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

Monday January 31, 2022

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 Discussion Paper, released on October 25, 2021 (the Discussion Paper).

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

DIGI and its members share and support the Government's strong commitment to privacy. We believe that innovative pro-privacy practices are critical to the long term success of an Australian digitally-enabled economy.

DIGI's members believe that such practices go beyond merely providing privacy policies and notices, and extend to strong accountability-based practices and user controls. They continue to make extensive investments in the privacy of their users, including: having cross-functional privacy experts and teams who ensure that privacy is built into their products and services ('privacy by design'); providing information and tools to provide people with transparency, choices and control in relation to their personal data; and recognising their customers' rights to access, delete, correct and control personal data as part of global data protection frameworks including the Australian Privacy Act 1988, and the European Union's General Data Protection Regulation (GDPR).

DIGI fully supports modernising of the Privacy Act for a digital era, and sees the Privacy Act Review as a key opportunity to afford consumers choice, control and transparency while encouraging organisational accountability and best practice across the range of entities covered under the Act.

DIGI applauds the thorough and thoughtful approach to the Discussion Paper, and the extent to which it has meaningfully engaged with a variety of stakeholder views and proposed a range of proposals and options to reflect and balance these. In this submission, DIGI has provided a brief perspective on each of the proposals. In advance of that, we advance several high-level considerations that we encourage the Privacy Act Review team to consider.

Interoperability with the GDPR

DIGI supports interoperability between global privacy regimes in order to provide greater legal certainty to companies, and consistency of experience for consumers who regularly interact with services being offered outside of Australia. This both serves to promote innovation and engenders trust in a digitally enabled economy that increasingly relies on cross border trade that, either directly or indirectly, utilises

data that is sometimes personally identifiable. 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[1]. The GDPR, introduced on May 25, 2018, was a landmark legislation that has served as the new global standard for privacy legislation that thousands of companies with a global presence have implemented.

While we acknowledge and welcome the proposals that align with GDPR in the Discussion Paper, we consider there are many opportunities for closer alignment with the GDPR. In particular:

- DIGI supports the adopting of "data controller" and "data processor" designations to increase organisational accountability across complex digital supply chains, and recommend that such an approach be taken in the updated Privacy Act. 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. This approach offers advantages to individuals, organisations and regulators alike.
- We also support the six lawful bases for data processing data under GDPR's approach, and encourage adoption of this model for Australia.
- We believe that Discussion Paper's definitions of "personal information" and "consent" should use the GDPR's definitions.
- We believe that the Bill's proposals in relation to ceasing to use or disclose personal information upon request should be amended for consistency with the GDPR's right to object.

Any departures from GDPR should be explicitly justified in relation to what is specific to the Australian context that necessitates a different approach.

Standardising whole-of economy protections

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 have responsibilities in relation to that information.

While we have focused our comments in this submission on the Discussion Paper's proposals, we note the discussion questions posed in relation to whether exemptions to the Privacy Act should continue to be afforded to political parties, small business, and media organisations. To the extent that such services do use personal information in the marketing of their services and other promotional or commercial functions, DIGI believes in the need for a defined, whole-of-economy, set of privacy requirements that take into account proportionality and public interest.

DIGI has a particular interest in combating mis- and disinformation, having developed *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM) to realise Australian Government policy in this area. This code has been signed by eight major technology companies to provide Australians with safeguards in relation to mis- and disinformation on digital platforms. Addressing these challenges is a multi-stakeholder effort and, especially in light of the growing list of non-parliamentary parties, we share concerns raised by other stakeholders in relation to potential voter manipulation if the political party exemption is retained.

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.

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

As a result of that and their depth of technical expertise with data governance, we would posit that the privacy, safety and cyber security investments made in this sector may exceed those in other high risk sectors that equally use personal information, but do not have as much experience nor the same levels of public scrutiny.

DIGI sees an important opportunity for system-wide improvements through the Privacy Act Review, and caution against a sectoral "patchwork" approach that affords consumers with protections around their information in some sectors but not others.

Data minimisation

DIGI welcomes the fact that the universally accepted privacy best practice of data minimisation forms part of the existing APPs under the Privacy Act 1988 (Cth)[2]. As you would be well aware, data minimisation requires goods or service providers to not seek to collect data beyond what is reasonably needed to provide the good or service, or to employ adequate measures to anonymise data using proven techniques such as differential privacy. We believe that privacy risks – such as inappropriate use or disclosure or poor security – can be reduced or avoided altogether by adopting a data minimisation approach. Data minimisation is also a key principle of the Consumer Data Right (CDR)[3].

We observed that the principle of data minimisation was not specifically discussed in the Discussion Paper, and we urge the retaining of and refreshing this principle in the reformed Act from a protective viewpoint. DIGI believes that encouraging data minimisation engenders more trust in innovative digitally enabled services, and it should be a core privacy principle.

DIGI is concerned that the proposals for parental consent in the Discussion Paper and related provisions around age verification contained within the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 run counter to the principle of data minimisation. We are concerned that these well-intentioned efforts will see Australians sacrifice their privacy as part of efforts to protect it, by providing services with more information to verify age and guardianship. Similarly, DIGI is concerned that the Social Media (Anti-Trolling) Bill 2021 encourages a wide variety of entities to collect verified personal information from users in order to have access to a safe-harbour defence. DIGI encourages the Privacy Act Review team to consult DIGI's submissions on these two bills, separately provided to the Attorney General's Department.

Whole of Government approach

DIGI welcomes a whole-of-Government approach to this Privacy Act Review reform process. We acknowledge the thoughtfulness with which the review team considered the overlap between the review's scope and the CDR in relation to data portability. **We encourage further examination of other Government reform processes, and an analysis of where the Discussion Paper's proposals may help or hinder goals in other arms of Government.**

For example:

---

[2] OAIC, *Australian Privacy Principles*, available at: https://www.oaic.gov.au/privacy/australian-privacy-principles, aee APP 3 and APP 11.
[3] OAIC, *Chapter 3: Privacy Safeguard 3 — Seeking to collect CDR data from CDR participants*, available at: https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-3-privacy-safeguard-3-seeking-to-collect-cdr-data-from-cdr-participants/

- The Department of Prime Minister & Cabinet (PM&C) is leading the development of the Australian Data Strategy, which encourages more data-driven innovation across the public and private sectors, fuelled by data analytics.
- The Government has made a $120 million investment in its "Deregulation Agenda", overseen by PM&C[4] which included an update to the Regulator Performance Guide which states that "Best practice requires that regulators consider, and aim to improve on, the combined regulatory burden of governments on business and the community.[5]"
- The Government has made $124.1 million investment under the Artificial Intelligence (AI) Action Plan, overseen by the Department of Industry, Science, Energy and Resources, which sets out a vision for Australia to become a global leader in developing and adopting AI[6].
- The AI Action Plan is part of the Government's wider Digital Economy Strategy that aims to make Australia a leading digital economy by 2030[7], led by PM&C.

As Australia develops a roadmap to meet its goal of becoming a leading digital economy by 2030, we need to be acutely aware that we are starting this race at the back of the pack with the second smallest technology sector in the OECD[8]. While the incentives under the Government's Digital Economy Strategy are extremely important, we need a Whole-of Government approach to this goal that pulls levers that maximise the business opportunities in creating and expanding technology companies in Australia, minimise their risk, and optimise global interoperability of regulatory settings. **We encourage the Privacy Act Review team to undertake further consultation with PM&C and other relevant Departments and stakeholders to ensure the Privacy Act Review supports these Government strategies.**

We hope that the Privacy Act Review team can closely consider DIGI's specific recommendations enclosed in the remainder of this submission, along with the overarching principles DIGI has highlighted in this opening letter. We thank you for your engagement with stakeholders to date and look forward to continuing to engage with you on this important process to modernise 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

---

[4] Department of the Prime Minister and Cabinet (20/04/2021), *Deregulation agenda removing business red tape and lifting regulator performance*, available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F7917440%22;src1=sm1

[5] Department of the Prime Minister and Cabinet (01/07/2021), *Regulator Performance Guide and supporting material*, available at https://deregulation.pmc.gov.au/priorities/regulator-best-practice-and-performance/regulator-performance-guide

[6] Department of Industry, Science, Energy and Resources, *Australia's Artificial Intelligence Action Plan*, available at: https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan

[7] Department of the Prime Minister and Cabinet, *Department of Digital Economy Strategy*, available at https://digitaleconomy.pmc.gov.au/

[8] AlphaBeta (September 2019), *Australia's Digital Opportunity*, available at https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf

Table of contents

DIGI's input on the Discussion Paper's specific proposals

Proposal	Support (Yes/No/ Maybe)	DIGI's input
1. Objects of the Act		
1.1. Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows: a) to promote the protection of the privacy of individuals with regard to their personal information, and b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities undertaken in the public interest.	Y	DIGI supports this proposal insofar as it establishes the basis for a provision akin to the "legitimate interest" legal basis under the GDPR. Legitimate interests is one of the six lawful bases for processing personal data, and enables organisations to weigh considerations of public interest[9]. DIGI encourages the Privacy Act Review team to enact an equivalent legal basis.
2. Definition of personal information		This section raises questions in relation to the inclusion of technical data in the definition of personal information. IP addresses and device identifiers are collected by websites for basic and essential functions and usually cannot be used to identify an individual (unless the website happens to be owned by a device manufacturer or an ISP). Almost every website requires the collection of this essential information to meet basic consumer expectations in relation to the services they access, and the services cannot be provided without such processing. For example, an IP address often ensures that a website is simply displayed in the correct language. As a result, we do not think that this technical data should be classified as personal data unless it is used, or combined with other data, to identify an individual. The GDPR makes clear that technical data is only personal information if it can be used to indirectly identify an individual when combined with other data available to the data controller.
2.1. Replace the word "about" with "relates to".	Y	We support aligning the definition of "personal information" under the

[9] Information Commissioner's Office, *What is the 'legitimate interests' basis?*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

			Privacy Act to the GDPR definition of “personal data”, and encourage the review team to adopt it in full. Article 4 of the GDPR defines personal information as follows: “‘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.”
2.2.	Include a non exhaustive list of examples of types of information covered.	Y	Examples are helpful for companies to easily operationalise the amended definition. A list of types of information that are not covered by the definition would also be valuable.
2.3.	Define "reasonably identifiable" as circumstances where an individual can be directly or indirectly identified.	Y	This change appears to increase interoperability with the GDPR’s definition of personal information (above). Consistent with that definition, we would caution against the inclusion of public or other sources of data that do not relate to a specific individual or device. The updated Act should serve to encourage the use of less identified data wherever possible.
2.4.	Amend definition of "collection" to include data collected from any source through any means including inferred or generated.	M	While the Discussion Paper 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". Therefore 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 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. However, DIGI supports the intent behind this proposal. To achieve that intent, DIGI supports users being able to exercise privacy rights to access or erase information inferred about themselves from providers. We also believe the intent can be served by Option 1 in Section 11 on restricted and prohibited practices. Other areas of the updated Act can address potential concerns about the risk and transparency of inferred data, whereas expanding the definition will create confusion as to what falls under collection.
2.5. Require that personal information be anonymous before it is excluded from the Act.	Y	DIGI broadly supports this proposal. It is worth noting that certain proposed obligations cannot apply to pseudonymous data, such as rights to access, object or erase. We believe 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. This would align with Australia's Data Strategy that is encouraging further use of data analytics economy-wide.
2.6. Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments	Y	DIGI understands that this Bill amends the Privacy Act to introduce provisions which prohibit conduct related to the re-identification of de-identified personal information published or released by Commonwealth entities. DIGI supports this proposal.
3. Flexibility of the APPs		
3.1. Amend the Act to allow the IC to make an APP code on the direction or approval of the Attorney General: where it is in the public interest to do so without first having to seek an industry code developer, and where there is unlikely to be an appropriate industry representative to develop the code.	M	We believe the suitability of this recommendation applies in "emergency" situations, and that such situations should be clearly defined. However, DIGI believes the condition of "where in the public interest" is too broad and open to interpretation (as detailed below in relation to

		proposal 3.2). 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 is 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 coordinate 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 scope and approach of codes is publicly released by the Information Commissioner.

3.2.	On direction from the Attorney General, allow the Commissioner to develop / impose an APP code without first requesting industry to develop in cases of emergency or where in the public interest	M	As noted, we believe the suitability of this proposal in "emergency" situations, if clearly defined, but believe the condition of "where in the public interest" is too broad and open to interpretation. DIGI's concerns arise from a need to provide industry associations and industry participants clarity about code development processes in which they participate. We note when the draft Online Safety Bill was being progressed through parliament in February 2021, DIGI and several industry associations were concerned that the Bill afforded the eSafety Commissioner with the power to enact industry standards at any time, while a industry-led code development process was underway. We were concerned that this provision created uncertainty for industry associations leading the code development, and industry participants, working in good faith and with substantial time and cost investment to develop a code, as the rug could be pulled out from under them at any time if a standard were to be introduced that prevailed over the code. We were pleased that this concern was addressed in parliament, and that the final Online Safety Act requires the eSafety Commissioner to make "reasonable efforts" to ensure industry can develop codes before replacing them with standards. DIGI is currently leading the development of several chapters of these codes, and appreciates this clarity of process. We see similar concerns with this proposal, where the discretion of the Attorney General that a matter is in "the public interest" may see code development processes overturned without notice in favour of codes developed by the Privacy Commissioner.
3.3.	Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to: entities, or classes of entity; classes of personal information, and acts and practices, or types of acts and practices.	Y	DIGI broadly supports this proposal. A clear definition of "emergency" is required.
3.4.	Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.	Y	DIGI broadly supports this proposal, as long as clear safeguards exist for the receiving state and territory authorities such that the personal information shared is used for the purpose of managing the emergency

		in question.
4. Small business exemption 5. Employee records exemption 6. Political exemption 7. Journalism exemption		DIGI notes there are no specific proposals advanced in this section. In general, 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 such services do 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. DIGI has a particular interest in combating mis- and disinformation, having developed *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM) to realise Australian Government policy in this area. This code has been signed by eight major technology companies to provide Australians with safeguards in relation to mis- and disinformation on digital platforms. Addressing these challenges is a multi-stakeholder effort and, especially in light of the growing list of non-parliamentary parties, we share concerns raised by other stakeholders in relation to potential voter manipulation if the political party exemption is retained.
8. Notices of collection of personal information		
8.1. Express requirement in APP5 that notices must be clear, current and understandable.	Y	DIGI broadly supports this proposal. We caution against an over-reliance on consent mechanisms could contribute to "notice 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.

8.2.	Notices under APP5 limited to: - entity identity and contact details - types of information collected - purpose for collection and use - types of third parties that may need access - if collection was carried out by a third party, who that third party is and circumstances around collection - the fact that the individual may complain, or lodge a request (access, correction, objection or erasure) - location of privacy policy that sets out further information.	Y	DIGI broadly supports this proposal. We do note that not all data processing can accurately be summarised in a manner that is not misleading or obstructive; we therefore agree with the stakeholder perspective included in the Discussion Paper that the provision of a hyperlink to where individuals may choose to find privacy information should satisfy the obligation where appropriate, and that this should be made more explicit.
8.3.	Standardised notices can be considered under an APP code (or indeed the online privacy code) using commonly agreed icons, layout, wording.	M	DIGI agrees with the view put forward in the discussion paper that "Due to the wide range of contexts in which the Act applies, it is likely to be impractical to develop privacy notice templates, lexicon or icons that could be standardised across all APP entities". 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 industry, under the Online Safety Act, the digital 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 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 whereby 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.
8.4. Require notification at or before time of collection (or as soon as possible after collection if that is not possible) unless this is impossible or involves disproportionate effort.	Y	DIGI broadly supports this proposal.
9. Consent to the collection, use and disclosure of personal information		The Privacy Act is currently based on the principle of obtaining user agreement with notice in a limited set of cases; we believe this should continue with a GDPR-style approach where consent is one of several legal bases for data processing. In general, DIGI recommends that any changes to the current regulatory settings should focus less on strengthening consent requirements and more on incentivising regulated entities to be better caretakers of data through organisational accountability and affording consumers with choices. An approach to data protection which is entirely based on a consent-notice approach is problematic as it places a burden on consumers to read and understand privacy notices and then act. Consumers regularly report experiencing “consent fatigue” in relation to an excessive number of consents. Consent is also hard to obtain, particularly when there is no user interface, such as with IoT devices; the approach DIGI recommends is more future-proof as technology evolves.

9.1.	Defined as voluntary, informed, current, specific and unambiguous through clear action.	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 a standard unless consent is continually being resought, which would result in considerable notice 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.
9.2.	Standardised consent flows can be considered under an APP code (or indeed the online privacy code) using commonly agreed icons, layout, wording or taxonomies.	M	As noted in relation to notices, DIGI questions the relevance of standardised consent flows across the digital industry should this sector be the subject of an APP code. To illustrate the diversity of the sector, under the Online Safety Act, the digital 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 further risk that standardised notices or icons may

			oversimplify the communication of different data practices. We suggest this proposal be rephrased whereby the OAIC may consider guidance of recommendations in relation to consent, but wording and iconography should be tailored to the users of the service and the data collection to which the consent relates.
10.	Additional protections for collection, use and disclosure of personal information		
10.1.	A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.	Y	DIGI broadly supports this proposal. We encourage as much interoperability with the final provision and the inclusion of a "legitimate interests" legal basis under the GDPR. A model may be to retain the "legitimate interests" wording along with guidance akin to the legitimate interests balancing test.
10.2.	Collection, use or disclosure under APP3 or APP6 must be fair and reasonable and legislated factors to consider could include; - whether an individual would reasonably expect their information to be collected, used or disclosed under the circumstances - the sensitivity and volume of information being collected, used or disclosed - whether there is a foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure - whether the collection, use or disclosure is reasonably necessary to achieve the functions and activity of the entity - whether loss of privacy is proportionate to the benefits received - transparency of the collection, use or disclosure - if information relates to a child, whether the collection, use or disclosure is in the best interests of the child.	Y	DIGI broadly supports this proposal. We agree that specific privacy protections for minors should be expanded upon within the Privacy Act. Our understanding “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 platforms, 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. The UK’s Age Appropriate Design Code gives some thought to this, and we do see that as a useful model.
10.3.	New requirement in APP3.6 where if the entity does not collect the information directly from the individual, take reasonable steps to satisfy themselves that the collection was in accordance with APP3.	Y	DIGI broadly supports this proposal.
10.4.	Define 'primary purpose' as purpose for the original collection and 'secondary purpose' as directly related to, and needed to	M	DIGI questions whether this approach is interoperable with GDPR. In particular, we caution that the definition for secondary purpose

support, the primary purpose.		advanced in the discussion paper may be too narrow. For example, a secondary purpose might entail fraud protection or ensuring the security of the data through providing data visibility to a security partner; a user may not consider this related to the primary purpose. DIGI believes that the approach under the GDPR, whereby there are six lawful bases for data processing (consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest) is a more effective approach, and is more transparent to a user about how their data may be used. We also believe that the GDPR's concepts of "data controllers" and "data processors" may complement the intent of this proposal, as many of the functions undertaken by data processors may correspond with "secondary purposes".
11. Restricted and prohibited practices		
Option 1: entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate the risks; - direct marketing (including online targeted advertising on a large scale) - collection, use or disclosure of sensitive information on a large scale - collection, use or disclosure of children's personal information on a large scale - collection, use or disclosure of location data on a large scale - collection, use or disclosure of biometric or genetic data, including the use of facial recognition software - sale of personal information on a large scale - collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale - collection, use or disclosure of personal information for the purposes of automated decision making with legal or significant effects - any collection, use or disclosure that is likely to result in high privacy risk or risk of harm to an individual	Y	DIGI strongly supports this proposal, and sees this as an important consumer protection against privacy risks.
Option 2: increase an individual's capacity to self manage their privacy in relation to the above restricted practices. Examples include through consent (expanding the definition of sensitive information), granting absolute opt out rights for	N	DIGI prefers option 1, as it puts the onus on companies to proactively address potential consumer consumer concerns, rather than placing the onus completely on consumers to manage their own privacy risks.

restricted practices, or by mandating explicit notices for restricted practices.		We believe a focus on organisational accountability measures should be complemented by self-management measures to afford consumers with broader rights to erasure, or the right of access. Some services will not be able to enable consumers to withdraw consent for certain practices while continuing to offer the core service; for example, a consumer would be unlikely to be able to use a navigation service if they withdrew their consent for the collection, use or disclosure of location data. Similarly, a service powered by advertising may not be able to offer the service without advertising for technical or budgetary reasons.
12. Pro-privacy default settings		
Option 1: pro privacy settings enabled by default (particularly relevant for multiple settings)	N	While DIGI's members offer pro-privacy default settings in relation to aspects of their services, particularly in services used by minors, we favour a variation of Option 2 as an approach that may be more applicable to the broad array of APP entities. The discussion paper entertains the idea of enacting default privacy settings in the Basic Online Safety Expectations (BOSE) instrument under the Online Safety Act. We caution against this approach because of the confusion of having privacy requirements in safety legislation (though note well the connection between these issues) and because of the extremely broad scope of the BOSE that applies to every website in Australia, every messaging service and every service that enables interactions between two or more end users. Default privacy settings across such a wide array of services may not be in line with all consumers' expectations of those many services. It also makes assumptions about users and what they want from their online experience. We note that the findings of a 2020 OAIC survey indicated that most Australians (58%) agree it is fair that they share some information if they want to use a digital service and, if they have to receive any ads, they would prefer that they are targeted (48%). Further, the level of comfort with targeted advertising varies widely across

		different demographics[10]. DIGI believes that the final recommendation needs to accommodate these varying preferences in a wide array of areas, and that a modified version of Option 2 achieves this more effectively.
Option 2: Provide an obvious and clear mechanism to set all privacy controls to most restrictive (e.g. through a single click)	M	DIGI favours this option, though would modify it in favour of a proposal to have consumers nominate their privacy settings at the point of account creation and renewal. This approach is less presumptive that the most restrictive is the most optimal state for all users.
13. Children and vulnerable adults		
13.1. Amend Act to require parental consent for children aged under 16 by either (a) consent before collection, use or disclosure, or (b) consent before sensitive information is collected or as a mechanism for secondary use or disclosure of personal information	N	The Act does not contain any express requirements regarding children's privacy as it affords protections to all Australians regardless of age. We appreciate that minors are a vulnerable group and that additional protections should be considered to account for this vulnerability. As stated above, we support other proposals in relation to this endeavour, in relation to the restricted practices and additional protections which both cover minors. However, we echo concerns detailed in our submission on the Online Privacy Bill, separately provided to the Attorney General's Department, with regard to age and guardian verification. In brief, obtaining verified parental consent may require the collection of secondary documents to verify parental status or guardianship. For example, there are many parents or guardians who do not have the same last name as their children. This may be because their children have the last name of their spouse, due to adoption, or for legal guardians who are not biological parents. Is the Government expecting parents to provide a birth certificate, Medicare card or other identification in order to demonstrate their guardianship of a particular minor? This would increase the amassing of personal identification documents at the platform level, and runs counter to the principle of data minimisation that is covered

[10] OAIC, *Australian Community Attitudes to Privacy Survey 2020*, available at https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey, p32-33

		under the existing APPs. This also overlooks scenarios where a young adult may require access to digital services outside of the purview of their legal guardian, such as to access assistance or health information. This is particularly relevant in situations where the minor's relationship with their guardian may be constrained. This is one of several concerns identified in the UNICEF Discussion Paper in relation to the CRC's Article 2 concerning non-discrimination, where it states: *It is important that age assurance processes do not inadvertently discriminate against children who do not have access to official documents, children with developmental delays, children whose ethnicity is not recognized by algorithms used to assess age, or children who do not have parents or caregivers who are able to engage with verification processes that require parental input.* The UNICEF discussion paper also discusses Article 5 of the CRC, which focuses on parental guidance and a child's evolving capabilities where it states: "It may be difficult to reconcile age-based restrictions with the concept of the evolving capacities of the child." Consideration needs to be given to the varying impact of the Bill on young adults, not just children[11].
13.2. Require APP5 notices to be clear, current and understandable particularly for information addressed to a child.	Y	DIGI broadly supports this proposal. We echo the same challenges raised in previous recommendations about the inclusion of "current" in relation to the logistical questions it poses, and interoperability with GDPR.
14. Right to object and portability		
14.1. An individual may object or withdraw consent to the collection, use or disclosure of their information at any time. Entities must	M	DIGI supports the right to erasure under the GDPR, which applies to many of our relevant members. As noted, we support interoperability

[11] UNICEF, (2021), *Digital Age Assurance, Age Verification Tools, and Children's Rights Online across the Globe: A Discussion Paper*, available at https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf

take reasonable steps to stop collecting, using or disclosing their information and must inform the individual of the "consequences of their objection".		between Australia's updated privacy regulation with the GDPR and propose that this proposal be amended for consistency with the GDPR. As currently drafted, the right to object would extend beyond comparable requirements under the GDPR, where a right to object is only available for data processed on the grounds of legitimate interests or public interest. For example, it is not clear whether the proposal would apply to information collected from end-users through consent. Without further clarity, this is a possible interpretation of the Bill. In the development of a right to object, it will be important to ensure it does not impede advertising-supported business models. Guidance needs to be provided to entities that may not be able to provide an advertising-free version of their services for technical or budgetary reasons.
15. Right to erasure of personal information		
15.1. Erasure can be requested in the following instances; - personal information must be destroyed or de-identified under APP11.2 - personal information is sensitive information - an individual has mounted a successful objection through the right to object - personal information has been collected, used or disclosed unlawfully - the entity is required to destroy the information (by a court or by law) - personal information relates to a child and the erasure is requested by the child or their parent / guardian	Y	DIGI broadly supports 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. 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. In response to the Discussion Paper's question about how to address freedom of speech and practical difficulties for industry, 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, and the Social Media Anti-Trolling Bill (ATB). The ATB requires the collection of contact information as part of a safe harbour for digital platforms, and raises questions as to the scenarios where the user in question has exercised

			their right to erasure. Additionally, consideration needs to be given 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 be given to whether an independent adjudicator can determine when objectionable content pertaining to an identified individual should be erased from the Internet.
15.2.	An entity could refuse to erase on the basis of an exception to all or part of the information	Y	DIGI supports this portion of the proposal.
15.3.	An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.	Y	DIGI supports this portion of the proposal.
16.	Direct marketing, targeted advertising or profiling		
16.1.	The right to object includes an unqualified right to object to any collection, use or disclosure of information for the purposes of direct marketing (and targeted advertising or profiling?). Individuals could also simply request not to receive direct marketing. Direct marketing must include a notification of the right to object.	M	DIGI raises the same concerns as above in relation to the right to object and its compatibility with GDPR, and its implementation on ad-supported platforms. DIGI notes that its relevant members allow users to opt out of targeted advertising, but to offer an ad free version of a range of websites may not always be technically and feasibly possible in all cases.
16.2.	The use, collection or disclosure of personal information for the purposes of influencing behaviour or decisions must be a primary purpose notified to the individual when their information is collected.	M	There is ambiguity about the situations in which this notice would have to be served because of the breadth of including the three concepts of "use, collection or disclosure". We suggest the definitional circumstances be narrowed to avoid notice fatigue.

16.3.	Include the following in the privacy policy: - whether the entity is likely to use, alone or in combination with other information, information for the purpose of influencing behaviour or decisions and the types of information that will be used, generated or inferred - whether the entity uses third parties in the provision of marketing materials (and if so, the details of these third parties and how to opt out).	Y	DIGI supports the portion of this proposal relating to additional disclosures in privacy policies.
16.4.	Repeal existing APP7 (which relates to direct marketing).	Y	DIGI broadly supports modernising this provision in line with GDPR, and taking into consideration our comments in relation to related recommendations advanced elsewhere in this submission.
17.	Automated decision making		
17.1.	Require privacy policies to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on people's rights.	Y	DIGI broadly supports this proposal.
18.	Accessing and correcting personal information		
18.1.	An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.	Y	DIGI broadly supports this proposal.
18.2.	Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information: the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.	Y	DIGI broadly supports this proposal.
18.3.	Clarify the existing access request process in APP 12 to the effect that: ● an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access	Y	DIGI broadly supports this proposal.

	request would require the provision of personal information that is highly technical or voluminous in nature, and • where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.		
19.	Security and destruction of personal information		
19.1.	Amend APP11.1 to state that reasonable steps includes technical and organisational measures	Y	DIGI broadly supports this proposal.
19.2.	Include a list of factors that would be considered 'reasonable steps'	Y	DIGI broadly supports this proposal.
19.3.	Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.	Y	DIGI broadly supports this proposal.
20.	Organisational accountability		
20.1.	Amend APP6 to expressly require entities to determine, at or before using information for a secondary purpose, each of the secondary purposes for which the information will be used or disclosed and record those purposes	M	DIGI restates the concerns made above in relation to the proposal to differentiate between primary and secondary uses of data.
20.2.	Introduce further organisational accountability requirements into the Privacy Act, targeting measures to where there is the greatest privacy risk.	M	DIGI supports organisational accountability measures in principle, and efforts to remove the privacy burden from consumers. However, as currently proposed, this proposal lacks detail. Care will need to be taken to ensure the measures are proportionate for businesses of different sizes.

20.3.	Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.	M	DIGI supports internal recording keeping about the disclosure of data for secondary purposes, and placing a summary on public record in Privacy Policies. As explained below, we believe connecting or replacing the primary and secondary purpose concepts with the GDPR's concepts of "data controllers" and "data processors" is a more effective approach.
21.	Controllers and processors		DIGI notes there are no specific proposals advanced in this section. DIGI strongly supports the differentiation between "data controllers" and "data processors" which we consider provides proportionate and clear organisational responsibilities across complex digital supply chains, and recommend that such an approach be taken in the updated Privacy Act.
22.	Overseas data flows		
22.1.	Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).	Y	DIGI broadly supports this proposal, noting that these transfers would be similar to those facilitated through adequacy agreements under the GDPR.
22.2.	Make standard contractual clauses for overseas transfers available to entities	Y	DIGI broadly supports this proposal, noting its alignment with GDPR.
22.3.	Remove the informed consent exception in APP8.2B (exemption to comply where consent is given to overseas transfer)	M	DIGI is not well informed enough about this exception to advance an informed view.
22.4.	Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.	M	Given the global nature of a variety of data processors that APP entities may work with, and the high potential for changes in their global footprint, DIGI questions whether disclosures about countries where data may be shared can ever be comprehensive, and whether they would meaningfully inform consumer choices. DIGI posits that other protections, including protections aimed at ensuring cyber security in line with GDPR, will address perceived consumer risks with data transfer overseas.
22.5.	Introduce a definition of 'disclosure' consistent with that contained within the APP Guidelines (making personal information accessible to others outside the entity and releasing the subsequent handling of the information from its effective control)	Y	DIGI supports this proposal. 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".

22.6.	Amend the Act to clarify relevant circumstances for determining what 'reasonable steps' are (APP8.1)	Y	DIGI believes this clarification may be helpful. However we caution against over-complicating the process of overseas data transfer given this is common for multinational companies through intra-company transfers, and given the global nature of a variety of data processors that APP entities may work with, and the high potential for changes in their global footprint. DIGI questions whether disclosures about countries where data may be shared can ever be comprehensive, and whether they would meaningfully inform consumer choices. As mentioned, DIGI posits that the cyber security and other protections will address perceived consumer risks with data transfer overseas.
23.	CBPR and domestic certification		
23.1.	Continue to progress implementation of CBPR	Y	DIGI supports this proposal. Many DIGI members already participate in third party verification schemes that promote organisational accountability and compliance, such as APEC CBPR.
23.2.	Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside, CBPR	Y	DIGI supports this proposal as it is necessary for CBPR implementation.
24.	Enforcement		
24.1.	Create tiers of civil penalty provisions to allow more flexibility in determining fines; including a series of low level breaches of specific APPs with an attached infringement notice regime and a mid tier offense for interference with privacy	Y	DIGI broadly supports this proposal, and considers it sensible to have a tiered approach.
24.2.	Clarify what constitutes a repeat or serious interference with privacy	Y	DIGI believes such clarification would be helpful, and encourages further consultation on this guidance.

24.3.	The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.	Y	While DIGI broadly supports this proposal, as it increases public confidence in the regulator, we believe that the consumer interest is best served by targeted audits in response to a proven breach of data protection law and measurable consumer harm. We note that many European Data Protection Agencies appear to be moving away from periodic routine audits, as this has proven to be too resource and time-intensive and not scalable in the long-term[12].
24.4.	Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.	Y	DIGI broadly supports this proposal, as it Increases public confidence in regulator.
24.5.	Amend para 52(1)(b)(ii) and 52(1A)(c) to require an entity to "identify, mitigate and redress actual or reasonably foreseeable loss"	Y	DIGI broadly supports this proposal.
24.6.	Give Federal Court the power to issue an order after a section 13G penalty provision has been established	M	DIGI has not had the opportunity to further explore this proposal to advance an informed view.
24.7.	Introduce an industry funding model incorporating two levies; 1 - Cost recovery levy (to fund guidance, advice and assessments) 2 - Statutory levy (to fund investigation and prosecution of entities operating in a high risk environment)	N	DIGI is concerned that this proposal lacks a meaningful precedent. While the example of ASIC's industry funding is raised, DIGI posits that ASIC oversees a relatively more defined industry sector within financial services. By contrast, the OAIC oversees a far broader set of organisations within the APP entities, that span an extremely wide array of sectors. DIGI is concerned by the proposal advanced in the discussion paper where it states: "A narrower group of entities which operate in a high privacy risk environment could also contribute a statutory levy to support the OAIC's management of public inquiries and investigation into their acts or practices (i.e. entities that collect, use or disclose significant amounts of personal information or engage in sophisticated information handling practices). This may include social media platforms and entities which trade in personal information such as digital marketing businesses."

[12]: Data Protection Commissioner, *Final Report of the Data Protection Commissioner of Ireland | 1 January – 24 May 2018*, available at https://www.dataprotection.ie/sites/default/files/uploads/2018-11/DPC%20annual%20Report%202018_0.pdf, p. 25.

			This statement assumes that sectors such as social media carry the highest privacy risks, and we do not believe this has been established through evidence. 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. Note that the Deloitte Privacy Index 2018 observed that digital companies provide greater transparency for their users than non-digital companies[13]. 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.
24.8.	Amend annual reporting obligations for the Commissioner to include outcomes of all complaints lodged (including number of dismissals)	Y	DIGI broadly supports this proposal, and initiatives that encourage greater transparency for Australian regulators.
24.9.	Alternative regulatory models •**Option 1** - Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them. •**Option 2** - Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes. •**Option 3** - Establish a Deputy Information Commissioner – Enforcement within the OAIC.	M	Of the options, DIGI supports Option 3 but notes that the OAIC already has a complaint handling division. We are interested to understand the reason(s) for introducing new regulatory models and remain concerned that external schemes may lack due expertise in privacy.
25.	Direct right of action		

[13] Deloitte, *Deloitte Australian Privacy Index 2018*, available at https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html

25.1.	Create a direct right of action with the following design elements: •The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity. •The action would be heard by the Federal Court or the Federal Circuit Court. The claimant would first need to make a complaint to the OAIC (or FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman. •The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application. •The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.	N	DIGI is concerned with this proposal. We note that this right can only be exercised *after* a complaint has been through the OAIC or an external dispute resolution scheme. However, a complainant can choose not to proceed to conciliation and launch a direct action; we therefore suggest that this is changed so that a complainant must go through conciliation process in good faith and that direct action can only be brought if conciliation fails or OAIC determines that the matter is not appropriate for conciliation. In addition, in order to prevent spurious or frivolous claims, DIGI suggests the introduction of a serious harm threshold, as was recently added to the Model Defamation Provisions. 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. 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, when well promoted, may mitigate the need for this direct right of action.
26. Statutory tort of privacy			
26.1.	**Option 1**: introduce a tort for invasion of privacy (as recommended by the Law Reform Commission Report 123)	N	It is not clear from the Discussion Paper 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
26.2.	**Option 2**: introduce a minimalist tort recognising the existence of	N	The benefits of a court driven process, as opposed to a common law

	a cause of action but leaves scope and application to be developed by courts		approach, are not apparent. As the Discussion Paper points out, this approach would rely on cases coming before the courts and may therefore involve long periods of uncertainty as the law develops.
26.3.	**Option 3**: do not introduce a tort but common law to continue to develop through judicial determinations	Y	DIGI supports Option 3.
26.4.	**Option 4**: In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.	N	DIGI supports Option 3.
27.	Notifiable Data Breaches Scheme		
27.1.	Amend to include that for any eligible data breach, an entity 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	DIGI broadly supports this proposal.
28.	Interactions with other schemes		
28.1.	Encourage regulators to continue fostering coordination in enforcing matters relating to mishandling of personal information	Y	DIGI broadly supports this proposal.
28.2.	Establish a Commonwealth, State and Territory working group to harmonise privacy laws	Y	DIGI broadly supports this proposal.