuring compliance across the wide range of entities subject to the APPs. There may be some confusion if there are duplicative processes or related efforts, such as the idea of a Cyber Security Act, which is contemplated in the Government's 2023-2030 Australian Cyber Security Strategy. Legislative approaches to private sector cyber security should be within the reformed Privacy Act and the Notifiable Data Breaches scheme (in addition to a range of other targeted measures as part of the wider strategy).
Proposal 21.3 Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.	Y	OAIC guidance is always welcome. However, there should be an acknowledgement that the measures may differ from service to service, and the detail of those measures may need to be confidential in order to ensure their ongoing effectiveness, and to prevent bad actors from circumventing security measures.

[21] DIGI (22/12/2022), [Media Release], *Digital industry strengthens misinformation code in response to community feedback*, available at https://digi.org.au/digital-industry-strengthens-misinformation-code-in-response-to-community-feedback/

Proposal 21.4 Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information.	Y	DIGI is supportive in principle of this proposal, provided that there is an acknowledgement under Proposal 21.3 that the reasonable steps may different for personal information and de-identified information. We also agree with the Report's assessment that 'that the level of protection afforded to de-identified information may be to a lower degree than personal information.'
Proposal 21.5 The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.	Y	DIGI is supportive in principle for this proposal, and for further OAIC guidance developed in consultation with industry.
Proposal 21.6 The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information. This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial. However, this review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 and the independent reviews and holistic reform of electronic surveillance legislative powers.	Y	DIGI is supportive of this proposal in principle, and agrees with the need for this review and the importance of data minimisation in relation to the mitigation of data breaches in particular.
Proposal 21.7 Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.	Y	DIGI is supportive of this recommendation in principle. Any documentation required from this proposal should be suitably proportionate for different types of APP entities.

Proposal 21.8 Amend APP 1.4 to stipulate that an APP entity's privacy policy must specify its personal information retention periods.	M	DIGI is supportive of Proposal 21.7, however we question the need for retention periods to be disclosed in public privacy policies, which is not a harmonised approach with GDPR or the UK GDPR. This may also require an entity to update its privacy policy, and notify users, each time its data retention policies under Proposal 21.7 change. This could counterintuitively serve as a deterrent for APP entities to regularly review their internal data retention policies by hinging this to an external privacy policy change.
22. Controllers and processors of personal information		
Proposal 22.1 Introduce the concepts of APP entity controllers and APP entity processors into the Act. Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.	Y	DIGI welcomes this proposal and strongly support the adopting of 'data controller' and 'data processor' designations to increase organisational accountability across complex digital supply chains, as well as interoperability with GDPR. An accountability-based approach enables organisations to adopt methods and practices that reach privacy protection goals by putting the customer at the centre of the business model, as is explicitly codified by Article 24 of the GDPR.
23. Overseas data flows		

Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.	Y	DIGI agrees that further consultation on the 'Australian link' test is needed. As the Report acknowledges, DIGI was one of many organisations that expressed concerns about the scope of extraterritoriality of the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. 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. 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 is concerned that these extraterritoriality provisions of the Bill exceed the provisions in the 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. 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. 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.
Proposal 23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).	Y	DIGI broadly supports this proposal in principle, assuming that these transfers would be similar to those facilitated through adequacy agreements under the GDPR.
Proposal 23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.	Y	DIGI broadly supports this proposal in principle, noting its alignment with GDPR.
Proposal 23.4 Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure.	Y	DIGI is likely to be supportive of this proposal in principle, however we find there is not a clear description of the proposal's intent or effect in the Report, and we would seek further information in order to advance a firm opinion.

Proposal 23.5 Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas.	Y	DIGI is supportive of this proposal in principle. We note that there is a qualifier of 'where practicable' in relation to recipient countries and we ask that this same qualifier be added in relation to the types of information.
Proposal 23.6 Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.	Y	DIGI is supportive of this proposal in principle. Provisions need to be added to ensure data can be passed intra-company, whereby the offices may be distinct legal entities; such sharing should not be considered to be 'outside the entity'.
24. CBPR and domestic certification (nil proposals) 25. Enforcement		
Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses: (a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision. (b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.	Y	DIGI broadly supports this proposal, and considers it sensible to have a tiered approach. However, we also consider that the effectiveness of such a scheme hinges on the definitional clarity of 'serious'. More broadly, we encourage the Government to avoid an approach that makes enforcement the single measure of success. The updated Act should also ensure that OAIC has a positive duty to aid compliance, through actionable guidance, and sectoral compliance efforts. There should also be an emphasis on consumer education to Australians so that they can better understand the value exchange in relation to data processing.
Proposal 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: (a) those involving 'sensitive information' or other information of a sensitive nature (b) those adversely affecting large groups of individuals (c) those impacting people experiencing vulnerability (d) repeated breaches	M	DIGI is concerned that this definition does not provide a clear threshold for APP entities. We understood that The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 added penalty provisions for 'serious' and 'repeated' infringements and, while we sought definitional clarity, the combination of these two elements provides a more appropriate threshold. For example, the expansive definitions of 'sensitive information' could see a breach involving one individual's political views considered to be a serious breach resulting in penalties of $50 million or 30 per cent of an entity's domestic turnover in the relevant period; we do not consider this to be the intent of this change. We instead suggest a focus on

(e) wilful misconduct, and (f) serious failures to take proper steps to protect personal data. The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.		egregious breaches of the Act (e.g. breaches involving deliberate or reckless conduct on the part of an APP entity)
Proposal 25.3 Amend the Act to apply the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers.	Y	DIGI is supportive in principle of such recommendations that increase the empowerment and resourcing of the OAIC.
Proposal 25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.	Y	DIGI is supportive in principle of such recommendations that increase the empowerment and resourcing of the OAIC.
Proposal 25.5 Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined: a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals. The OAIC should publish guidance on how entities could achieve this.	Y	DIGI is supportive in principle of guidance produced by the OAIC to identify, mitigate and redress loss and we recommend further industry consultation in relation to this guidance.
Proposal 25.6 Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established.	Y	DIGI is supportive in principle of this proposal. Care should be taken to avoid risk of overlapping or inconsistent orders.

Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.	M	DIGI agrees that the OAIC needs better resourcing. In exploring an industry funded model, attention must be given to the fact that the OAIC oversees an extremely broad set of organisations that span an extremely wide array of sectors, which may render an industry funding model unworkable. While the example of ASIC's industry funding is raised, DIGI posits that ASIC oversees a relatively more defined industry sector within financial services. 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 would posit that the privacy and safety investments made in this sector may exceed those in some high risk sectors that equally use personal information, but do not have as much experience nor the same levels of public scrutiny. While we believe the regulator should be well-resourced, cost-recovery may not be the best approach in this case as it could unintentionally incentivise enforcement actions.
Proposal 25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation.	Y	DIGI is supportive in principle of this proposal. While the Report highlights enforcement proceedings against well resourced entities, we consider that the enforcement strategy of the OAIC should be multi-pronged, examining a wide range of entities in order to encourage compliance and the expectation of enforcement economy-wide. The Government should avoid enforcement becoming the primary measure of success of privacy reform and ensure that the OAIC balances enforcement with other important work including aiding company compliance, engagement with data-driven sectors of the economy and consumer education.
Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.	Y	DIGI is supportive in principle of this proposal.
Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.	Y	DIGI is supportive in principle of this proposal. As noted, we recommend that enforcement does not become the primary measure of success and that this is balanced with other work. We consider that the enforcement strategy of the OAIC should be balanced with a broad set of statutory duties. For example, the UK GDPR reforms will require the ICO to have regard for the economic impact of its decisions and introduce new statutory duties to promote competition and innovation. OAIC governance should also be reviewed, to ensure continuity in the interpretation of privacy rules and accountability for its strategy and outcomes for the economy and society.
Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.	Y	DIGI is supportive in principle of this proposal. However, it is important that the OAIC exercises any oversight and investigatory powers in a consistent and predictable way that supports innovation and investment. We therefore recommend that consumers be required to avail of a company's internal complaints procedure before reporting a matter to the EDR scheme or the OAIC. This would enable quick resolution of non-complex complaints and

		ensure regulatory resources are focused on more complex cases or egregious breaches of privacy rules. OAIC guidance establishing clear rules and thresholds for initiating investigations would avoid the arbitrary selection of cases.
26. A direct right of action		
Proposal 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in this chapter.		DIGI is concerned with this proposal, and feel it is unnecessary where there is a well-understood and well-functioning system for user complaints outlined above. We expect that this direct right of action will largely be explored by people with the wealth and time to pursue court action, and this will not provide privacy protections to other Australians to the same extent as expanded privacy rights and organisational controls. DIGI is concerned that this will see a larger volume of claims proceed to the courts, and considers that such court processes remove agency from the OAIC, and we consider the regulator better suited to shape and balance the privacy interests of all individuals. Private rights of action may lead to inconsistent case law, resulting in legal uncertainty. By contrast, the OAIC is well placed to issue clear and consistent consumer-facing guidelines. We appreciate the changes in the Report, since the release of the Discussion Paper, to clarify that this right can only be exercised after a complaint has been through the OAIC or an external dispute resolution scheme. However, we are still concerned that the proposal does not go far enough to prevent spurious or frivolous claims, which could be addressed through the introduction of a serious harm threshold, as was recently added to the Model Defamation Provisions. A direct right of action could also inadvertently incentivise APP entities to produce highly legalistic disclaimers in privacy policies and notices. DIGI believes that strong privacy rights afforded elsewhere in the updated Act, such as the proposed consumer rights, organisation scope and the reconsideration of exemptions, will be more effective in encouraging widespread industry compliance than opening direct rights of action.
27. A statutory tort for serious invasions of privacy		
Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.	N	It is not clear from the Proposal whether this tort relates to invasions of privacy conducted by individuals using a particular APP entity, or by the APP entity itself. Greater clarity in this area would be helpful. We are concerned if the proposal holds APP entities liable for any invasions of privacy that people may be subjected to by other individuals online, this would have enormous implications for the wide variety of APP entities.

28. Notifiable data breaches scheme		
Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.	Y	DIGI is supportive in principle of proposals to strengthen the Notifiable Data Breaches Scheme, and considers this to be a key tool to draw upon learnings realised after the prominent data breaches of late 2022. Ensuring this scheme is up to date, rather than the creation of new frameworks as is contemplated in the Government's *2023-2030 Australian Cyber Security Strategy Discussion Paper*, will provide industry with greater clarity about its responsibilities toward affected users and the Australian Government when faced with a data breach or major cyber security incident.
Proposal 28.2 (a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. (b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable. (c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.	Y	Per our comments under 28.1, DIGI is supportive of this proposal in principle.
Proposal 28.3 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.	Y	Per our comments under 28.1, DIGI is supportive of this proposal in principle.

However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information.		
Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.		
Proposal 28.4 Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.	Y	Per our comments under 28.1, DIGI is supportive of this proposal in principle.
29. Interactions with other schemes		
Proposal 29.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.	Y	DIGI is supportive of this proposal in principle.
Proposal 29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.	Y	DIGI is supportive of this proposal in principle, and other cooperation mechanisms between regulators. DIGI notes that the Privacy Act Amendment amended 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. We understood that this provision was intended to facilitate better cooperation between the OAIC and ACMA. We assume the intent of this provision was that any concerns that the ACMA may find in its regulation of the communications and media sector can be referred to the OAIC, and 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. This would reflect the economy-wide relevance across all sectors of managing and not mishandling personal information. For example, 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. In order to reflect this data, and the economy-wide nature of data privacy concerns, there should be a comprehensive view of relevant enforcement and regulatory authorities and entities and co-operation mechanisms to address the mishandling of information[22]. Any cooperation between regulatory authorities on the interpretation and enforcement of privacy rules should be transparent and accountable to ensure predictability and certainty for APP entities.
Proposal 29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.	Y	DIGI is supportive of this recommendation in principle.
30. Further review		
Proposal 30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.	Y	DIGI is supportive of this recommendation in principle. Consideration should be given to whether a two-year review may provide more timely insights given the likely economic impact of these proposals.

[22] OAIC, *Notifiable data breaches publications*, available at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications