The Australian Industry Group
Level 2, 441 St Kilda Road
Melbourne VIC 3004
PO Box 7622
Melbourne VIC 3004
Australia
ABN 76 369 958 788

6 December 2021

Attorney-General's Department
Email: OnlinePrivacyBill@ag.gov.au

Dear Sir/Madam

ONLINE PRIVACY BILL EXPOSURE DRAFT

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (OP Bill) by the Attorney-General's Department (AGD).

Ai Group's membership comes from a broad range of industries and includes businesses of all sizes. Given the growing engagement across the business community with every business having the capability of having an online business or platform, we are particularly focused on the implications for the broader cross-section of Australian businesses. This is not limited to only large technology companies, but also SMEs and businesses from a range of sectors.

Overall, industry recognises the importance of protecting the privacy, safety and security of the Australian community, both in the physical and online realm. Indeed, Ai Group works closely with governments and their agencies in a diverse range of areas. In this mix, the Office of the Australian Information Commissioner (OAIC or Commissioner) has an important specific role to promote privacy protections.

Our submission therefore does not object to the underlying intention behind the Bill, which is to provide appropriate online privacy protections for the Australian community. However, we consider that as a matter of good policy and regulatory practice, proper analysis and assessment of issues, underlying causes, options to address these issues, as well as a robust and considered cost-benefit assessment for any proposed regulatory or legislative change, need to be given to this consultation.

Further, given the potential uncertainties and significant impact on many stakeholders arising from the AGD's concurrent privacy reforms (i.e. broader review of the *Privacy Act 1988* (Cth) (Privacy Act Review) and the OP Bill), the AGD should build more time and stages to enable for proper consultation on these reforms with affected stakeholders.

At this stage, we do not consider that this has been done and more work is required. It would therefore be prudent for proposals arising from the OP Bill to be considered as part of the AGD's broader Privacy Act Review (as opposed to separately undertaking a parallel consultation on the OP Bill) and to provide stakeholders with an opportunity to consult on the overall package of reforms.

Otherwise, there is a strong risk that these parallel consultations will lead to confusion, unintended consequences, and unnecessary regulatory complexity, burden and costs for businesses and regulators, especially during a period of economic recovery from this pandemic.

And from a global perspective, the speed and lack of due process of many of these proposed legislative changes risk creating the perception that Australia is not a favourable destination for digitally focused companies. This undermines the otherwise great work that Australia is doing in global digital trade rules, namely with Digital Free Trade Agreements and at the World Trade Organisation.

Below is a summary of our issues and recommendations.

Issues	Recommendations
1. Problem and rationale for regulation	• A more detailed analysis of the problem statement should occur before proceeding with the OP Bill. The Privacy Act Review provides the perfect platform for this.
2. Interactions with Privacy Act Review	• The Privacy Act Review should take precedence over the OP Bill to ensure proper analysis, assessment and consultation of the issues and underlying causes (if any), as well as options to address these. • Sufficient time and consultation stages need to be allocated for providing proper stakeholder consultation on the AGD's concurrent privacy reform consultations, including the proposed approach for development of the Online Privacy Code (OP Code). • If it were not possible to pause the OP Bill to allow for the Privacy Act Review to take precedence, the scope of the OP Bill should be limited to those aspects requiring Government's critical attention and subject to further consultation.
3. Interactions with other interrelated reforms	• Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation. • Government should improve coordination between government agencies and departments with respect to this consultation and other interrelated reforms, legislations and regulations. • Government should review the interactions between the CDR and Privacy Act more broadly with the objective of reducing regulatory duplication and red tape. • Government should explore other options to enable sharing of information between the OAIC and eSafety Commissioner to avoid regulatory duplication and overlap. • An alternative option could include establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to online activities.
4. Overly broad and disproportionality in scope of targeted businesses	• Subject to properly assessing the issues and underlying causes, Government should further clarify the businesses that it intends to target under the OP Bill. • Based on clearly defined targeted businesses under the OP Bill, Government should undertake a proper assessment of the impact on targeted businesses including cost-benefit assessment and other relevant implementation considerations (e.g. compliance time and assistance).
5. Lack of consideration of other options and solutions	• Government should explore other options to the OP Bill and these should be considered as part of the Privacy Act Review, including: o Providing sufficient resources to the OAIC funded by Government in the first instance; o Reviewing the effectiveness of the APPs; and o Providing businesses with transition assistance such as an industry engagement plan for enabling business privacy capability uplift, Government funding to support business uplift, and providing industry with a reasonable timeframe to meet any new compliance requirements.

1. Problem definition and rationale for regulation

The genesis behind the proposed Bill is based on the following propositions made in media statements and the Explanatory Paper:[1]

- The Privacy Act does not currently specifically protect against the misuse of Australians' personal information by social media and other online platforms.

- In response to one particular data harvesting incident, the Government has committed to introduce a binding code of practice for social media and other online platforms that trade in personal information, and enhance enforcement mechanisms and penalties provisions under the Privacy Act.

- The ACCC's Digital Platforms July 2019 Final Report, recommending the development of a privacy code for digital platforms and increasing penalties for breach of the Privacy Act.

- In March 2019, the Government committed to undertaking reforms to regulate "online platforms **that trade in personal information**" (emphasis added) to require companies to "be more transparent about any data sharing and requiring more specific consent of users when they collect, use and disclose personal information".[2]

1.1 Purpose of the Privacy Act Review

With respect to the first proposition above, the Regulation Impact Statement (RIS) suggests in further detail areas where there are limitations in the Privacy Act, the need for strengthening penalties and enforcement mechanisms, who the problem affects and potential magnitude, and need for government action.[3] We consider that insufficient work has been undertaken to arrive at these conclusions and there warrants further assessment as part of the Privacy Act Review.

For instance, we note that social media and other online platforms must comply with the Privacy Act and therefore are not unregulated. In this regard, the broader review of the Privacy Act includes determining whether the Act is fit for purpose, and if it is not then amendments will be proposed.

We discuss further regarding the critical interactions of this consultation with the Privacy Act Review in section 2.

1.2 Potential conflation of issues

With respect to the second proposition above, it is not clear whether substantiated evidence has been provided to demonstrate that a systemic problem exists across the wide range of businesses potentially subject to the Bill to justify a broad-brush approach to privacy reform in the form of this OP Bill. Without such evidence and rigorous assessment, there is a risk of conflating issues and creating unnecessary regulatory burden that could impact a wide range of businesses and chill investment and innovation just as businesses seek to recover from the COVID-19 pandemic.

For example, we note that the OAIC initiated legal proceedings in response to this particular data harvesting incident. This suggests that the current framework adequately provides the regulator with an appropriate avenue to address circumstances in which organisations regulated under the Privacy Act are suspected to be in violation of their obligations under the Act.

---

[1] AGD, Explanatory Paper, Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (October 2021), p. 3.
[2] Attorney-General and Minister for Communications Minister for the Arts, "Tougher Penalties to Keep Australians Safe Online" (Joint Media Release, 25 March 2019), https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F6577790%22;src1=sm1.
[3] AGD, Enhancing online privacy and other measures: Early Assessment – Regulation Impact Statement (October 2021), Pp. 4-12.

1.3 Further work required following ACCC Digital Platforms Inquiry

With respect to the third proposition above, we previously raised with the AGD that more work was required. There appeared to be theoretical assumptions and hypotheses made in the ACCC's Digital Platforms Inquiry Final Report, requiring further analysis and assessment including in relation to underlying causes for purported issues and options to address these. A compelling case was not sufficiently made to identify what actual consumer harm or detriment had occurred by the collection and use of data to justify these recommendations. We are also concerned to ensure that relevant assessments and analyses take account of the privacy paradox which causes consumers to say one thing but do another. 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.

For instance, one Ai Group member commented that the ACCC's Final Report read more like an Issues Paper, which would usually initiate a multi-staged consultation process. The ACCC provided commentary that there previously has not been significant reflection on the implications and consequences of the business models of digital platforms. A further 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 ACCC's Final Report); analysis of interviews to determine causes (including consumer and business behaviour); and assessment of functionality of current privacy frameworks against these consumer and business behaviours. These are initiatives where the AGD can substantively improve upon the outcomes in the ACCC's Final Report.

1.4 Wide breadth of organisations covered

Finally, with respect to the fourth proposition above, we note that the RIS proposes that around "500 organisations (approximately 150 social media platforms, 85 data brokers, and 265 large online platforms)" should be subject to the OP Code. We consider this to be a particularly broad net, especially considering that many of these likely do not "trade in personal information".

For instance, of the approximately 500 entities estimated by the Government, it is reasonable to expect at least 300 entities would wish to actively participate in Code development. The RIS considers that there would be two OP Code developers. How these developers would coordinate or otherwise work together to develop one OP Code is not explained.

The large number of covered entities and the diversity of their business interests and activities will add substantial complexity and cost. As a result, the true cost to covered entities in working on an OP Code will be much higher than the estimates in the RIS.

It would be appropriate to conduct a critical review of the need, cost and benefit of making organisations subject to the OP Code ahead of completion of the Privacy Act Review.

More appropriately limiting the scope to those aspects requiring Government's critical attention may be able to reduce the complexity of the OP Code and meet its timeline targets.

We discuss further about issues related to the wide breadth of organisations targeted by this Bill and other options associated with the Bill in the sections below.
Overall, we strongly recommend that the above considerations be properly assessed as part of the broader Privacy Act Review to enable proper consideration of the issues, their underlying causes (including the extent), and developing proportionate responses.

Otherwise, without a holistic assessment of issues and potential solutions in relation to privacy reforms, there is a risk of conflating issues and developing solutions that can inadvertently affect many businesses. This includes creation of unnecessary regulatory duplication, burden and costs on affected stakeholders. There is also a risk that proceeding with the OP Bill diminishes industry confidence in legislation and regulation in this domain, as well as devalues the purpose of the Privacy

Act Review. Such an outcome would be inconsistent with the Australian Government's deregulation agenda.[4] We discuss further about the Privacy Act Review in the next section.

Ai Group recommendation: A more detailed analysis of the problem statement should occur before proceeding with the OP Bill. The Privacy Act Review provides the perfect platform for this.

2. Interactions with Privacy Act Review

The AGD acknowledges in this consultation that there are interactions between its OP Bill and the Privacy Act Review. However, the AGD suggests that the Bill "addresses the pressing privacy challenges posed by social media and other online platforms", while the Privacy Act Review "seeks to build on the outcomes of the Online Privacy Bill to ensure that Australia's privacy law framework empowers consumers, protects their data and best serves the whole of the Australian economy".[5]

However, we consider that the issues raised and solutions proposed in the OP Bill are intertwined with the wider Privacy Act Review. We are concerned if the OP Code (under the Bill) were to be developed ahead of completion of the Privacy Act Review, without proper consideration of the practical challenges and other options including amending the Bill.

2.1 Broader key issues relating to Privacy Act Review

In our previous submission to the AGD on its issues paper for the Privacy Act Review, we raised several issues that would also be relevant to this OP Bill.[6] The following key topics included:

- Proper understanding and assessment of consumer expectations with respect to privacy;
- Addressing multiple legislative and regulatory regimes associated with personal information;
- Appreciating the value and role of principles-based regulation enabled through Australian Privacy Principles (APPs) under the Privacy Act;
- Caution against adopting EU GDPR (fully or partially) without proper understanding of its operation and context;
- Appreciating the role of employee records exemption and areas for improvement in this provision under the Privacy Act; and
- Issues associated with introducing legislative and regulatory requirements related to:
  - Collection of personal information notice;
  - Consent to collection and use and disclosure of personal information;
  - Right to be forgotten or erasure;
  - Direct right of action;
  - Statutory tort for invasion of privacy;
  - Proper support for businesses with respect to mitigating Notifiable Data Beaches (NDBs) e.g. uplift initiatives; and
  - Proper coordination and integration between legislative and regulatory reforms and other activities.

Therefore, before contemplation of a solution (in this case, the OP Bill), as a matter of good policy and regulatory practice the above matters need to be properly assessed and options should be developed and consulted upon to address the underlying issues and causes.

Further, we have observed on several occasions a sense of Government urgency in passing through legislation, especially where it relates to online activities. However, this has been at the risk and detriment to stakeholders of not being provided sufficient consultation, clarity, certainty and regulatory

[4] See: https://deregulation.pmc.gov.au/.
[5] See: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.
[6] Ai Group submission to AGD (November 2020), https://www.ag.gov.au/sites/default/files/2020-12/ai-group.PDF.

safeguards, leading to potential unintended consequences, and regulatory burden, complexity and costs.

For example, we note that the concurrent privacy reform reviews and timeframes allocated for consultation are insufficient, especially in addressing potential uncertainties arising from these reforms. The AGD should build more time and stages to enable for proper consultation with affected stakeholders on these reforms that can have a significant impact on many stakeholders.

We therefore strongly encourage the AGD to have regard to these various considerations.

2.2 Practical challenges with concurrent consultations

The following are practical challenges raised by our members that will need to be considered with respect to the concurrent consultations:

- Online Privacy (OP) organisations will be required to meet requirements additional to those under APPs 3, 5 and 6 relating to the collection, notification of collection and use and disclosure of personal information, notwithstanding that the Privacy Act Review is currently reviewing each of these aspects and currently seeking input on proposals that would see a significant shift in the content and use of both Privacy Policies and Collection Notices. The failure to align the timing of the OP Bill and Privacy Act Review will:

    - require OP organisations to invest in the implementation of systems and processes to meet the requirements of the OP Code which will, within a short period of time, need to be reviewed holistically to ensure alignment with the definitions and content of the Privacy Act following completion of the current review; and

    - place those future-thinking OP organisations already working to meet the likely requirements of the revised Privacy Act and evolving customer expectations at risk of getting this wrong (in an environment of increased penalties). A slowdown in innovation in this area will be to the detriment of consumers and the digitally enabled economy in Australia.

- The Discussion Paper for the Privacy Act Review outlines possible alternatives that have not yet been selected, and developed to a level of specification so that their practical effect and operation can be assessed with any reasonable reliability. Many of the matters to be addressed in an OP Code require covered entities to anticipate how complex areas proposed for substantial change in the Discussion Paper will be regulated under a revised Privacy Act.

- An OP Code developed in advance of Privacy Act reform to address mandatory inclusions as specified by the OP Bill is likely to have substantially different operation and effect once Privacy Act reforms contemplated by the Discussion Paper are enacted. The then changed legislated provisions today cannot be reasonably anticipated in development of an OP Code in advance of those changes.

- The foundational elements that industry requires to build a clear, comprehensive and sufficient Code are not specified in the OP Bill in sufficient detail to enable covered entities to develop a detailed OP Code compliant with the stated requirements. Examples of foundational elements not yet been determined include: the definition of “personal information”; requirements for valid “consent”; circumstances in which express consent must be sought and obtained; scope of operation of transparency requirements in relation to respectively privacy policies and privacy (collection) notices (e.g. what must be addressed in each); the extent to which use of technical information for differentiated treatment of users will be regulated under the Privacy Act; whether there should be a broad form opt-out option for users of online services; and reasonable bases for exceptions from an opt-out option (i.e. any carve-down for reasonably anticipated or compatible uses or legitimate uses or interests).

- Because the required inclusions in the OP Code are only very broadly stated and not specified as foundational elements (a design specification) for development of an OP Code, it is very likely that any OP Code (whether negotiated by industry or determined by the Commissioner) will require substantial rewriting to address a revised Privacy Act. Presumptive coverage of areas proposed

for substantial change is likely to result in misspecification in an OP Code as to the substantive effect of foundational elements as given operation in a revised Privacy Act.

- The first round of Code development will require substantial working up of foundational elements that would not have yet been determined by the legislature and are still unclear as to design for implementation. The first iteration of the Code is likely to have a limited period of operation before covered organisations must fundamentally rewrite it to address new and changed requirements of a revised Privacy Act. The first iteration of the Code development process will need to be repeated in a second round of Code development following Privacy Act reform. Given the range and complexity of matters to be addressed in the Code, the number and range of covered organisations, and diversity of their business activities, it is estimated that industry will likely need at least 12 months, after the design specification for an OP Code is settled upon passage of the Bill, to develop a draft Code and submit this draft to the Commissioner for review. A reasonable estimate is that an OP Code developed following passage of an OP Bill is unlikely to enter into operation before Q2 2023, about the same time as a substantially revised Privacy Act enters into operation. The first iteration of the Code will then require revision to address changed and supplemented legislated requirements that are likely to commence in operation almost immediately upon the first Code entering into operation.

- Areas of uncertainty and cost of duplicated effort will likely be compounded by the large number of entities that would fall within the proposed broad categories of covered organisations and diversity of their business activities, as discussed earlier. Further, presumptive coverage in a detailed OP Code of complex areas proposed for substantial change would be difficult to achieve even if the OP Bill envisaged coverage of a small number of entities conducting similar business activities. It is most unlikely to be achieved given the large number of covered organisations and the diversity of their business activities.

Therefore, it would be prudent that matters considered under the OP Bill be included as part of the wider Privacy Act Review.

2.3 Proposed amendments to the Bill

If Government decides to proceed with its Bill despite our above concerns, development and commencement of the OP legislation including Code should be reviewed so that businesses can be sure that their investments will be able to meet the future requirements of the Privacy Act.

In particular, our member feedback raise the following considerations (including amendments to the Bill) that would warrant further consultation:

- Government should have regard to how it can meet its stated objective of regulating online platforms that trade in personal information without imposing unnecessary regulatory costs on a significant number of businesses. This is particularly relevant as Australia looks to develop its digital capabilities and future. In particular, a case has not been made at this stage for the inclusion of "large online platforms" and this should be excluded pending fuller consideration as part of the Privacy Act Review**.** For example, if Government and the legislature were concerned that industry development may be delayed or stall due to complexity and range of covered activities and covered entities, the sensible way to address that concern is to narrow the range of entities and activities to be covered, and to require the Code to address only those matters where Government and the legislature require urgent attention. This should be undertaken in a way that reasonably meets stakeholder expectations and reasonably anticipates future reforms. It would be premature for the OP Code to include a category as broad as "large online platforms" which do not necessarily trade in personal information, pending further consideration as part of the Privacy Act Review.

- OP organisations will be subject to the OP Code, including all areas of enterprise (i.e. including areas beyond those activities outlined in section 6W of the Bill "Meaning of OP organisation") unless expressed otherwise in the OP Code (section 26KC(9) of the Bill). Consideration should be given to narrowing the scope of the OP Code such as covering only those acts and practices involving the collection, use and disclosure of personal information relating to personally identifiable individuals whose information is derived from conduct covered by the OP Code.

- OP organisations will be required to stop using or disclosing individuals' personal information on request. It would be of benefit to members if section 26KC(2) of the Bill could be amended to clarify that this requirement does not limit the use of anonymised information.

- Development of an OP Code should specify how covered entities would address current core APP requirements, applying current Privacy Act definitions and requirements as to the giving of notices (transparency) and as to consent, to the extent that the Government considers that these core requirements are not currently being appropriately addressed by some covered entities.

- There should be a clearly staged (phased) approach to development of the OP Code, so that industry is not pre-empted by intervention by the regulator as a result of unrealistic expectations as to how quickly a Code may be developed.

- At a minimum, industry should be allowed a clear 12 months from enactment of the OP legislation to finalise a final draft OP Code for submission to the Commissioner for registration.

Ai Group recommendations:

- ***The Privacy Act Review should take precedence over the OP Bill to ensure proper analysis, assessment and consultation of the issues and underlying causes (if any), as well as options to address these.***

- ***Sufficient time and consultation stages need to be allocated for providing proper stakeholder consultation on the AGD's concurrent privacy reform consultations, including the proposed approach for development of the OP Code.***

- ***If it were not possible to pause the OP Bill to allow for the Privacy Act Review to take precedence, the scope of the OP Bill should be limited to those aspects requiring Government's critical attention and subject to further consultation.***

3. Interactions with other interrelated reforms

In addition to the Privacy Act Review, there are a range of other reforms, legislations and regulations that Government needs to be mindful of and avoid potential scope creep, overlap and duplication. And there is a larger impact on affected stakeholders that the RIS may not fully appreciate, which is the cumulative impact of multiple forms of regulation in relation to online activities.

Without properly considering these other reforms more holistically, there will likely be similar problems as running concurrent privacy reforms as discussed above. It would also be an administratively inefficient outcome and inappropriate use of public resources if there were to be overlapping regulations and therefore overlapping responsibilities between regulators.

Given the interactions between these areas of reform, we also recommend that consideration be given to improved coordination within Government on these matters. It also raises the broader question of how these fit under the Government's various strategies including the Digital Economy Strategy, Australian Data Strategy and Cyber Security Strategy.

In addition to the issues raised in our previous submission to the Privacy Act Review regarding interrelated government activities, the next sections consider issues that have since arisen.

Ai Group recommendations:

- ***Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation.***

- ***Government should improve coordination between government agencies and departments with respect to this consultation and other interrelated reforms, legislations and regulations.***

3.1 Consumer Data Right

In our submission to Treasury on its Consumer Data Right (CDR) Strategic Assessment Consultation Paper, we suggested that it would be prudent for Treasury to consider integrating or aligning its CDR Review with the Privacy Act Review, especially as there are interrelated privacy and data protection regulation considerations.[7] This would benefit consumers and industry by ensuring a more integrated approach – as opposed to creating multiple and overlapping privacy regimes.

In this regard, we welcome the AGD's consideration of the potential overlap between the OP Code (as proposed in this Bill) and the CDR regime, with the AGD having consulted with other Government Departments on these reforms, according to the RIS.[8]

However, we would like to see more integration and coordination between Treasury and the AGD to ensure there is proper alignment of activities associated with the CDR and Privacy Act more generally. For example, as we previously raised with Treasury and the AGD, the CDR has effectively created a dual privacy regime with regulatory oversight of the CDR Privacy Safeguards by the ACCC and OAIC for sectors subject to the CDR. Such an outcome creates complexity and compliance costs for businesses that have to comply with both regimes, and also for small businesses that may not currently be subject to the Privacy Act and therefore not familiar with privacy regulatory regimes. Here, there would be benefit in reducing regulatory duplication and associated red tape.

Ai Group recommendation: Government should review the interactions between the CDR and Privacy Act more broadly with the objective of reducing regulatory duplication and red tape.

3.2 Landscape of regulatory processes relating to online activities

We note that there are several concurrent regulatory processes initiated by government agencies and departments with a focus on online activities where these processes appear to be targeting so-called digital or online platforms. However, as noted earlier, many businesses have the capability of having an online business or platform, with online services delivered via various digital media (e.g. websites, social media, apps and other digital or online platforms) which are B2C or B2B in nature, and affect businesses of all sizes. In fact, there are only low barriers to an online presence and it is common for even small businesses today to have any online presence.

For example, in addition to the proposed OP Code:

- The eSafety Commissioner is currently overseeing industry codes being developed under the *Online Safety Act 2021* (Cth);[9]
- The eSafety Commissioner is also consulting with industry on a roadmap for the introduction of mandatory age verification and the Restricted Access Systems Declaration;[10]
- The Department of Infrastructure, Transport, Regional Development and Communications is currently consulting on the Basic Online Safety Expectations;[11]
- Home Affairs has put forward a proposal for a new cyber security code under the Privacy Act as part of its Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper;[12] and

[7] Ai Group submission to Treasury (September 2021), https://www.aigroup.com.au/news/submissions/2021/treasury-consultation-paper--strategic-assessment-on-implementation-of-an-economy-wide-consumer-data-right/.
[8] AGD, RIS (October 2021), p. 25.
[9] See: https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper.
[10] See: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification; https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system.
[11] See: https://www.infrastructure.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation.
[12] Ai Group submission to Home Affairs (August 2021), https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/australian-industry-group.pdf.

- Most recently, the AGD has initiated consultation on its Exposure Draft of the Social Media (Anti-Trolling) Bill 2021.[13]

These concurrent activities suggest a lack of coordination across Government, as well as lack of appreciation of the potential negative cumulative impact that this could have for a wide range of businesses, not just for large technology companies.

To reiterate, there would be a greater benefit if there could be better coordination between all government agencies and departments in relation to multiple industry codes and regulations relating to online activities that are becoming an overcrowded landscape of regulation for a wider range of businesses.

3.3 Overlapping regulatory bodies and functions

In addition to concurrent interrelated government activities with respect to the online domain, there is a consequential risk of overlapping regulatory bodies and functions in regulating this area.

An option that has been put forward in the OP Bill is to empower the eSafety Commissioner to be an alternative complaints body to the OAIC. The rationale provided in the Explanatory Paper is to "allow information sharing to occur in the event of overlap between privacy complaints and complaints to the eSafety Commissioner – such as cyberbullying, cyber abuse and image-based abuse complaints".[14]

Another example of overlap with questionable public benefit relates to the section 52A(1)(c) of the Bill, whereby the Commissioner can require the publication or communication of a statement in those cases where there has been an interference with the privacy of an individual. This overlaps with the NDB Scheme and may cause information that is harmful to the relevant entity to be published e.g. notification of weaknesses in systems may be exploited by malicious actors if made public.

In principle, we support administrative efficiency that enables information sharing between government bodies (subject to appropriate regulatory safeguards) and reduces regulatory red tape for businesses. However, we would be concerned if the eSafety Commissioner were to be given powers that extended beyond its remit of promoting online safety and duplicating the regulatory responsibilities and functions of the OAIC with respect to privacy related matters. There should be other options explored, without necessarily expanding the eSafety Commissioner's powers that could risk creating regulatory uncertainty, overreach and duplication. It should be made clear that the eSafety Commissioner will only deal with online safety matters and the OAIC deal with privacy matters.

Further exploration of other options through proper stakeholder consultation could include assessing the merits of establishing a central regulatory body (under a central government department such as the Department of the Prime Minister and Cabinet (PM&C)) that can properly coordinate between the various regulators responsible for developing codes and regulations. This could enable a more holistic consideration including understanding the cumulative regulatory impacts and costs on affected stakeholders who may be subject to multiple regulations related to online activities. The PM&C also plays an important role, providing oversight of the Digital Economy Strategy, Australian Data Strategy and most recently Critical Technologies Blueprint and Action Plan, so this coordinating approach could be another advantage.

Ai Group recommendations:

- ***Government should explore other options to enable sharing of information between the OAIC and eSafety Commissioner to avoid regulatory duplication and overlap.***
- ***An alternative option could include establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to online activities.***

[13] See: https://www.ag.gov.au/legal-system/publications/exposure-draft-social-media-anti-trolling-bill-2021.
[14] AGD, Explanatory Paper (October 2021), p. 22.

4. Overly broad and disproportionality in scope of targeted businesses

If Government were to decide to proceed with an OP Bill, an OP Bill consistent with the Government's stated policy commitments would address services that involve trade in personal information.

In this section, we discuss various examples that have been raised by our members in which many businesses and activities could be unintentionally captured in the Bill, which should be amended if Government were to decide to proceed with an OP Bill.

4.1 Data analytics activities

The draft definitions in the OP Bill of "data brokerage service" and "large online platforms" to information collected by those services create substantial uncertainty as to coverage that includes data analytics activities where relevant information is ingested (i.e. received or "collected") in effectively anonymised form and then used to derive substantially transformed data analytics outputs, such as reports and insights, that are then made available or used only in effectively anonymised form. This would not be consistent with "trading in personal information", but nonetheless caught within the very broad proposed definitions in section 6W(3)(a) and 6W(4)(b) of the Bill.

If the Government proposes to extend coverage of the OP Bill beyond the Government's policy commitments, coverage of the OP Bill might also include providers of data brokerage services, and large online platforms, that disclose information to third parties in a form in which:

- any individual is reasonably identifiable by any direct or indirect recipient; or

- in circumstances in which any individual is reasonably identifiable by any direct or indirect recipient, having regard to other information reasonably available to that recipient i.e. having regard to likelihood of "collection" of personal information by the recipient in circumstances where there is no direct disclosure to that recipient of information in personally identifying form.

Coverage for data brokerage services and large online platforms would therefore already be consistent with the Commissioner's guidance as to operation of the current APPs in relation to disclosure and collection of personal information about individuals – which is an already expansive interpretation of current definitions in the Privacy Act – and reflects interpretation as canvassed for endorsement in the Discussion Paper.

4.2 Data brokerage services

The currently unclear and vague definition of "data brokerage service" may include more organisations or businesses than originally intended. It would appear to arguably capture organisations which do not trade in personal information, on a common understanding of such a term, and as such impose obligations on such organisations which are unintended or may be difficult or impossible to comply with. Organisations that take sufficient steps to avoid interaction with, or trading of, personal information should be exempted from being subject to the Bill.

4.3 Electronic services

The Explanatory Paper and RIS suggest that it is only aimed at "OP organisations", namely categorised as "social media services", "data brokerage services", and "large online platforms".[15] Despite this, a broad definition of "electronic service" has been used within each of these categories, which "will capture a broad range of existing and future technologies, including hardware, software, websites, mobile applications, hosting services, peer-to-peer sharing platforms, instant messaging, email, SMS and MMS, chat services, and online gaming".[16]

However, as noted above, many businesses could be captured by the OP Bill given their online capabilities, not just large technology companies. While some attempt has been made to narrow the Bill to "large online platforms", the broad inclusion of "electronic services" across the different

[15] AGD, Explanatory Paper (October 2021), pp. 6-9; AGD, RIS (October 2021), pp. 13-14.
[16] AGD, Explanatory Paper (October 2021), p. 7.

categories of organisations ensures that as many businesses are captured in the Bill. Whether or not this is Government's intention, it creates too much uncertainty for many businesses and risks potential scope creep that could inhibit business innovation and competitiveness, especially during this period of economic recovery from the pandemic.

4.4 Customer loyalty schemes

Businesses providing services that offer customer loyalty schemes that rely on data have been specifically discussed.[17] While there are some exclusions relating to such schemes in the Bill, there are also potential inclusions, which present a range of problems:

- While the Bill provides a carve-out for loyalty schemes, their inclusion muddies the waters – they are specifically noted for inclusion in the Privacy Act Review. Loyalty schemes and their extended activities (e.g. use of the data connected to the sale of goods or services) should be clearly expressed to fall outside the scope of the OP Bill and they should be considered only within the separate scope of the Privacy Act. Loyalty schemes engage with members to provide them with benefit. Given the current review of the scope of personal information in the Privacy Act Review Discussion Paper, this would allow industry to comment with greater clarity on the impact of the proposed reforms.

- The current definition of "large online platforms" lacks precision: the reference to 2.5 million end users, for example, might be expected to refer to active users only but this is not made clear. Loyalty schemes do not generally require members to provide evidence of their identity. Accordingly, any one person could hold multiple accounts e.g. in an effort to access additional offers or benefits such as may be available when they join the scheme. Where this can be detected, it would seem counterintuitive to count accounts held by one party as separate individual end users.

- The Bill does not currently make clear that all data related to loyalty scheme end users comes within scope of the carve-out in section 6W(5). Faced with the additional risk of penalties matching those under the ACL, there is a real need for clarification. It would be extremely helpful if any additional information could be provided to explain why the arbitrary figure of 2.5 million end users has been selected. As outlined earlier, this threshold should be tested.

4.5 Profiling op-out

Section 26KC(2)(h) of the Bill is directed at implementing a profiling opt-out but, as currently drafted, is able to be applied across all activities of an OP organisation. There is no basis for this broad application to the detriment of OP organisations and there would be value in determining the feasibility of entities complying with such requirements in circumstances where only limited personal information is available to them. It cannot be Government's intention that entities collect additional information to be able to comply with a request not to use or disclose an individual's personal information.

4.6 Other business online activities and technologies

Other business online activities and technologies may be inadvertently captured in the OP Bill, such as: handling high volumes of personal information online to host events or meetings; other business and customer engaging activities; use of digital technologies that includes recording data such as CRM; and embedding third party online services within the business enterprise or their products. Further clarity will be needed regarding the extent of such regular business activity that will be captured by the Bill.

4.7 Limited exemptions

The OP Bill attempts to narrow the scope by offering certain limited exemptions relating to acts or practices under a contract with the Australian Government or outside of Australia in compliance with an applicable foreign law.[18] However, we do not consider that this provides sufficient regulatory certainty to industry.

[17] AGD, Explanatory Paper (October 2021), p. 8; AGD, RIS (October 2021), pp. 13-14.
[18] AGD, Explanatory Paper (October 2021), p. 9.

In addition, the estimated cost impact on industry in the RIS presumes a narrower definition of organisations that could be subject to the OP Code, indicating that two industry bodies will participate in the Code making process.[19] If this is the case, then the scope and definition of organisations covered in the Bill should be clearly defined to reflect this cost impact assumption.

However, if it is the intention for the legislation to capture a wider range of businesses, it is important that the AGD appreciates the diversity of businesses, and therefore provide a proportionate response. This includes ensuring that the Bill takes into account the diversity of many businesses (including size and sectors) and reasonable time to enable affected businesses to meet any new requirements.

Without properly considering the scope, we consider that such legislation could create unnecessary regulatory compliance burden and costs for a wide range of businesses that would also be inconsistent with the Australian Government's deregulation agenda as noted earlier.

Each OP organisation is covered and regulated for all of their activities, not only provision of a service that led to them becoming within coverage. The only exception (outside exercise of Ministerial discretion) is in the event that section 26KC(9) of the Bill is used by the OP Code developer or the Commissioner to take out of coverage particular activities of a covered entity as specified by the Code developer or the Commissioner respectively. This leads to clear inequity as between specialist entities and diversified entities and makes it much less likely that potentially covered entities will be able to negotiate and agree on an OP Code: the range of activities that will need to be taken into consideration in drafting of an OP Code is huge. This is a disproportionate response to policy relevant concerns as articulated by the Government to date.

This also creates the likelihood that an OP Code will not be agreed upon (because of diversity of interests and concerns of potentially covered entities) and therefore that the Commissioner will determine the Code.

The OP Code should cover acts and practices in collection and handling (including disclosures) of personal information relating to personally identifiable individuals where that information is directly or indirectly derived from conduct of an activity which is a covered activity. Coverage of the OP Code in relation to each OP organisation should be related to their relevant service activities in provision of a service that brings that organisation within the coverage, and uses of data derived from those service activities, and not of other services or lines of business.

Ai Group recommendations:

- ***Subject to properly assessing the issues and underlying causes, Government should further clarify the businesses that it intends to target under the OP Bill.***
- ***Based on clearly defined targeted businesses under the OP Bill, Government should undertake a proper assessment of the impact on targeted businesses including cost-benefit assessment and other relevant implementation considerations (e.g. compliance time and assistance).***

5. Lack of consideration of other options and solutions

5.1 No options presented

Setting aside our concerns with the OP Bill, we are also concerned regarding the lack of options presented in the RIS to demonstrate that the solution offered (including the introduction of an OP Code) is the most appropriate response. This is acknowledged in the RIS where only one option has been put forward, indicating that it is to meet Government's commitment to strengthen the Privacy Act by introducing reforms to amend the Act, centred around introducing a binding OP Code and strengthening enforcement measures and penalties.[20]

[19] AGD, RIS (October 2021), p. 23.
[20] AGD, RIS (October 2021), p. 13.

We consider that good policy and regulatory practice should entail a proper consideration of various options once the problem has been properly assessed, rather than immediately leaping to one solution. This is more reason why the Privacy Act Review should take precedence and properly consulted upon.

5.2 Alternative solutions

5.2.1 Providing sufficient resources for the regulator

We are cautious with proposals to strengthen regulatory enforcement powers and penalties without a proper assessment of whether the regulator (in this case, OAIC) has the sufficient resources funded by Government to execute its functions. For instance, there may be adequate regulations in place, but the regulator may have insufficient resources. If the regulator were to be provided with sufficient resources that contributed to addressing an identified issue, then this suggests that the regulations in place are sufficient. We suggest this would be a more prudent step rather than immediately resorting to legislative amendments in the first instance.

5.2.2 Reviewing effectiveness of APPs

We noted earlier that the RIS suggests there are limitations to the APPs as a reason that would justify introducing new requirements via an OP Code. A valid question is if it were to be determined that the current APPs are limited, a prudent response would be to review whether the APPs should be amended with new requirements. This should be considered as part of the wider Privacy Act Review.

5.2.3 Providing business transition assistance

While the OP Bill heavily focuses on traditional regulatory approaches such as amending legislation, creating new regulations, and increasing enforcement powers and penalties, there lacks alternative solutions that may be more productivity enhancing and effective. For example, there is an important role that the Government or OAIC can provide through developing business uplift with respect to privacy.

Consider the NDB Scheme under the Privacy Act as an example. While the OAIC produces half-yearly reports about the Scheme, it would be useful for the OAIC to develop with industry more proactive initiatives to help mitigate such breaches occurring in the first place. The introduction of the mandatory NDB Scheme left many businesses stranded with a compliance mindset as opposed to providing them with adequate uplift support – this is likely to be an even more significant issue for SMEs. While the RIS briefly mentions about how businesses may benefit from improved OAIC education material and programs based on the OAIC's increased ability to understand emerging systemic privacy issues, it would be useful to see an industry engagement plan developed that clearly spelt out meaningful actions (including resourcing, scheduled initiatives and collaboration with key stakeholders) and measures of success. This could be co-designed with industry to develop a genuinely effective and mutual outcome that benefits the Australian community. Again, this is an example of a matter that should be considered as part of the broader Privacy Act Review.

If it were decided to proceed with an amendment to the legislation that could lead to some form of OP Code, it will be important that companies are provided with proper transition support from Government to meet these new compliance requirements. This will be especially important for companies that are not traditionally subject to these types of online activity reforms. These companies will need as much assistance as possible to ensure that they are properly accounted for. This includes Government funding and being provided a reasonable timeframe to meet any new compliance requirements. It is important to note that this is not necessarily about providing funding support for large technology businesses, but about SMEs and wider industry that may be captured under these requirements with practical uplift support. Related to this, relevant industry associations that might be required to develop industry codes should be properly identified, consulted with and appropriately supported by Government (including funding and resources) to undertake such activities.

Ai Group recommendations:

Government should explore other options to the OP Bill and these should be considered as part of the Privacy Act Review, including:

- ***Providing sufficient resources to the OAIC funded by Government in the first instance;***
- ***Reviewing the effectiveness of the APPs; and***
- ***Providing businesses with transition assistance such as an industry engagement plan for enabling business privacy capability uplift, Government funding to support business uplift, and providing industry with a reasonable timeframe to meet any new compliance requirements.***

If you would like clarification about this submission, please do not hesitate to contact me or our adviser Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,

Louise McGrath
Head of Industry Development and Policy