The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

12 September 2019

The Treasury
Structural Reform Division
Email: DPIConsultation@treasury.gov.au

Dear Sir/Madam

DIGITAL PLATFORMS INQUIRY FINAL REPORT

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission to the Australian Government's consultation on the Final Report of the Digital Platforms Inquiry by the Australian Competition and Consumer Commission (ACCC).

1. Introduction

Ai Group's membership comes from a broad range of industries and includes businesses of all sizes. Given the breadth of this inquiry, we have received input from businesses in the IT, telecommunications, energy and retail sectors.

Overall, industry recognises the importance of protecting customer information and data, and supports a data and privacy regime which can benefit both customers and businesses through outcomes such as improved transparency and customer experience. However, we are concerned about the breadth of scope, and lack of evidence-based analysis and assessment of underlying causes for purported issues and associated recommendations in the ACCC's Final Report, which will likely have economy-wide impacts.

More rigorous investigation will be required relating to the recommendations discussed in this submission. This will need to include proper consultation, analysis and assessment of issues, underlying causes, and options to address these issues. A robust and considered cost-benefit assessment for any recommendations will also be required. In absence of these considerations, it is unclear whether the recommendations will provide material benefit to consumers and businesses in the long term, which may result in potentially unintended consequences. General comments about these concerns are discussed in the next section.

For the remainder of the submission, we provide specific comments about recommendations of concern for a wide range of industry sectors. These are recommendations 16 to 23 in the Final Report relating to privacy, data protection and unfair practices, as well as dispute resolution and complaint handling processes.

Our submission should not be regarded as exhaustive. However, it does identify our members' key areas of concern that require further consideration at this stage. As further consultation is undertaken, there may be additional matters raised.

We would also welcome the opportunity to work with the Government to bring together a range of industries who may be affected by this Final Report to be consulted with further.

2. General comments

Applicable to each of the recommendations discussed in this submission, we question whether proper consultation, analysis and assessment of issues and underlying causes have been undertaken in developing the recommendations, as well as consideration of factors including assessment of proportionality of response, relationship with and effectiveness of existing regulations, and proper consideration of consumer views and expectations.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

2.1. Proper consultation, analysis and assessment of issues and underlying causes

It is important to note that when the Privacy Act was introduced, the development of the law was methodical, properly considered and took almost 10 years. To provide another example, the European Union General Data Protection Regulation (EU GDPR), which has been heavily referenced in the Final Report, took at least six years to be developed.

In contrast, the scope of the ACCC inquiry was originally narrowly focused on digital platforms and took a period of 18 months. Only during the latter third of this period was the scope of this inquiry effectively expanded to apply to other businesses more broadly, with the Preliminary Report setting out a number of recommendations that would apply across the economy, while lacking sufficient detail and reasoning to enable proper consultation. This has now been followed with a more substantive 600+ page Final Report, which includes some further information about the previous recommendations in the Preliminary Report as well as new recommendations.

Therefore, there has been limited opportunity for proper consultation on these recommendations, with a total of only 12 weeks allocated for this Government consultation, including six weeks for making this submission. We caution against rushing through any proposed significant reforms in the Final Report, without proper consultation, as this will likely lead to unintended and serious consequences, as we have seen in the Government's consultation process for the *Assistance and Access Act 2018* (Cth).[1] Significant lessons should be learnt from the negative industry and public experience with that Act, and avoid repeating them again in relation to this consultation.

In addition to this consultation, there are multiple data- and digital-related consultations including on artificial intelligence (AI) ethics, data sharing and Consumer Data Right (CDR). These are either overlapping in scope or being considered concurrently and still open for consideration for some time now. These multiple consultations are very resource intensive and we question the capacity of any relevant stakeholder to participate comprehensively and thoroughly with this additional Digital Platforms Inquiry. The quality of engagement, and ultimately output, may be compromised.

In our previous submission on the Preliminary Report, we highlighted that more substantive work will be needed to develop a basis and detail for the recommendations before these can be consulted on further. While we appreciate the Final Report is more substantive in content, we still consider more work is required. In absence of this, there appears to be theoretical assumptions and hypotheses made in the Final Report, which requires further analysis and assessment including in relation to underlying causes for purported issues and options to address these. A compelling case has also not been sufficiently made to identify what actual consumer harm or detriment has occurred by the collection and use of data to justify these recommendations.

For instance, one member commented that the Final Report reads more like an Issues Paper, which would usually initiate a multi-staged consultation process. The ACCC provides commentary that there previously has not been significant reflection on the implications and consequences of the business models of digital platforms. One comment was that reflections on perceived issues cannot provide a basis for recommendations, but rather act to initiate investigation and quantitative and qualitative analysis, which would provide an evidence base for any recommendations. They cannot provide the basis for recommendations on their own. Future analysis and assessment could include: detailed consumer interviews (with questions more specific than those provided in the Final Report); analysis

[1] This Act was rushed through Australian Parliament last year without full consideration of the impact that this could create for a broad range of stakeholders. This has led to unintended consequences, including Australia's image overseas in relation to trust in Australian products and concern that the legislation could lead to the weakening of existing cyber security of businesses and its customers. See: Joint submission by Communications Alliance, Ai Group, AIIA, AMTA, DIGI and ITPA to the Parliamentary Joint Committee on Intelligence and Security on "Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" (Submission No. 23, July 2019); Australian Strategic Policy Institute, "Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018" (December 2018), p. 3.

of interviews to determine causes (including consumer and business behaviour); and assessment of functionality of current privacy frameworks against these consumer and business behaviours.

Ai Group recommendation: A proper analysis and assessment of the issues and underlying causes will be required, as well as options to address these, with respect to recommendations discussed in this submission. Proper consultation on these will also be required, which should be significantly longer than the total allocation of 12 weeks for this Government consultation.

2.2. Proportionality of response in recommendations

While the ACCC's recommendations in the Final Report suggest that the current privacy regime is insufficient, these recommendations lean more towards a disproportionate response through major legislative change as opposed to strengthening existing arrangements. There is also limited assessment of the material regulatory burden that these recommendations could place on businesses, especially smaller businesses – the impact of which will require further investigation.

Ai Group recommendation: Further consultation, analysis and assessment (including cost-benefit assessment) will be required relating to the recommendations discussed in this submission including their impact on the wide range of industry sectors and smaller businesses covered by the recommendations.

2.3. Relationship with and effectiveness of other existing regimes

We raised in our previous submission a need to clarify the scope of the ACCC's inquiry. This included consideration of other concurrent activities such as the CDR that is currently being implemented for certain sectors, as well as industry-specific regulations. Without proper consideration of these other interrelated regulations, there is a strong risk of regulatory fragmentation, which will ultimately impact businesses. At this stage, there does not appear to be proper coordination or consultation.

It is also important to recognise that the Digital Platforms Inquiry is part of a series of reforms (largely arising from the Productivity Commission's 2016 Data Availability and Use report), directed at unlocking the economic and social benefits of data. However, we are also operating in a changing environment. The impact of the proposed reforms in the Digital Platforms Inquiry needs to be viewed in this context and holistically with other regulations and reforms under way.

CDR

In the case of the CDR, the Final Report attempts to rationalise the scope of the CDR, and its relationship to the ACCC's privacy recommendations, as follows:[2]

> *… this Inquiry's recommendations are forward-looking proposals for the Government to generally update and strengthen the overarching Australian privacy regulatory framework. In contrast, the CDR operates within the existing legislative framework to deal with certain types of data and mechanisms for accessing that data in specific sectors of the economy. The CDR privacy protections should therefore be viewed as extra protections applicable only to CDR data, as defined for the purposes of the CDR legislative framework.*

This statement does not provide industry sufficient comfort or certainty. Outstanding questions remain as to how the ACCC's privacy reform recommendations will fit with other multiple forms of regulation in this area. We do not consider that a case has been made in the Final Report on whether the other existing regimes have been effective or ineffective. There are also growing concerns about how the

[2] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 437.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

CDR will interact with the current privacy regime. Making changes to the current privacy regime will likely create additional complexity and uncertainty.

The separation of CDR data from consumer data discussed in the Final Report does not seem realistic. It seems like a highly complex approach to assume that future CDR reforms to strengthen privacy regulation will be a separate consideration to legislative amendments made to protect consumers while sharing their data with third parties. The ACCC should provide case study explanations of how they expect this to function so stakeholders can provide appropriate feedback.

For instance, the current Government focus with the CDR has been for the banking sector. However, there has been limited consideration of the broader impact on other sectors when the CDR operates beyond banking. In particular, there has been no consideration for existing consumer rights in relation to access to data where such rights are not currently used, as is the case in the energy industry.

In this regard, we understand that the priority datasets for the energy sector under the CDR are already being consulted on. The ACCC will undertake consultation on the authorisation and authentication models for the sharing of energy consumer data. The ACCC should provide a case study explanation and examples of how consideration of these CDR models will specifically interact with their recommendations.

EU GDPR

Another regulation is the EU GDPR, which commenced operation in May last year, and may be applicable to some businesses in Australia. The ACCC makes a number of recommendations to adopt reforms similar to the GDPR. In the Final Report, the ACCC suggests it is not looking at wholesale adoption of the GDPR, but will look to more closely align with the GDPR. We would like to highlight issues that may arise in considering the GDPR:

- Some businesses may be subject to and compliant with the GDPR; if the privacy regime is changed to align with the GDPR, there may be an assumption that the regulatory burden would be minimal for businesses. But not all businesses, including smaller businesses, are subject to the GDPR and will likely see a greater regulatory burden and create a competitive disadvantage.

- For businesses compliant with the GDPR, there is a false economy if an ACCC recommendation varies from the GDPR. This issue is discussed further in the context of consent requirements.

- The GDPR operates in a very different legal framework than Australia's Privacy Act and relies on different administrative and enforcement structures. For these reasons, it cannot simply be implemented into Australia.

- Given the GDPR is relatively new, the Centre for Information Policy Leadership identified unresolved issues and challenges with the GDPR one year after it commenced operation, "where organisations feel the Regulation has not lived up to its objectives and has presented practical difficulties, despite their dedication to implementing the new requirements".[3] The International Association of Privacy Professionals also found more work is still required for companies to comply with the GDPR.[4]

- The potential impact of any GDPR type reforms to Australian businesses must also be carefully assessed. We should learn from the successes and failures of the GDPR and consider the real impact GDPR has had on individuals and businesses in Europe and elsewhere. We should not simply align to GDPR where the scope and potential impact of GDPR is unclear or untested, or where requirements are overly cumbersome with limited positive impact on privacy protection.

[3] Centre for Information Policy Leadership, "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges" (May 2019).
[4] International Association of Privacy Professionals, "GDPR compliance: Hits and misses" (May 2019).

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

Ai Group recommendation: Before further consideration of reforms to the privacy regime, a more comprehensive assessment will be required of the effectiveness of the existing privacy regimes, as well as regulatory reforms currently under consultation or implementation, including for different industry sectors and jurisdictions.

2.4. Proper consideration of consumer views and expectations

Despite the ACCC's references to consumer surveys to support some of its arguments on behalf of the consumer, there are questions about whether the ACCC's issues and recommendations properly reflect consumer views and expectations that are material in nature.

As the Final Report acknowledges, there is the concept of the "privacy paradox":[5]

> *In essence, the privacy paradox refers to a perceived discrepancy between the strong privacy concerns voiced by consumers who, paradoxically, do not appear to make choices that prioritise privacy.*
>
> *One possible explanation for the privacy paradox is that consumers claim to care about their privacy in theory but, in practice, the value they derive from using a digital platform's services outweighs the 'price' they pay in allowing the collection of their user data. A further explanation is that, while consumer attitudes are often expressed generically in surveys, actual behaviours are specific and contextual, and therefore, consumers' generic views regarding privacy do not necessarily predict their context-specific online behaviours.*

Even so, the ACCC does not appear to give much weight to this concept on the basis that the privacy paradox rests on the premise of consumers making informed decisions in their transactions with digital platforms; the ACCC is of the view that consumers may be prevented from making informed choices.

Notwithstanding the ACCC's views, we consider that the potential for a privacy paradox highlights a need to conduct more rigorous consumer interviews and dialogue to accurately identify the drivers of consumer perceptions. Without accurate identification of drivers, there is risk that recommendations made will not address potential underlying issues.

For instance, Government's interest in this area of reform relates to providing transparency and consumer value. However, the proposed reforms that are based on these aspirations may instead lead to impractical outcomes for consumers such as information and communication overload. There are also practical questions about: whether the consumer would actually go searching for information as a result of increased information and communication; and whether consumers will ultimately be disadvantaged by not getting access to, for example discounts or specials, as a result of new requirements such as opt-in consent discussed below.

Ai Group recommendation: Before further consideration of reforms to the privacy regime, a proper contextual analysis of consumer issues should be undertaken to assess the materiality of consumer concerns.

3. ACCC Recommendation 16(a): Update 'personal information' definition

As part of the ACCC's overarching recommendation 16 (aimed at strengthening protections in the *Privacy Act 1988* (Cth)), the ACCC's recommendation 16(a) to update the definition of "personal information" in the Privacy Act is based on their view that the current definition creates legal uncertainty and should therefore be aligned with the definition in the GDPR.

A member concern is that changing the definition of personal information will shift the emphasis from consumer protection (i.e. protecting identification of individuals) to data protection (i.e. protecting

[5] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 384.

identification of devices e.g. capturing technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual). The latter form of protection is based on the GDPR definition of personal information. It is unclear how defining such information as personal information will materially benefit consumers.

In addition, we note that the current definition of "personal information" already includes things like IP addresses in situations where they can reasonably identify someone (or are associated with other information that is about someone or which could reasonably identify someone). As the Office of the Australian Information Commissioner (OAIC) points out in their own guidance, whether a person is reasonably identifiable "is an objective test" which depends on the "context in which the issue arises".[6] The ACCC's proposal to amend the Privacy Act and define things like IP addresses and other metadata as "personal information" in all cases (even in circumstances where the metadata can't reasonably identify someone) is not necessary as: if the information could reasonably identify someone, it is already covered by the definition; and if it cannot reasonably identify someone, then it does not require the same level of protection as other personal information.

Further, while the recommendation purports to be in alignment with the GDPR, the proposed expansion of the definition for personal information under the Privacy Act will actually be broader in scope than the GDPR. For businesses already subject to the GDPR (as well as those who are not), this will likely create a new regulatory burden. Smaller businesses will also likely face a greater burden than larger businesses.

Questions also remain on how changing the definition of personal information will fit with other multiple forms of regulation in this area, including the CDR and industry specific regulations. Making changes to the definition of personal information will likely create additional complexity and uncertainty.

Alternative approaches do not appear to have been properly considered before the ACCC arrived at its recommendation. For example, instead of immediately resorting to changing the legal definition for personal information, a solution could be for the OAIC to provide additional guidance around the existing definition on a case by case basis. Such an approach would be a more proportionate response to address issues of legal uncertainty, without creating an unnecessary degree of regulatory burden for businesses.

As a matter of principle, the ACCC should consider issues and solutions within the current frameworks prior to introducing new frameworks. Otherwise, the ACCC should provide evidence as to why organisations such as the OAIC are not equipped to address the perceived issues.

Ai Group recommendation: Before deciding whether to proceed with ACCC recommendation 16(a), further work will be required to properly assess whether the current definition of personal information is appropriate. A proper assessment of options will also be required, including cost-benefit assessment.

4. ACCC Recommendation 16(b): Notification requirements

The ACCC's recommendation 16(b) proposes that the collection of personal information should be accompanied by a notice from the Australian Privacy Principle (APP) entity collecting the personal information (whether directly from the consumer or indirectly as a third party) unless the consumer already has this information or there is an overriding legal or public interest reason. The ACCC suggests that this will address information asymmetries for consumers and better inform them. They also acknowledge that this can create the risk of information overload on consumers and suggest ways that this could be minimised.

If such notification requirements were to be introduced, there is a risk that these could lead to a cumulative increase in notifications (albeit shorter in length) from APP entities (including third parties)

[6] OAIC, Australian Privacy Principles Guidelines, Chapter B: Key Concepts, July 2019, p. 20.

to consumers. Therefore, it is not clear how this recommendation will reduce information overload for consumers and be of material benefit to them.

As the Final Report acknowledges with respect to the effect of information overload:[7]

> *Information overload may result in suboptimal outcomes such as:*
> - *consumers putting off making a purchase that would have made them better off*
> - *consumers remaining with their existing supplier when switching suppliers would have made them better off*
> - *low consumer awareness and understanding of product risks, for example the risk of data breaches or targeted advertising*
> - *consumers feeling anxious and stressed from information overload.*

Elaborating further on the above, while the Privacy Act currently allows notification to be provided after collection (where it is not practicable to do so before), the ACCC's recommendation, if adopted, would require notification to be given at the time of collection. While this might be achievable where the data controller is collecting information from sites it owns and operates, this is more difficult and less practical where data is collected from third party sites, particularly where multiple APP entities are collecting information via one site.

Where multiple APP entitles are collecting information from one site, imposing notification obligations at the time of collection could result in consumers receiving multiple simultaneous notifications. This would not only impose a complex regulatory burden on business, but would increase the risk of "information overload" leading to consumer confusion and ultimately disengagement, an outcome that appears disproportionate to any demonstrated consumer benefit. To address this concern, we suggest that instead of requiring each APP entity collecting information to notify customers at the time of collection, the Government could require the third party site operator to provide the relevant notice of the collection by the APP entity, via either their privacy notice or some other means.

If there is limited benefit to consumers in introducing this new notification requirement, it would be inappropriate to create a new regulatory burden on businesses. Nevertheless, the ACCC "considers that the regulatory burden from the strengthening of notification requirements is unlikely to outweigh the benefits, particularly as the size of the burden imposed by stricter notification requirements will be commensurate with the extent to which the APP entity collects, uses and discloses the personal information of Australian consumers".[8]

We consider that this reasoning is inadequate and requires more rigorous analysis and assessment (including cost-benefit assessment). Otherwise, this recommendation will likely place an even greater regulatory burden for smaller businesses, not just larger businesses.

In the absence of substantiated evidence to the contrary, we consider that the current regime is operating adequately, striking the right balance between protecting the consumer without overloading them with information that may have limited value in practice, and not creating an unnecessary regulatory burden on businesses.

Ai Group recommendation: Before deciding whether to proceed with ACCC recommendation 16(b), further work will be required to properly assess whether there is material consumer benefit from these proposed notification requirements. A proper assessment of options will also be required, including cost-benefit assessment.

5. ACCC Recommendation 16(c): Consent requirements and pro-consumer defaults

The ACCC's recommendation 16(c) proposes to require consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal

[7] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 404.
[8] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 462.

information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason. The recommendation goes to both the circumstances in which consent is required for data processing under Australian law, and the requirements for obtaining a valid consent. The ACCC suggests that this will improve consumer choice over their information, as well as suggesting this will closely follow current non-binding APP guidelines and the GDPR.

Similar to our concern with the ACCC's recommendation 16(b), creating a new consent requirement for APP entities will likely create information overload for consumers – in this case, consent fatigue – as well as practical implementation issues for businesses to seek consent. Consumers will also be likely to miss out on benefits as a consequence of opt-in consent. In this respect, consumer expectations need to be properly considered, including the benefit that they may receive from having opt-out consent. For example, consumers do benefit from targeted advertising through improved customer experience and service.

While the ACCC suggests that the recommendation aligns with the GDPR, it recommends that Australia not adopt the GDPR principle that processing of data is also lawful if undertaken for the legitimate interest of the data controller. This is because it considers that the GDPR is too wide and flexible with respect to consent requirements. The recommendation therefore seeks to import a regime similar to that included in the GDPR without the inclusion of a critical component of that regime. As a result, the recommendation is not aligned with the GDPR. On this basis, there will likely be a regulatory burden for any business if this new requirement were to be introduced, with a greater burden felt by smaller businesses.

Exploring this further, the GDPR legitimate interest exception gives data controllers the ability to process data without obtaining the consent of the data subject where the data processor's legitimate interest in processing the data does not override the fundamental freedoms of the data subject. For example, the organisation may have a legitimate interest in processing personal data to enforce a legal claim, prevent fraud, or manage information security.

In this way, the GDPR attempts to strike a balance between the legitimate interests of the data processor (or a third party) and the fundamental privacy rights of individuals. This approach encourages data processors to think more about the impact of processing on individuals and the safeguards required to minimise undue impact on the data subject. Having a balanced legitimate interest exception also reduces the need to burden consumers with intrusive and repeated consent requests, particularly where the impact on the individual is limited or negligible. For example, balancing the privacy interests of users who want and expect to receive interest-based ads that help connect them to relevant products or services, and who have not opted out for such services, can be achieved through privacy safeguards to ensure the end result of processing does not produce legal or similarly significant effects on the data subjects. Such safeguards may include pseudonymising and segregating data and minimising retention periods where possible.

The ACCC's recommendation removes the balance struck by the GDPR where the privacy impact to individuals is minimal. The only reason given by the ACCC for rejecting the "legitimate interests" exception is the ACCC's view that "there is considerable uncertainty and concern surrounding the relatively broad and flexible definition of the 'legitimate interests' basis for processing personal information under the GDPR". This is not a valid reason to remove an element critical to the workings of the GDPR regime. While the ACCC acknowledges the real possibility of consent fatigue, no clear mechanism has been proposed to deal with it. Without this, there is a risk of creating a more cumbersome, confusing and intrusive experience for consumers while bringing no meaningful improvement to their understanding of data practices.

Before radically departing from the GDPR's legitimate interest test, the Government should carefully weigh the consumer benefits of this approach against the risk of consent fatigue and the impacts on the data management and privacy collection practices of Australian business across the economy.

Even in the event of there being sufficient evidence to support proceeding with the ACCC's recommendation 16(c), entities should not be expected to obtain consent for data already obtained

prior to this new requirement and should be exempted from the effect of this recommendation. That is, the recommendation should not have a retrospective effect.

We understand that collections required to perform a contract are excluded from the ACCC's proposal in recommendation 16(c). However, if such collections were not excluded and the definition of personal information were also broadened to include online identifiers, recommendation 16(c) could be expected to seriously impact online data collection practices as online identifiers will be required to perform a contract in order to engage in data processing.

Ai Group recommendation: Before deciding whether to proceed with ACCC recommendation 16(c), further work will be required to properly assess whether there is material consumer benefit from these proposed consent requirements. A proper assessment of options will also be required, including cost-benefit assessment.

6. ACCC Recommendation 16(d): Erasure of personal information

The ACCC's recommendation 16(d) proposes to amend the Privacy Act to give an individual the ability to request APP entities to erase that individual's personal information, without delay. The ACCC suggests that this will help mitigate the bargaining power imbalance for consumers and give them greater control over their personal information.

Several members identified a number of issues with the ACCC's recommendation.

This recommendation is akin to the GDPR's "right to be forgotten". While this concept has been implemented in the EU, the relatively new GDPR is not without its challenges, as discussed earlier. There are important lessons for Australia if a similar requirement were to be contemplated.

One member, while not opposed to the concept, is currently subject to the GDPR and has shared their own practical problem in complying with this GDPR requirement. For their business, they are placed in a position where they have to determine whether it is in the public interest to remove content about an individual if requested. In this example, inclusion of judicial oversight to make this determination would help this company resolve this matter, which is not currently available under the GDPR.

Another member is not legally obliged to erase personal information. However, in practice they may receive fewer than five requests of this nature from their Australian customers every year. Where they legally can, the member will endeavour to accept the customer's request, although it takes significant time for the company to process it. The limited number of requests that this company receives raises questions regarding the actual materiality of the need for consumers to seek erasure of their personal information, which will likely create a regulatory burden on businesses should they be required to comply with such a legal requirement.

If IP addresses and other metadata are defined in the Act as "personal information" (as per the ACCC's recommendation 16(a)) and this recommendation to allow consumers to request deletion of their personal information (and for entities to be required to delete it unless an exception applies) is also taken on board, there is a potential that individuals could misuse this right. The ACCC's proposed exceptions to this requirement to delete personal information relate only to information that is:

- required for the performance of a contract to which the consumer is a party;
- required under law; or
- otherwise necessary for an overriding public interest reason.

These exceptions should be expanded (or the public interest exemption clarified) to cover situations where the information is required to be retained in order to safeguard customer privacy or security or to prevent fraudulent activity. For example, a customer who asks one of our members to delete their metadata (after they have ceased to be a customer) – including device information and IP address – may do so in order to engage in fraudulent activity without our member knowing who they are. More work needs to be undertaken on considering the consequences of allowing individuals to request that this data (if defined as personal information) be deleted from an entity's records.

There are also potential privacy risks that might arise with the ACCC's recommendation. Therefore the recommendation needs to be clarified and carefully considered with a focus on ensuring privacy protection. For example, requiring APP entities to erase personal data that has been rendered pseudonymous may require an APP entity to reattribute full personal data such as name and email address to pseudonymous data to enable erasure. This could undermine the privacy protection offered by pseudonymisation in general, and increase the privacy risk to both the individual requiring erasure and other data subjects whose data is pseudonymised under the reattribution key. Careful consideration should be given to the ways privacy risk can be minimised without unintentionally jeopardising the individual's and other individuals' personal information. It should also be acknowledged that in some cases, there will be legitimate business requirements for APP entities to retain data, and in these circumstances, the focus should be on the use of effective privacy safeguards to minimise any risk.

In addition, the CDR may also include a requirement to erase personal information. As discussed above, consideration needs to be given as to how new requirements under the CDR interact with the ACCC's recommendations, including whether this ACCC recommendation is necessary.

Ai Group recommendation: Before deciding whether to proceed with ACCC recommendation 16(d), further work will be required to properly assess whether there is material consumer benefit from being given a right to erase their personal information. A proper assessment of options will also be required, including cost-benefit assessment.

7. ACCC Recommendation 16(e): Direct rights of action for individuals; ACCC Recommendation 19: Statutory tort for serious invasions of privacy

The ACCC's recommendation 16(e) on introducing direct rights of action for individuals and recommendation 19 on statutory tort for serious invasions of privacy are closely related so these are discussed together in this section. The ACCC suggests that recommendation 16(e) will empower consumers and give them greater control over their personal information by giving them another avenue for redress, and will incentivise APP entities to comply with the Privacy Act. For recommendation 19, the ACCC suggests that the new cause of action relating to statutory tort for serious invasions of privacy will lessen the bargaining power imbalance for consumers, address existing gaps in the privacy framework and increase the deterrence effect on businesses.

While it is important for consumers to have access to an avenue to seek redress for breaches of the Privacy Act, caution needs to be taken when considering creating any new forum or cause of action.

Firstly, we consider that the forum with the appropriate expertise lies with the OAIC to assess breaches relating to privacy and act on an affected individual's behalf. If there are concerns that the OAIC has insufficient resources to undertake its responsibilities or expeditiously resolve matters, a more appropriate response would be to increase the OAIC's resources.

Secondly, creating another avenue and action for redress through the courts may create other problems, including shifting the administrative burden from the OAIC to the courts, duplicating the OAIC's function, and potentially opening up the flood gates to a litigious culture. Such an outcome would be an administratively inefficient use of public resources.

Finally, there may be a false economy created for the consumer in seeking legal action through the courts. There will be legal costs for consumers and businesses in using this avenue which needs to be accounted for.

Ai Group recommendation: Before deciding whether to proceed with ACCC recommendations 16(e) and 19, further work will be required to properly assess whether there are material consumer benefits with these recommendations. A proper assessment of options will also be required, including cost-benefit assessment.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

8. ACCC Recommendation 16(f): Higher penalties for breach of the Privacy Act

The ACCC's recommendation 16(f) proposes to increase the civil penalties for breach of the Privacy Act to mirror the civil penalties of the Australian Consumer Law (ACL). The ACCC suggests that the previous penalties under the ACL were seen to be insufficient to deter profitable breaches of the ACL as a cost of doing business and that increasing penalties would act as a deterrent; the ACCC considers that there are parallels with the Privacy Act.

The ACCC's rationale for aligning the penalties in the Privacy Act with the ACL requires further substantiation.

Firstly, it is not clear whether the circumstances in which the ACL may be breached are similar in nature to a breach of the Privacy Act, except that it may involve a business and an individual.

In our research, we found that since the Notifiable Data Breach (NDB) Scheme under the Privacy Act commenced in February last year, there were over 1,000 data breaches reported by the end of March this year.[9] For this period, almost 60% were due to malicious or criminal attacks and over a third were due to human error.[10] Despite our own survey findings that found improvements in cyber security investment by businesses, causes for the NDB data breaches point to the need for improved cyber security and data management posture within organisations, where government support might assist. We do not consider increasing the penalty provisions will assist businesses or address underlying causes in any way. Bodies such as the Australian Cyber Security Centre (ACSC) should be commended for working closely with organisations affected by data breaches. However, as the ACSC has noted, this is help after the fact.[11]

Secondly, it is also unclear whether the OAIC is sufficiently equipped in undertaking its responsibilities. Providing the OAIC with adequate resources to administer its responsibilities will more likely assist all affected parties and would be a more proportionate response, without necessarily resorting to heavy-handed approaches such as increasing penalties.

Finally, reputation is invaluable and difficult to repair if it is damaged – policy makers and regulators should not underestimate this. As we have seen in media reports, companies that experience data breaches have not fared very well, not only with their shareholders, but also customers and partners, regulators and general public.

Ai Group recommendation: Before deciding whether to proceed with ACCC recommendation 16(f), further work will be required to properly assess options for deterring breaches of the Privacy Act, including cost-benefit assessment.

9. ACCC Recommendation 17: Broader reform of Australian privacy law

The ACCC's recommendation 17 proposes broader reform of Australian privacy law, which it believes will provide for a more robust privacy regulatory framework that better meets consumer expectations, maintains consumer trust and increases potential data portability. It also considers that this reform would assist in encouraging and sustaining data innovation and be fit for purpose in the digital age. This recommendation is wide-ranging, covering various topics including objectives, scope, higher standard of protections, inferred information, de-identified information, overseas data flows and third-party certification.

[9] Ai Group, "The Fourth Industrial Revolution: Australian businesses in transition" (Report, August 2019), p. 6.
[10] Following our report, the OAIC released its latest quarterly report for the April to June period. For this period, 245 data breaches were reported. Similar to our report, over 60% were due to malicious or criminal attacks and over a third were due to human error. See: OAIC, "Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019" (Report, August 2019).
[11] OAIC, "Notifiable Data Breaches Scheme 12-month Insights Report" (Report, May 2019), p. 19.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

For the purposes of this submission, we wish to provide a general comment about the role of regulation in the current Australian context. In short, we would be concerned if there were to be broader reform of the privacy regime that shifted from the current principles-based regulatory approach.

A general criticism about regulation is that it is too slow and inflexible to adapt and respond to technological change. Thoughtful strategy and credible policy responses from governments and regulators are important to plan for and respond to economic and technological change in ways that will meet community expectations.

Australian businesses are currently in transition to and within the Fourth Industrial Revolution. This includes entry into new technology sector markets, which requires positive measures from Government. However, more can be done to make us globally competitive. Regulation can boost or break the growth of an early stage industry sector or for an incumbent business that is seeking to make a transition. The extent to which new technologies are regulated can act as an investment barrier and diminish our attractiveness relative to other jurisdictions.

Highly reactive or overly change-averse responses risk curtailing innovation, reducing competitiveness and limiting the benefits of developments like digitalisation. A policy and regulatory vacuum is likely to provoke subsequent hasty overreaction to any problems that emerge. Regulation has a role in addressing reasonable public concerns including around privacy. But there are also often alternative approaches to the regulatory "stick", including consultation and dialogue, codes of practice, transitional support and education. Where regulatory measures are warranted, they still require careful development.

Government should proactively:

- consult about major technological and economic changes;
- consider the full range of options for response;
- adopt regulatory responses only where they are proportionate and likely to provide net community benefits; and
- develop any regulatory response in full consultation with affected stakeholders.

More generally, Government should reinvigorate best practice regulation initiatives, and study global best practices in regulation and business support that encourage – rather than inhibit – innovation and productivity.

Returning to the ACCC's recommendation, it is important to consider whether the current privacy regime is appropriate in light of the above context. We consider that a principles-based approach to privacy regulation, as currently reflected in the Privacy Act, is flexible enough to enable future proofing and therefore technology neutrality in a rapidly changing environment. This strikes the appropriate balance between protecting the privacy of individuals and regulating businesses.

As the former Privacy Commissioner, Karen Curtis, stated:[12]

> *By encouraging organisations to recognise the business advantages of good personal information handling practices and regulating their behaviour accordingly, government regulators can minimise regulatory intervention and red tape. This has been a common theme of our regulatory approach where a legislative framework is balanced by an emphasis on business privacy awareness and self-regulation. The idea is to inculcate the values and objectives of privacy law in business rather than just the superficial rules. When this happens organisations will be better equipped to deal with technological change because they will understand the ideas behind the laws – the principles – and will not become as confused by detailed technology-specific regulations.*

In reference to the former Commissioner's remarks, the ALRC concluded:[13]

> *In this way, principles-based regulation aims to minimise the need for enforcement by 'encouraging organisations to understand the values behind the law and change their behaviour accordingly; not*

[12] ALRC, "For Your Information: Australian Privacy Law and Practice" (Report 108, August 2008), p. 237.
[13] Ibid.

because they might get caught out by a regulator, but because they understand why the law is there and what its objectives are'.

In contrast, an alternative to principles-based regulation (i.e. prescriptive-based regulation) runs the risk of stifling innovation and making Australia less competitive compared to its more advanced peers. Regulation should be drafted to allow it to be nimble and flexible rather than overly prescriptive and heavy handed in the first instance. This will be especially important, given the significant wide scope of this Digital Platforms Inquiry and its potential impact on a wide range of stakeholders.

Ai Group recommendation: In the absence of substantiated evidence to the contrary, we consider that a principles-based approach as currently reflected in the Privacy Act is appropriate. Further consultation will be required if any broader reforms to the current regime were to be considered.

10. ACCC Recommendation 18: OAIC privacy code for digital platforms

The ACCC's recommendation 18 proposes the development of a privacy code to be developed by the OAIC for digital platforms with the view that this would address specific data practices of concern associated with digital platforms. It is our understanding that this recommendation would apply to "all digital platforms supplying online search, social media, and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information".[14] That is, it is not designed to have an economy-wide application, unlike recommendations 16, 17 and 19.

In general, there may be support for this code, especially if it is used as an instrument to raise consumer awareness about how personal data is handled and inform the public about tools that may be available to them. However, this recommendation raises similar issues as the ACCC's recommendations 16 and 17. For instance, questions arise as to whether there is substantiated evidence to support the ACCC's recommendation 18, and whether it significantly departs from the current principles-based regulatory approach under the privacy regime. Without proper consideration, unintended consequences could potentially serve to chill investment, innovation and diminish our attractiveness relative to other jurisdictions.

We would also caution if the application of this code were considered to be expanded by Government to have an economy-wide application. If a broad interpretation of digital platforms were to be taken, this may apply to other businesses which have the capability of being a digital platform or business. In that scenario, this could raise a separate question about what type of businesses would be subject to this recommendation, and how this proposal would fit in with any existing obligations for affected businesses. There could also be an additional complexity with the operation of the CDR, raising another question about how the code would interact with the CDR. A broad interpretation of the definition of digital platforms could also be ambiguous and create uncertainty as to who is subject to and not subject to the code.

Ai Group recommendation: We caution against any broad interpretation of the application of ACCC recommendation 18. If this recommendation were to be broadly applied, further work will be required to clarify the scope of this recommendation, and properly consult with consumers and industry experts.

11. ACCC Recommendation 20: Prohibition against unfair contract terms; ACCC Recommendation 21: Prohibition against certain unfair trading practices

The ACCC's recommendations 20 and 21 have been considered together in this section. The ACCC recommends that the existing unfair contract terms regime be amended to include civil penalties

[14] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 481.

(recommendation 20) and that a new prohibition on "unfair trading practices" be introduced (recommendation 21). The basis for the ACCC's recommendation 20 is that the existing approach to unfair terms as being able to be declared void provides insufficient deterrence, and it considers there are significant information asymmetries and bargaining power imbalances for the consumer, leading to consumers being unable to negotiate a bargain with digital platforms for their personal data. For recommendation 21, the ACCC considers that there are gaps in the *Competition and Consumer Act 2010* (Cth) (CCA) and ACL which may not currently be caught but which has the potential for significant consumer harm. The ACCC considers this to be an economy-wide issue.

It is important to note that current notions of unfairness in Australian law are at the core of several provisions in the ACL:

- unconscionability under common law (which is incorporated into the ACL in section 20);
- the statutory form of unconscionability (section 21);
- unfair contract terms (section 23); and
- the "unfair practices" set out in Part 3.

Some elements of fairness also inform other provisions in the CCA, including transparency in dealings in the general prohibition on misleading or deceptive conduct (ACL section 18) and a notion of commercial non-discrimination – or "level playing field" – that can be relevant to cases under the law against the misuse of market power (CCA section 46). There are also a range of sector-specific norms that would overlap with a general unfairness provision, notably rules on "good faith" in franchising and insurance. Taken together, these existing provisions represent substantial regulation of unfair conduct.

In our previous submission, we highlighted the following work that needs to be done and is still applicable to these recommendations:

- It is not clear whether the existing provisions are insufficient to protect consumers. Without substantiated evidence to the contrary, a case has not been made that a problem exists under the current law; therefore changes should not be made to the existing regime. In other words, the existing unfair contracts regime, and the related protections in the ACL, appears to be working effectively for consumers and businesses.

- It seems that such prohibitions could potentially open the door to significant uncertainty with consequential difficulties in practical compliance by businesses. For instance, the ACCC notes that such prohibitions could be used to protect consumers from conduct that they are unaware of, such as certain types of data collection, yet the Privacy Act already sets out the sorts of information for which disclosure is required and it is unclear why an amendment of that mechanism is not the best available means to address these issues.

- Even in the event of there being sufficient evidence to support proceeding with the recommendation relating to unfair contract terms, existing contracts already in place should be protected and exempted from the effect of this recommendation. That is, the recommendation should not have a retrospective effect. Otherwise, changes arising from the recommendation could lead to open ended challenges to a broad range of existing contracts (agreed to prior to the recommendation) and create inconsistencies in the execution of these contracts.

Further to our previous comments, the following are additional comments in light of the ACCC's recommendations 20 and 21. These highlight reasons why the proposal similar to recommendation 20 was previously rejected, and the lack of substantiating evidence and inadequate assessment in the Final Report behind the ACCC's recommendations 20 and 21.

Unfair contract terms

The introduction of penalties for unfair contract terms has been rejected previously on the basis that the standard of assessment is too ill defined to be applied directly. The same issues arise in the context of recommendation 20.

The Final Report of the *Review of the Australian Consumer Law* (ACL Review) in 2017 considered and rejected a less ambitious proposal than the ACCC's recommendation. The ACL Review considered an amendment such that it would be illegal to include terms in a contract that had previously been found unfair by a Court. The proposal was rejected, partly because terms should be considered in the context of individual contracts on a case-by-case basis. (The ACL Review report also noted that if a term has been found unfair, the inclusion of that term in a similar contract would constitute misleading conduct on the part of the business imposing it.) Such an approach would leave businesses in a position where they could not include terms necessary to protect their legitimate interests, which may differ from those of other businesses. It would also not take into account the broader context within which a term is used, including whether a term is reasonable when considered in combination with other provisions of the same contract. This same risk of uncertainty would arise with respect to recommendation 20.

Although the ACCC has claimed that the current approach does not provide sufficient deterrence, no evidence is offered to support the claim. Changes to the current unfair terms laws should only be made if it can be shown that there will be a significant improvement in conduct or efficiency compared to the current approach of terms being declared void. Any changes should also address the current uncertainty that arises with respect to the definition of small businesses through "bright line" but arbitrary thresholds on yearly transaction values and employee numbers. It will often be difficult or impossible for businesses to ascertain whether a business is a small business when developing standard form contracts and in individual cases, there is potential for a counterparty to change status simply through growth or attrition in employee base.

Unfair trade practices / commercial practices

The ACCC suggests the existing ACL provisions are inadequate to catch some unfair conduct and it proposes a new general prohibition against "unfair trading practices". The argument it makes is that some commercial practices do not fit within the existing provisions. However, the Digital Platforms Inquiry did not include an assessment of where the current ACL provisions, when considered in conjunction with its proposed amendments to privacy laws (if enacted) would fail to address the conduct described. There is in fact a risk that these recommendations taken together would lead to both duplication and inconsistency.

The ACCC acknowledges that, if the proposal were introduced, some guidance would be required to provide certainty. The guidance a regulator in the position of the ACCC can provide would only be its view of the substantive provision; it should not be empowered to define forms of conduct that would or would not contravene the law itself – that is, the ACCC should not define "black lists" of conduct that would contravene the law, or "white lists" of what would not. Providing the ACCC with a broad rule-making power to decide forms of conduct that are unfair (similar to that exercised by the United States Federal Trade Commission (FTC) under the FTC Act) would sit uneasily in Australia's constitutional and administrative structure, exposing businesses to significant penalties while creating significant uncertainty with respect to compliance.

In supporting its proposals, the ACCC refers to unfair provisions that apply overseas, in particular section 5 of the FTC Act and Article 5 of the European Unfair Commercial Practices Directive 2005/29/EC. Those comparisons do not sufficiently take into account that Australia already has a range of detailed consumer protections. The Australian approach reflected in the ACL and its predecessors was to prohibit particular forms of conduct individually from the start. In particular, the catalogue of "unfair practices" in part 3 of the CCA is already expansive. The Australian statutory form of unconscionability also affords protection in appropriate circumstances.

Ai Group recommendation: In the absence of substantiated evidence to the contrary, the current unfair contract terms and unfair trading practices should be considered to be operating appropriately. Further development and consultation will be required if ACCC recommendations 20 and 21 were to be considered.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

12. ACCC Recommendation 22: Digital platforms to comply with internal dispute resolution requirements; ACCC Recommendation 23: Ombudsman scheme to resolve complaints and disputes with digital platform providers

As the ACCC's recommendations 22 and 23 are related, these are considered together in this section. The ACCC's rationale for recommendation 22 is due to the rise of online scams, which it considers have been enabled by digital platforms; therefore it considers an internal dispute resolution mechanism can be set up to enable consumers to seek redress from digital platforms. If a consumer's complaint is not met, then an external body would be able to facilitate resolution of their complaint under recommendation 23. The ACCC considers that this would take down scam ads and similar content for consumers that have experienced harm.

Currently, there are multiple bodies responsible for complaints handling including the OAIC, State Fair Trading and Consumer Affairs bodies, Ombudsmen such as the Small Business Ombudsman, and eSafety Commissioner. There are also international standards for complaints handling recognised by ASIC and APRA, as well as Regulatory Guide 165 which ASIC has released. At this stage, it is not clear whether the existing bodies and their complaints handling processes are ineffective such that they would warrant consideration of recommendations 22 and 23.

Even if there were problems with the current administration by the multiple relevant regulatory bodies, a more proportionate response would be to improve the existing arrangements; as opposed to creating new bodies or responsibilities that leads to conflicts with the existing bodies. We consider that the existing bodies, especially OAIC, have the relevant privacy expertise. These bodies have also developed invaluable knowledge in working with industry and the public.

Ai Group recommendation: In the absence of substantiated evidence to the contrary, we do not support ACCC recommendations 22 and 23.

Should the Government be interested in discussing our submission further, please contact our Digital Capability and Policy Lead Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,

Peter Burn
Head of Influence and Policy