Australian Banking Association

6 December 2021

Ms Amy Jarvoll

Online Privacy Bill

Attorney-General's Department

By email: OnlinePrivacyBill@ag.gov.au

Dear Amy

Online Privacy Bill Consultation

The Australian Banking Association (**ABA**) is pleased to make this submission to the Attorney-General's Department consultation on the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (**the Bill**).

The Bill enables the development of an Online Privacy Code (**OP Code**), enhances the enforcement and information gathering powers of the Office of the Australian Information Commissioner (**OAIC**) and significantly increase the penalties applicable to serious or repeated interferences with an individual's privacy. As the Bill is currently drafted, the OP Code may apply to banks' online product distribution and servicing channels and banking apps. Such an outcome would go far beyond the recommendation of the Australian Competition and Consumer Commission (**ACCC**) in its Digital Platforms Inquiry (**the Inquiry**) Final Report. The application of the OP Code to the banking sector is neither necessary nor appropriate given the heavily regulated, and complex, environment in which banks operate.

The ABA strongly recommends the Bill be amended to apply the OP Code more clearly and narrowly to the digital platforms on which the Inquiry focussed and the banking sector be expressly excluded from the definition of OP Organisations. The annexure provides detail in support of the recommendation. Additionally, in part two of the annexure we make suggestions in relation to the OP Code development, the OP Code scope and drafting matters relating to the Bill.

I would be pleased to provide further details should it be required. The ABA would also appreciate the opportunity to further engage with the Attorney-General's Department on the scope of the exemption for banking and financial services.

Kind regards,

Emma Penzo

Policy Director

The ABA's mission is to support our member banks to build a strong, stable, and trusted banking system, to grow the Australian economy and build the financial well-being of all Australians.

Australian Banking Association

ANNEXURE

1. Application of the Online Privacy Code to banks

1.1 Issue statement

The *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (**the Bill**) establishes a framework for the development of a binding Online Privacy Code (**OP Code**). As drafted, the Bill may have the effect of making the OP Code applicable to banks' online product distribution and servicing channels and banking apps (**Bank Digital Platforms**) as:

- 'Organisations providing data brokerage services'[1]
- 'Large online platforms'[2].

Such an outcome would go far beyond the recommendation of the Australian Competition and Consumer Commission (**ACCC**) in its Digital Platforms Inquiry (**the Inquiry**) Final Report to develop an enforceable privacy code for online search, social media, and content aggregation services. It would also not be necessary or appropriate given the heavily regulated, and complex, environment in which banks operate.

1.2 Rationale

1.2.1 Digital Platforms Inquiry Final Report Scope

The ACCC's recommendation for an OP Code, set out in the *Digital Platforms Inquiry Final Report*[3] (**DPI Report**) was targeted at 'all digital platforms supplying online search, social media, and content aggregation services to Australian consumers'[4]. Other online platforms, including Bank Digital Platforms, were not the subject of the Inquiry or the recommendation. The ACCC did not identify any special privacy risks relating to digital banking.

The objective of the ACCC's recommendation was to 'establish a Privacy Code applying specifically to digital platforms that process a large volume of Australian consumers' personal information, to proactively target concerning data practices of digital platforms identified in this Inquiry'[5] [6].

The digital platforms identified in the Inquiry were defined as 'digital search engines, social media platforms and other digital content aggregation platforms' (**Targeted Digital Platforms**)[7]. Examples of the platforms provided in the Inquiry's final report included Google, Bing, Yahoo!, DuckDuckGo (search engines), Facebook, Instagram, Snapchat (social media platforms), and Google News, Apple News and Flipboard (digital content aggregation platforms). Bank Digital Platforms were not included.

In December 2019, the government reconfirmed its March 2019 policy statement with an in-principle support of the DPI Report's recommendation for the introduction of an OP Code for Targeted Digital Platforms (Recommendation 18). The government response noted an action to 'draft legislation to amend the Privacy Act, including to introduce a binding privacy code that would apply to social media

[1] Under clause 6W (3) of the Bill. The definition of data broker is currently broad enough to capture online brokers of securities and other financial transactions, given they are effectively facilitating the exchange of information (e.g., purchase / sale price, HIN / SRN, and other personal information for inclusion on share registers etc.) between the ASX, market participants, listed companies, and buyers / sellers of securities. The definition of data broker also appears to capture a bank's provision of a good or service to a consumer (for example a personal financial management or budgeting tool) as an Accredited Data Recipient under the CDR Regime.
[2] Under clause 6W(4) of the Bill.
[3] Australian Competition & Consumer Commission (2019) Digital Platforms Inquiry Final Report (June) link.
[4] DPI Report page 36
[5] DPI Report page 454
[6] For further context, we note that this recommendation was initially made in the Digital Platforms Inquiry Preliminary Report in December 2018 (Refer to Digital Platforms Inquiry Preliminary Report, December 2018, recommendation 9 link) and that in March 2019, in response to this preliminary report, the government announced its policy to include 'legislative amendments which will result in a code for social media and online platforms which trade in personal information (refer to The Hon. Christian Porter MP Attorney General and Senator the Hon. Mitch Fifield, Minister for Communications, Joint Media Release, 24 March 2019 link).
[7] DPI Report pages 41, 616

platforms and other online platforms that trade in personal information'[8] In this response, the government did not extend the scope of the ACCC's recommendation, and it did not identify other types of digital platforms beyond Targeted Digital Platforms as additional platforms of concern[9].

Further the Online Privacy Bill Explanatory Paper (**the EP**) has not referenced the potential expanded scope listing several examples of the services intending to be covered by the Bill, including Apple, Amazon, Spotify, WhatsApp and several of the services listed above but does not mention Bank Digital Platforms.

As noted by the DPI report, the 'trading of personal information' through the harvesting of people's data as they interact with the online platform is foundational to the business models of Targeted Digital Platforms and their ability to generate revenue. Banks offer substantially different services to the Targeted Digital Platforms through Banks' Digital Platforms.

The potential application of an OP Code to the banking sector would therefore represent a change in government policy, hitherto uncommunicated. Further, unlike those identified for Targeted Digital Platforms, it is unclear what specific issues within banking the OP Code would be addressing.

1.2.2 Banks operate in a highly regulated environment

Banks are <u>required</u> to collect and use personal information

Banks offer substantially different services to Targeted Digital Platforms, and operate in a different, heavily regulated environment. For example, banks, unlike Targeted Digital Platforms, are required to:

- Collect and use personal information to fulfil 'Know Your Client' (**KYC**) obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* (**AML/CTF Act**) in order to provide a banking service;
- hold an Australian Financial Services License (**AFSL**) to provide financial product advice to customers. AFSL holders 'have a general obligation to provide efficient, honest, and fair financial services'[10] and the collection and handling of personal information forms an integral part of how those financial services are delivered[11]; and
- manage consumer credit information in accordance with the requirements of the credit reporting scheme in Part IIIA of the Privacy Act 1988 (Cth) (**Privacy Act**) and the Privacy (Credit Reporting) Code.

Banks collect, use, disclose information to <u>support</u> compliance with laws, regulations, codes

Banks also collect, use, and disclose information in accordance with and to support their compliance with other laws, regulations, and codes. For example:

- to fulfil requirements of the Banking Code of Practice (**BCOP**) to employ a range of practices that can identify common indicators of financial difficulty and take 'extra care' with customers experiencing vulnerability[12];
- to make inquiries and take verification steps sufficient to comply with responsible lending obligations under the National Consumer Credit and Protection Act 2009 (Cth) (**NCCP Act**);
- to conduct essential business processes, such as credit risk analysis, complaints handling, investigations under the ePayments Code or scheme rules, the handling of customer data in

[8] Treasury, 2019, Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 12 December 2019 p18 Link
[9] That the government response to recommendation 18 was specific to Targeted Digital Platforms is evident from its response to recommendation 17 which indicated that consumer data protection in respect of broader online services would be considered in the review of the Privacy Act (Treasury, 2019, Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 12 December 2019 p18)
[10] https://asic.gov.au/for-finance-professionals/afs-licensees/afs-licensee-obligations/
[11] ASIC Regulatory Guide RG166
[12] The BCOP, which forms part of the broader financial services consumer protection framework, and which includes commitments to protect customers' privacy and confidentiality. The BCOP also forms part of the terms and conditions that govern the banking products and services customers acquire from banks. The BCOP is an Approved Code under ASIC's Regulatory Guide RG183 which requires periodic review and approval by ASIC

connection with the New Payments Platform Scheme, remediation of errors or mistakes in accordance with the law and contractual obligations;

- in compliance with the banker duty of confidentiality which is an implied term in contracts between banks and their customers;
- to fulfil the record-keeping requirements of the AML/CTF Act, NCCP Act and other laws; and
- to comply with the Consumer Data Right legislative regime, which includes extensive rules around the handling of consumer banking data.

Other proposed legislation may also impact on requirements on banks' collection, use, and disclosure of personal information. For example, the proposed digital identity regulation will introduce a new, scheme-specific regulatory regime governing the handling of individuals' personal information.

Banks are required to store data securely

Banks are subject to existing obligations relating to the security of customer data in addition to those that apply to other entities *and* have mature processes to comply with these. Unlike Targeted Digital Platforms, banks must protect information in accordance with Australian Prudential Regulation Authority's standard CPS 234 Information Security.

Banks maintain mature customer grievance processes

Unlike the Targeted Digital Platforms, in addition to the Office of the Australian Information Commissioner's (OAIC's) complaints channel, banking consumers have at their disposal other legislated dispute resolution schemes for raising grievances and seeking redress where they believe their personal information has been collected, used, disclosed, or otherwise handled improperly:

- Privacy-related complaints can be heard by the Australian Financial Complaints Authority (AFCA); and
- Banks are also required establish and maintain internal dispute resolution systems that meets the Australian Securities and Investments Commission's (ASIC's) standards and requirements, as set out in ASIC's Regulatory Guide 267.

Additionally, the BCOP includes commitments in relation to the protection of customers' privacy and confidentiality. Breaches of bank duties in relation to privacy and confidentiality may be reported to the Banking Code Compliance Committee (BCCC), giving the BCCC visibility of potential industry level issues pertaining to data handling practices in relation to banking customers.

OP Code interaction with bank obligations

Finally, we note that, except for the Consumer Data Right, the EP did not expand upon how the OP Code would interact with the significant obligations with which banks already comply. For example, the proposal for the OP Code to include specific age requirements for consent may lead to adverse outcomes for young people regarding access to banking, and it does not reflect the banking sector's mature processes for onboarding minors to banking products.

To the extent that banks are subject to any new OP Code, the code would need to be carefully crafted to avoid potential conflicts or potential degradations of existing consumer protections in the broad range of regulatory and other legal obligations that banks must comply with.

It is the ABA's view that to introduce an OP Code to the already heavily regulated banking sector risks creating further complexity to bank operations and is an instance of overregulation, without justification or sufficient evidence to suggest that this is warranted.

1.2.3 Privacy Act Review

The ongoing Privacy Act review includes an expansive set of reform proposals that, if implemented, could significantly impact how any OP Code would operate, requiring it to be substantially revised, possibly even before it is launched. Proposed reform areas of the Privacy Act which may impact on the requirements of the OP Code include:

- Notices and consent (proposal 8 and 9);
- A right to object or withdraw consent to the collection, use or disclosure of personal information (proposal 14); and
- Children and vulnerable groups (proposal 13).

Some matters under review could have significant ramifications for banking, including any changes to the definition of 'sensitive information' to include financial information. This could require a reconfiguring of the way in which personal information is managed by banks.

It would be impractical and potentially confusing for customers for these operational changes to be made following both the release of the OP Code and the completion of the Privacy Act Review. Rather, any OP Code should be drafted to be consistent with the outcomes of the Privacy Act Review. This would allow any operational changes to be implemented at one time, and would provide customers with a clearer, simpler, more streamlined change experience.

A tactical solution may be appropriate to address the specific privacy risks identified by the ACCC relating to Targeted Digital Platforms prior to the completion of the Privacy Act review. A long-term solution dealing with broader privacy risks would, however, be better dealt with as part of the full Privacy Act review. This approach also aligns with the 2019 government response as noted in section 1.2.1.

1.2.4 Current exceptions are limited

The Bill includes an exception from the definition of 'electronic service' for services with the sole purpose of processing payments or providing access to a payments system[13]. We support this exception given the nature of payments systems in providing critical customer services. We also note that payment systems operate closely with banking platforms. For example: mortgage loan accounts offer deposit and redraw features; deposit accounts hold the funds from which or to which transactions are processed. The exception as currently drafted does not provide sufficient scope for banking and financial services as a whole to be exempted, despite the interdependence of banking and financial service to payments systems.

1.2.5 OP Code application to banks could undermine existing consumer protections

In contrast to Targeted Digital Platforms, banks provide consumers with access to goods and services through both online *and* offline channels (including through branches, and business centres). If the OP Code were to apply to Banks' Digital Platforms, banks would be required to manage the personal information of customers differently depending on whether the information was collected through an online or offline channel. Further, the OP Code would afford customers different rights in respect of their personal information – customers whose personal information had been collected through an online banking channel would have the right to request that the bank not use or disclose their personal information under the OP Code. However, no such right would be available to customers whose personal information has been collected solely through offline channels. The different treatment of customer information could result in confusion for customers, and the varying privacy rights could lead to allegations of unfairness.

[13] Clauses 6X(2)(c) and 6X(2)(d).

1.3 Recommendation

The application of the OP Bill to the banking sector will add significant complexity for banks and potential confusion for banking customers. Especially when considering the implications of overlaying the requirements of the OP Bill on existing banking laws, regulations, and codes.

The ABA strongly recommends that:

- the Bill be amended to apply the OP Code more clearly and narrowly to the Targeted Digital Platforms described at 1.2.1 of this submission and
- the banking sector be expressly excluded from the definition of OP Organisations. This could be done in the same way that loyalty schemes have been excluded for example by reference to excluding entities that hold an Authorised Deposit-taking Institution license, or an Australian Financial Services License, or Australian Credit License and in respect of all their banking and financial services activities.

The ABA would appreciate the opportunity to further engage with the Attorney-General's Department on the scope of the exemption.

2. Other matters

The ABA's view is that, to the extent Bank Digital Platforms are to be subject to the OP Code, the matters noted in this section should be considered.

2.1 OP Code scope

A consequence of a potential expansion of the types of digital platforms subject to the OP Code beyond the Targeted Digital Platforms is that it will likely necessitate a broadly drafted and broadly applicable OP Code. This may reduce the effectiveness of the OP Code in mitigating the specific privacy risks identified by the ACCC. For example, when making its recommendation for an OP Code, the ACCC referred to Google 'auto-delete controls' that enable customers to request automatic deletion of data in advance[14]. Such a control could not be used by a bank, which is often legally required to retain customer data (see section 1.2.2). It could not, therefore, be required by a broadly drafted and applicable OP Code. Standard definitions proposed by the ACCC[15] would also need to be drafted broadly.

2.2 OP Code development

We note the OP Code development schedule may be underestimated based on the following challenges and insights:

(1) Identifying an appropriate code developer.

The Australian Information Commissioner will be required to ensure appropriate expertise is available for the development of the OP Code. This will be challenging given the breadth of organisations that may be covered by the OP Code.

The Regulatory Impact Statement of the Bill (**the Statement**) states that one or two industry bodies will be involved in the code-making process as the OP Code developer. The Statement notes that the Commissioner, in selecting these bodies, will consider whether they are 'generally representative of the social media and online platform industry'.

It is not clear what the meaning of the 'online platform industry' is, or what kind of body would be 'generally representative' of it and the social media industry. It is unlikely that any such

[14] DPI Report page 428
[15] DPI Report page 487

industry body would be well placed to develop a code that regulates banks (or entities in other financial sector industries or even other established industries).

(2) OP Code is unlikely to be finalised in 12 months.

The ABA notes that the Credit Code review will be 18 months to finalisation, and this exercise is only a partial rewrite of the Credit Code. The OP Code will be new and, in its proposed form, is expected to cover disparate sectors with online platforms with different business models and varying maturities in respect to the management of customer personal information.

2.3 Bill drafting

The ABA suggests the following amendments to the Bill for improvements to the application and operation of the OP Code:

- ***Transition period:*** To enable in-scope entities to make any necessary changes to policies, notices, systems, and procedures in compliance with the OP Code the commencement of the Bill and OP Code must provide for a reasonable transition period following registration of the final form of the OP Code. The ABA suggests an 18-month transition period from the date on which the final version of the OP Code is approved by the Australian Information Commissioner.
- ***Digital platforms as a tool of business:*** Many entities deploy digital platforms such as Microsoft Teams to facilitate staff interaction in a business context. The ABA suggests the definition of social media service expressly exclude entity usage of such platforms for staff interactions.
- ***Banking*-as-a-service**: Banks may have banking-as-a-service arrangements with third parties, which in turn distribute banking products and services to their customers. To the extent the Bill and OP Code would apply to the banking sector, clarity is needed as to whether customers are "end-users" of those third parties (for the purposes of determining whether they are a large online platform), or only the bank that issues the products.
- ***Definition of Data Broker:*** The definition of data broker could capture credit reporting bodies that collect, use, disclose and otherwise manage consumer credit information in accordance with Part IIIA of the Privacy Act and the Privacy (Credit Reporting) Code. The ABA assumes these bodies are not intended to be captured by the Bill and recommends the definition be redrafted to expressly exclude these entities when acting in their capacity as a credit reporting body within the meaning of the Privacy Act.
- ***Definition of Large online platform:*** The definition of large online platform at clause 6W is unclear and, in particular, the relationship between the 2.5 million end-user threshold at clause 6W(a), and the criterion at clause 6W(b), namely the collection of personal information in the course of, or in connection with, providing access to information, goods or services, by the use of an electronic service. In the case of an organisation that provides more than one electronic service, it is unclear whether the 2.5 million end-user threshold should be applied to each of the platforms singly, or cumulatively to all platforms provided by the organisation. If it is the latter, then it is possible the OP Code may apply to platforms that have comparatively few end-users.
- ***Information derived from personal information***: The definition of data brokerage service lacks clarity in relation to the meaning of the words 'information derived from the personal information' at clause 6W(3)(b)(ii). It is not clear whether the derived information must also be personal information, or whether it would also include de-identified personal information.
- ***End-user:*** That the definition of 'end-user' be provided in the Bill to provide certainty as to when/if an organisation meets the 2.5 million end-user threshold.
- ***APP5:*** We note the OAIC's recommendation for a balance between strengthening notice requirements and minimising potential consumer consent fatigue in the OAICs submission to the Privacy Act Review Issue Paper. We suggest the Bill expressly require the OP Code to give due consideration to this balance when considering notification requirements under APP5.

- ***Request not to use or disclose personal information:*** As discussed above at 1.2.5, the provision of a new right for customers to request an OP organisation not to use or disclose their personal information would not be available to customers who engaged with banks in offline channels. Further, the exercise of any such right would need to be subject to clear and well-defined exceptions that would allow banks to refuse to comply with a request (whether in whole or in part) if the further use or disclosure of the relevant information were (i) required to allow banks to comply with their regulatory obligations; or (ii) reasonably necessary for banks' functions or activities. For example:
    - where use or disclosure of the personal information is reasonably necessary for a credit provider to comply with its responsible lending obligations;
    - where the personal information is used and disclosed for the purposes of preventing financial crime, or for customer remediation purposes.