

24 January 2022

Ms Amy Jarvoll  
Director, Information Law Unit  
Attorney-General's Department  
Email: [OnlinePrivacyBill@ag.gov.au](mailto:OnlinePrivacyBill@ag.gov.au)

## ONLINE PRIVACY BILL EXPOSURE DRAFT – REQUEST FOR ADDITIONAL FEEDBACK

The Australian Finance Industry Association (AFIA) welcomes the opportunity to provide additional feedback to the Attorney-General's Department's (AGD) consultation on the Online Privacy Bill Exposure Draft.

AFIA is a leading advocate for the Australian financial services industry and represents over 110 providers of consumer, commercial and wholesale finance across Australia including banks, finance companies, fleet and car rental companies, fintech lenders and BNPL providers who are at the forefront of financial innovation in Australia.

We believe that our industry can best support Australia's economy by promoting choice in and access to consumer and business finance, driving competition and innovation in financial services, and supporting greater financial, and therefore social, participation across our community.

## SUBMISSION

On 13 December 2021, AFIA was one of four signatories to a joint industry submission alongside the Australian Banking Association (ABA), Financial Services Council (FSC), and the Insurance Council of Australia (ICA).

We appreciate the opportunity to represent our members' views at an association level. As noted in the joint submission, we believe the Exposure Draft stage of the policy development process is not an appropriate stage for detailed examination of these issues and we welcome this opportunity for further consideration now. It will be critical to ensure any changes to the privacy laws protect consumers and do not inadvertently impact the provision of financial services in Australia.

## Expansion of the Digital Platforms Inquiry recommendations

AFIA stands by the collective view in the joint submission, being that the Exposure Draft represents a significant expansion on the recommendations of the Australian Competition and Consumer Commission (ACCC) Digital Platforms Inquiry Final Report (the DPI).

We also remain of the view that there may be adverse and unintended consequences arising out of this expansion in scope, particularly in relation to the definition of 'large online platform'.

The terms of reference considered by the DPI included “all digital platforms supplying online search, social media and content aggregation services”.<sup>1</sup> The Final Report provided more detail on the scope of the ACCC’s considerations, again making clear that the inquiry was focused on a relatively narrow set of entities, as did our discussion with you on 18 January 2022.

The Exposure Draft would substantially expand the application of the Online Privacy Code (OP Code) to specifically reference and define ‘large online platforms’. The two requirements would be that the entity:

- *collects personal information about an individual in the course of or in connection with providing access to information, goods or services (other than a data brokerage service) by use of an electronic service (other than a social media service); and*
- *has over 2,500,000 end-users in Australia in the past year, or if an organisation did not carry on business in the previous year, 2,500,000 end-users in the current year.*

While the Explanatory Paper cites the examples of Apple, Google, Amazon, and Spotify,<sup>2</sup> the term ‘large online platform’ would clearly capture a much broader range of entities on the above definition. It could extend to many of our members now or in the future, in particular banks and ‘neo-banks’, online small business financiers, and Buy Now Pay Later providers, which offer their products through various technology-enabled channels, partnerships and platforms.

### Support for consumer privacy safeguards

AFIA strongly supports consumer privacy safeguards. These safeguards should be applied consistently across all organisations that seek to collect consumer data. Therefore, we believe the OP Code should be constructed from the perspective of what makes sense to a consumer. In other words, it is important not to create unnecessary complexity for consumers and the application of the data standards in the OP Code should be consistent across all entities regardless of their size or the nature of their business or the products and services they supply.

Consumers will already find it difficult to navigate the complexity and interaction of the current privacy laws and regulations. The proposed fairness and reasonableness requirements, coupled with a high level of transparency required as to disclosures, will provide the desired consumer protections.

However, AFIA does not support using the OP Code to regulate the business activities of large online platforms or other entities in any way other than for the specific principle of consumer privacy safeguards consistent with existing and proposed privacy principles and legislation. Furthermore, while we appreciate the intent of the proposed changes to the privacy laws, we are specifically concerned with the potential for the proposed changes to significantly impact on competition and innovation in the financial services industry and for financial services providers to be caught up in the definition either because they have more than 2,500,000 customers (end users) or because of their use of data and technology to deliver product innovations and service solutions to their customers.

Many of our members currently have more than 2,500,000 customers on their technology-enabled channels and platforms. They collect personal and financial information in order to tailor and provide financial products and services to their customers and to assist their customers manage their finances and money, including through customer-centric account alerts, etc. Data and technology is core to the provision of financial services – customer data is regularly relied on

---

<sup>1</sup> ACCC (Dec 2017) Digital Platforms Inquiry: Terms of Reference ([link](#))

<sup>2</sup> Attorney-General’s Department (Oct 2021) Explanatory Paper: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, ([link](#)) 8

in the design, distribution, compliance, and management of financial products and services across all business models. Additionally, using a definition of 'large online platform' that relates to numbers of customers or end users is problematic because it discourages organisations from innovating to achieve scale, which would enable them to provide those scale benefits to consumers in the form of expanded product and service offerings and/or reduced prices.

AFIA promotes choice in and access to consumer and business finance, driving competition and innovation in financial services, and supporting greater financial, and therefore social, participation across our community.

Financial products and services being offered by 'large online platforms' may serve to promote access to, and choice in, new offers and in doing so will encourage innovation and promote competition. However, any entity offering financial products and services should be regulated under our existing legal and regulatory framework relating to these activities, alongside any other financial services provider, including financial services laws, the ASIC Act, APRA standards if they are an Authorised-Deposit Taking Institution (ADI) and the payments rules administered by the Reserve Bank of Australia.

All entities providing financial products and services must also be required to abide by the existing privacy laws, including the National Privacy Principles, and comply with various standards on consumer data, including the Open Banking regime and the Consumer Data Right. These laws exist to ensure consumer safeguards are in place and financial system stability is maintained.

### **AFIA Proposed Approach**

Should the ultimate objective be ensuring consumer data is not collected for one purpose (search or social media) and used for another (provision of financial services), and this is not already adequately mitigated in existing laws, then AFIA supports repeating and clarifying those requirements in the OP Code.

#### Definition

Therefore, a definition that might help satisfy this objective would be to limit the use of data collected by 'large online platforms' to the provision of services by that platform directly, and remove the ability to transfer or share or sell any data collected in the provision of that original product or service – without informed consumer consent – to any third party application or services provider that sits on the platform and which provides additional or add-on products or services and is not licensed to provide those products or services (i.e. as a financial services provider). This would also be the case in a situation where the third party application or services provider is wholly or majority owned by the large online platform, if it is operating under a different brand name. and has the appearance of being a separate entity.

This approach means that third parties who develop products or services that sit on top of a platform, or are connected to a platform, should be required to collect consent specific to their usage directly from individuals/end users – under the CDR privacy and consent regime or if they do not participate in the regime, in a manner that achieves the same data privacy standards and compliance required by financial services providers.

#### Carve-out

Financial institutions already operate within a heavily regulated and legally complex environment, with legal and regulatory complexity in the finance sector significantly increasing over the past few years, including the new rules for capture, use and transfer of consumer data. Specifically,

these new rules impose consumer safeguards and ensure data is managed appropriately for financial service providers.

AFIA notes that the main concern identified in the DPI was the lack of effective regulatory frameworks for some of the activities of large online platforms not otherwise regulated.

The Explanatory Paper accompanying the Exposure Draft does not provide any information regarding how the proposals would interact with existing regulatory obligations, compliance requirements and customer protections already required of entities already regulated (i.e. financial services providers). Specifically, it is unclear how the proposals would interact with requirements under the Open Banking regime and the Consumer Data Right. We continue to maintain there has not been any sustained examination of:

- a) how the measures in the OP Code would interact with existing complex legal and regulatory requirements
- b) whether a policy rationale exists at all for extending the recommendations in this way (given the absence of any identified or known gaps in the privacy practices of the financial institutions already regulated under other laws and frameworks sector or any examination/investigation into the finance sector's data handling practices), and
- c) how the OP Code would impact the complex and varied arrangements through which financial products, services and technologies are provided to customers, including arrangements or platforms through which authorised deposit-taking institutions, insurers and financial services licensees make the products and services for which they are licenses available to third party partners which in turn distribute products and services to their customers.

The financial services industry itself is diverse – there are a broad range of business models enabling customers to choose the right product or service for them depending on their financial needs and personal preferences. We believe any approach to the regulation of large online platforms should be introduced without inadvertently impeding innovation and competition in financial services.

Therefore, if the definition is to be included it warrants specific clarity for financial service providers, and we recommend a carve-out that should cover “licenced or registered financial institutions, being those that are Australian financial services licensees, Australian credit licensees, authorised deposit-taking institutions, restricted authorised deposit-taking institutions, registered financial corporations, and providers of purchased payment facilities.”

This approach would mean financial services providers regulated under existing financial services, credit and payments laws and regimes administered by ASIC, APRA and the RBA would not be required to meet the rules applied to ‘large online platforms’, recognising that these entities are already regulated and required to meet various data privacy standards and compliance requirements.

It is important not to create unnecessary legal complexity and regulatory duplication for financial services providers and/or stifle the legitimate activities of financial services providers, which could result in less innovation and competition in the market, prevent transition to our digital economy, and/or cause consumer harm, where consumer data is unable to be appropriately used.

## CLOSING REMARKS

The OP Code should be constructed in a way that puts the customer in the centre and considers the benefits of access to innovation and choice as well as the clarity and consistency of a privacy framework across all organisations with whom they share data and information.

This approach would be consistent with the Federal Government's various economic policies and strategies seeking to balance customer choice and consumer safeguards with innovation and competition as well as to create Australia as a financial and technology centre. This would also allow for the development and introduction of new products and services in manner that ensures consumers are appropriately protected, while providing customers with access to and choice in technology, product innovations, and service solutions.

AFIA looks forward to working with the Attorney-General's Department and contributing further information and data to support the creation of policy and regulatory settings that keep pace with evolving industry developments and customer expectations, strengthening our economic recovery, and supporting the shift to a digitised economy.

We hope our submission assists the Attorney-General's Department with its consideration of the most practical and effective model to safeguard consumer privacy and promote choice, competition and innovation. I would welcome the opportunity to provide further information if that would be helpful.

If you would like to discuss our feedback further or require any additional information, please contact me at [diane.tate@afia.asn.au](mailto:diane.tate@afia.asn.au) or Anna Fitzgerald, Acting Communications Director at [anna.fitzgerald@afia.asn.au](mailto:anna.fitzgerald@afia.asn.au).

Yours sincerely

Diane Tate  
**Chief Executive Officer**