Australian Finance Industry Association Limited
ABN 13 000 493 907
L11 130 Pitt Street Sydney NSW 2000
02 9231 5877 www.afia.asn.au

Australian Competition and Consumer Commission
By email: platforminquiry@accc.gov.au

15 February 2019

Dear Sir/ Madam

Digital Platforms Inquiry – Preliminary Report

The Australian Finance Industry Association [AFIA] welcomes the opportunity to comment on the Digital Platform Inquiry Preliminary Report. AFIA is well placed to advocate for the finance sector given our broad and diverse membership of over 100 financiers operating in the consumer and commercial markets through the range of distribution channels (including digital access). Further background on AFIA is available through: www.afia.asn.au.

While members have contributed to the discussion, from an organisational view the position being put by AFIA may not reflect their specific position on all the issues. These will get captured through the relevant member's organisationally-targeted submission.

Financial institutions hold data about their customers, including data about individuals, which is governed by the [Cwlth] Privacy Act. AFIA has an extensive history of providing insights based on operational feedback from our members to inform privacy developments in Australia including the consumer data right (CDR) and credit reporting reforms.

AFIA notes that the Inquiry's Terms of Reference requires the ACCC to focus on digital platforms and their impact on competition in the media and advertising market. However, the Preliminary Report includes a number of recommendations (including to amend the Privacy Act) where what the ACCC has proposed appears to have an intended application far beyond just digital platforms; in particular, Preliminary Recommendation 8 (amend Privacy Act - use and collection of personal information), Preliminary Recommendation 10 (statutory tort - serious invasions of privacy) and Preliminary Recommendation 11 (imposition of pecuniary sanctions for UCT breaches) - in *Chapter 5 - Digital Platforms and Consumers.* The outcome would see AFIA members impacted. Our feedback relates to these recommendations.

The Value of Data to Create Value for Customers

Data or customers' personal information is a significant business asset for AFIA members. AFIA is keen to work with the ACCC (and other relevant regulators – including the Australian Information Commissioner) to ensure data is used appropriately by our members and the broader market, noting that data has a multitude of users. AFIA's position is that when data is used appropriately and in line with consumer consent or expectations, it has the potential to build and enhance customer relationships, and to facilitate the development of better products and services tailored to meet particular customer needs.

In this context, AFIA raises the following general concerns regarding the proposed changes outlined in the Preliminary Report:

Scope of Preliminary Report

As noted above, the Terms of Reference for this Inquiry were focused on the impact of digital platforms. However, we note that Recommendation 8 proposes to amend the Privacy Act with a potential application to all APP-regulated entities (including AFIA members). We note that the ACCC has not specifically examined the potential impacts on market segments, including finance, that may be impacted by the Recommendation beyond the digital platforms.

We note (as detailed in more detailed comments below) that the proposed changes would impact industries differently and could lead to adverse outcomes. AFIA recommends further industry consultation with relevant market segments (including the banking and financial sector) that would be impacted by Recommendation 8 (or any other with a scope beyond digital platforms) to ensure appropriateness and applicability.

Increasing Policy Fragmentation – consequences for both consumers and business

Currently, numerous reforms regarding privacy in the banking and financial sector are taking place: including the Consumer Data Right (CDR) privacy protections, privacy measures in the credit reporting system including as part of mandating comprehensive credit reporting (CCR) and the current Privacy (Credit Reporting) Code 2014 amendments. These reforms are being progressed by a number of different Government departments and agencies including the ACCC, Treasury, Attorney-General's Department, and the Office of the Australian Information Commissioner (OAIC).

These reforms are designed to implement recommendations by the Productivity Commission in its Report culminating its Inquiry into Data Availability and Use[1], but we note a key element was

[1] Productivity Commission Data Availability and Use Final Report, Chapter 5 pp 197

implementation in a cohesive and holistic way. The current approach represents a fragmented implementation with no one agency having responsibility to ensure outcomes that work together efficiently and effectively. Consumers are likely to be confused by this approach with similar types of personal data having differing protections depending on who receives it and how. Such an outcome would clearly go against what was envisaged in the Productivity Commission's Report.

There is a real risk that such a fragmented approach may potentially misalign objectives, lack coordination and consistency and be unduly onerous to apply.

AFIA recommends that a more holistic view be adopted by the Government in the implementation of its policies to facilitate the design of an implementation framework that is cohesive, holistic and future-proofed (e.g. any new obligations under the APPs be aligned with the CDR where appropriate). This should include engagement and consultation with agencies involved, particularly with the OAIC as the privacy regulator.

Feedback on the specific recommendations

More detailed comments in respect of the specific recommendations follow:

1. *Recommendation 8(a) Strengthen Notification Requirements*

We note that APP5[2] already operates to provide much of the necessary detail so that regulated entities can provide notification to their customers. The ACCC recommends that 'greater notification requirements'[3] should be *imposed*'. Members would like clarification on:

- what constitutes "express requirement"
- details and guidance on what constitutes a notification being "intelligible…written in clear and plain language (particularly if addressed to a child)".

Members are concerned with the specific details of this recommendation, specifically, the granularity proposed for 3rd party disclosure. AFIA notes that problems may arise between brevity and compliance at such a granular level. In short, longer disclosures may not improve consumer outcomes, as they can lead to customers disengaging from the notification. This is particularly relevant due to the number of relevant services consumers seek to obtain which could be accompanied by such disclosures.

[2] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information

[3] Digital Platforms Inquiry: Issues Paper,' ACCC, 26 February 2018 ('ACCC Issues Paper'), pp 226.

2. *Recommendation 8(b) Introduce an Independent Third-Party Certification Scheme*

AFIA Members already comply with a large number of privacy obligations including the Privacy Act, relevant AFCA decisions and OAIC guidance. Given that compliance with various regulatory bodies and related policies exist, it is unclear whether the establishment of an independent 3rd party certification mechanism would bring benefits for consumers. Further detail regarding the problem the ACCC is trying to solve with this recommendation would greatly assist our understanding and facilitate design of a solution that achieves the objective minimising unnecessary additional compliance obligations.

Members are also concerned about how this would work in practice. AFIA requests that before moving further with the proposals, the ACCC clarify:

- the definition of 'identified objective threshold' to identify which APP entities require 3rd party certification;
- eligibility requirements, supervision and monitoring process of certification bodies; and
- validity period of data protection seal or mark.

We note that such an accreditation scheme would result in large additional costs for the Government (i.e. OAIC funding, training of certifiers, logistics and details) and for certified entities.

3. *Recommendation 8(c) Strengthen consent requirements*

AFIA notes the importance of ensuring appropriate consent for the collection of data. However, we are concerned that this recommendation will result in information overload for customers, leading to disengagement (e.g. consumers just ticking 'agree' to quickly access the relevant service). While an important goal should be to minimise information asymmetry between the consumer and entity, an exhaustive list may make it impractical and may not lead to improvements in outcomes for consumers.

With the CDR being progressed, AFIA notes that these recommendations should be aligned as these were developed for an online environment and will ensure there is a consistent experience for consumers under both regimes. We note some regulatory regimes (such as GDPR) are moving towards accountability on the entity to handle data appropriately – rather than relying on informed consent. This approach should be considered by the ACCC as it may bring greater protections and benefits for consumers.

Further, our Members have indicated that clarification would be needed on the following aspects of this draft recommendation:

- how should an entity gauge an individual's 'capacity to understand and communicate consent' [4] when online, given the lack of face-to-face interaction
- course/s of action when an institution's processes that handle personal information don't have the flexibility to be granular in their opt-in/opt-out consent (i.e. inherent system limitations).

4. *Recommendation 8(d) Enable the erasure of personal information*

Many organisations, especially those in financial services, have legal obligations to hold personal information for specific periods of time, such as under AML/CTF requirements, responsible lending and other laws. Organisations also need to hold data for audit and legal proceedings. Any recommendation for the erasure of data needs to have a caveat to allow organisations to keep certain personal information for lawful purposes such as these.

AFIA also notes that there are existing obligations (APPs 11, 12 and 13) that collectively mean that:

- organisations are obliged to delete data where it is no longer being held for the purposes it was collected; and
- consumers have the right to access and correct information held.

The proposed obligation to delete all user data (which exceeds existing obligations) would also be very complex to apply in practice. Modern systems, that are cross-linked across various databases and create numerous backups, make it nearly impossible to completely remove user data. AFIA members raise concerns on what an acceptable extent of deletion is, and its possible disruptive effect in maintaining database integrity where individuals have been de-identified.

For customer complaints and disputes, records are kept for investigation and satisfactory resolution. Any reform in this area should consider that, while deletion of user data may initially serve the customer's interest or instruction, continuity of services may be more difficult without previous user records. In the same vein, customers may not fully reap benefits that long-term clients receive if there are no historic records available to give context.

AFIA recommends that entities be able to outline to a customer the reasons why the data needs to be kept in situations outlined above (including examples of responsible lending, AML/CTF requirement, other laws) and retain the data. Should customers request deletion, 'reasonable steps' may be taken to remove the data; but what is 'reasonable' will depend on the particular circumstances.

[4] Digital Platforms Inquiry: Issues Paper,' ACCC, 26 February 2018 ('ACCC Issues Paper'), pp 230.

5. *Recommendation 8(e) Increase the penalties for breach*

AFIA notes that the ACCC proposal would be a significant increase in penalties for breach. A higher penalty does not always equate to stricter compliance and may in fact discourage public notification to avoid hefty penalties. AFIA views that penalties should be reasonable and tied to the type of data breach. Members have noted that clarification would be required on the categories of breaches, especially on what constitutes a '*serious*' or '*repeated interferences of privacy*'.

Members have also pointed out that OAIC's Notifiable Breaches scheme [5] is already in place and encourages entities to come forward and rectify breaches. ACCC should thus consider that penalising is likely to reduce the effectiveness of the notifiable data breach scheme.

6. *Recommendation 8(f) Introduce direct rights of action for individuals and recommendation 10 statutory tort - serious invasions of privacy*

In AFIA's view, current laws in Australia (eg Privacy Act) and avenues for complaint (eg for our Members – EDR via AFCA) are sufficient to address possible courses of actions by customers. In line with recommendations proposed by Commissioner Hayne in his Final Report, in preference to adding to the complexity by imposing additional regulation, a better approach would be to simplify the law to achieve the underlying consumer protection objective and for regulators to enforce those laws.

7. *Recommendation 11 – Pecuniary Penalties - UCT provision - breaches*

AFIA notes that the question of potential inclusion of sanctions was specifically considered as part of Treasury's review of the small business UCT provisions in November/December last year. We understand Treasury is reviewing submissions, including from AFIA (and we assume the ACCC), to formulate a recommendation to be considered by the Government on whether sanctions are warranted for inclusion. AFIA submits that any recommendation proposed by the ACCC should reflect the outcome of Treasury's consultation rather than proposing a view that may appears premature and may be at odds with Treasury's recommendation to the Government.

[5] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Next steps

Should you wish to discuss our feedback further, or require additional information, please contact me at helen@afia.asn.au or Alex Thrift, Economic & Senior Policy Adviser at alex@afia.asn.au or both via 02 9231 5877.

Kind regards

Helen Gordon
Chief Executive Officer