Australian Banking Association

18 January 2019

Manager
Consumer Data Right Team
Structural Reform Group
The Treasury
Langton Crescent
Parkes ACT 2600

Via email: data@treasury.gov.au

Dear Manager

ABA Response to Treasury: Privacy Impact Assessment – Consumer Data Right – December 2018

The Australian Banking Association (**ABA**) appreciates the opportunity to provide comments on Treasury's: Privacy Impact Assessment – Consumer Data Right - December 2018.

With the active participation of its members, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and community and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The Consumer Data Right (**CDR**) offers an opportunity for consumers to use data to assess banking products and access new services. It is important that the CDR appropriately balances efficiency in the transfer of data and the risks to consumers' privacy. The Privacy Impact Assessment (**PIA**) is an important step in achieving this balance.

The ABA appreciates the comprehensiveness of the PIA produced by Treasury. Assessing the risks to privacy associated with the CDR is a very complex task and the PIA represents a significant effort in understanding these risks and how they may be mitigated. The ABA supports the recommendations of the PIA to ensure the risk mitigation strategies outlined work as they are intended.

The ABA understands that this PIA will continue to be expanded and refined as consumer testing occurs and further details are settled and incorporated into the consumer data rules (**Rules**) and standards (**Standards**) prior to the launch of access to consumer data in February 2020. The Rules and Standards will have a material impact on the risks arising from the framework, and the ABA remains keen to continue to work collaboratively with Treasury to refine the PIA.

Our member banks have extensive experience in protecting their customers' privacy and data. The ABA has drawn from this experience in suggesting areas where the assessed risk levels may be reconsidered. The pilot program announced by the Government in December 2018 provides an important additional opportunity for the PIA to be informed, expanded and refined by the lessons learnt in the pilot[1]. As such, the ABA recommends that the terms of reference for the pilot specifically includes an assessment of the privacy risks.

[1] See http://jaf.ministers.treasury.gov.au/media-release/077-2018/.

Australian Banking Association

1. Ongoing refinement of the PIA

Many of the mitigation strategies identified in the PIA are focused on the provisions that are proposed for the *Competition and Consumer Act 2010* (Cth) (primarily the privacy safeguards). However, it will be important for these legal and regulatory protections to sit alongside the technical and operational risk mitigation measures which are intended to be contained in the Rules and Standards. We should not assume that laws protecting consumers will be adhered to and/or automatically and correctly applied at all times.

By way of an example, potential privacy risk 3.2[2] downgrades the likelihood of a third person posing as the accredited data recipient in order to gain access to the individual's consent information, from 'possible' to 'unlikely' following the application of, primarily, existing legal and regulatory risk mitigations, such as criminal laws and related penalties. The ABA view is that this fails to consider the intentions of fraudulent and criminal actors and cyber criminals who seek to operate using illegal means, and who may be difficult to enforce Australian laws against when located overseas or otherwise difficult to identify given the environment in which they operate, being primarily over the internet. This is supported by data reported by the Office of the Australian Information Commissioner (**OAIC**) showing that the largest cause of data breaches is malicious criminal attacks, such as the theft of personal information or hacking, phishing and other similar events[3].

As such, the ABA believes that the PIA could be improved if:

i) The Rules and Standards, as they are being developed and finalised, are considered in greater detail in the PIA.

ii) The risk of non-compliance with the proposed provisions of the Act was taken into account, which would allow a discussion of the regulatory strategies that the Australian Competition and Consumer Commission (**ACCC**) may adopt to promote compliance with those provisions.

iii) All privacy and data risks (including the additional CDR scenarios[4]) are tested as part of the pending pilot program to reflect the factual and technical nature of the given risks.

iv) The risk assessment follows the format of the risk assessment currently being applied by the OAIC in respect of assessments it conducts pursuant to Section 33C of the *Privacy Act 1988* (Cth) (**Privacy Act**) for consistency and alignment[5].

Once the PIA findings are known and considered, the lessons should inform compliance standards and align to the accreditation process beyond the principles currently set out in the ACCC Rules Outline (**Rules Outline**) issued in December 2018. This is of particular importance as the PIA currently envisages that accreditation will be tiered according to the risk level of the data in question. This tiered structure implies that certain accreditation requirements may only be minimum requirements and therefore may not have as onerous or substantive requirements as those which are required for the top tier of accreditation (such requirements may still be necessary depending on the nature of the accreditation provider). The PIA also does not identify what data will be considered of 'higher risk'.

The ABA is pleased to continue to work with Treasury on refining the PIA as the legislation, Rules and Standards are finalised.

2. Risks assessed under the PIA

The ABA has identified aspects of the PIA where industry experience would suggest a higher risk likelihood is plausible. As the PIA is refined, the ABA suggests that these risk assessments are reconsidered with input from the Rules and Standards that are developed, and also insights from consumer testing and the pilot program.

[2] See p.93.
[3] OAIC Notifiable Data Breaches Quarterly Statistics Reports, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-july-30-september-2018.
[4] As listed on pp.100 – 104.
[5] See Appendix A in https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments#appendix-a-risk-based-assessments-privacy-risk-guidance.

Phishing and other fraud

The threat of phishing attacks which exploit the CDR regime is a credible one and could result in considerable consumer detriment. Banks expend significant resources to protect their customers' data and have learnt that cyber criminals have proven themselves to be highly capable in creating new opportunities for phishing attacks and are quick to take advantage of new industry developments.

The ABA submits that the risk likelihood of the following potential privacy risks (following the application of risk mitigation strategies) are higher than that assessed under the PIA:

- Risk 1.1, in which a cyber-criminal poses as a data recipient to steal consumer data.
- Risk 1.2, in which a third party may use a false identify to acquire authentication information from the accredited data recipient.
- Risk 3.1, whereby a data recipient directs a consumer to a fake data holder website (i.e. where the data recipient knowingly engages in wrong-doing by directing the consumer to a phishing website). The PIA does not appear to have contemplated a scenario where a cyber-criminal attempts to tamper with the data recipient's website so that the website directs the consumer to a fake data holder website.
- Risk 3.2, whereby a cyber-criminal poses as a data recipient to direct a consumer to a fake data holder website.

The ABA considers that the adoption of the authentication flow articulated in the Open Banking Information Security Profile issued by Data61[6] will be an important risk mitigation measure. Decisions around the authentication flow should include an analysis of the risk that different models would pose to consumers, in terms of the likelihood of future phishing attacks, and the PIA amended to reflect these decisions.

Third party misuse of data

Risks associated with third party misuse of data are considered in risks 2.1, 2.2, 2.3, 2.4, 3.9, 5.1, 5.2, 5.3, 6.3 in the PIA.

Given our experience, ABA members would assess the likelihood of unauthorised access to consumer data by a third party is significantly higher than 'unlikely' in each of the above risks.

By way of example, risk 6.3 assesses the likelihood of the holding of data continuing even though the accredited data recipient is no longer an eligible data custodian as 'unlikely' (downgraded from 'moderate' after application of the risk mitigation strategies). However, in the example given where 'BetterDeal's' becomes a failed deregistered company, and control over Naomi's data is lost, the PIA does not appear to take into account that the risk mitigation strategies are practically very difficult to implement and also unlikely to be effective.

For example, the primary risk mitigation strategy of having a right to withdraw consent or request the deletion of information does not take into account the difficulties involved in (a) becoming aware in advance that BetterDeals (the data recipient) is going to be deregistered; (b) being able to contact BetterDeals to seek deletion of the relevant data; and (c) the loss of control over the data – that is, data is generally stored somewhere and if the company does not securely destroy the information prior to deregistration, the information is still stored somewhere (for example, by a cloud services provider) and is vulnerable to access by an unauthorised third person.

Strong identity and access management (**IAM**) controls at the data recipient will help mitigate this risk. The information security standards expected of data recipients that are established in the Rules could mandate appropriate IAM controls.

In addition, the ABA considers the following risk mitigation measures to be critical:

[6] See https://consumerdatastandardsaustralia.github.io/infosec/#4-authentication-flows.

- Data holders must have the power to withhold data if there is reasonable grounds that sharing data will lead to serious harm for the consumer or the security and integrity of the regime and data more broadly.
- The de-accreditation process should be robust (including that the accreditation register should allow for swift action to be taken once an Accredited Data Recipient (**ADR**) loses accreditation).
- Whilst we acknowledge that the Rules Outline (and PIA) do contemplate the existence of a rigorous consent framework, it is important that the framework is rigorously monitored and enforced including re-consent requirements.

Hacking

Malicious attacks by hackers or other cyber criminals are a significant cause of data breaches globally. The likelihood of an ADR's systems being compromised by an external attacker, enabling the attacker to access and use CDR data, will largely be a function of the cyber security capabilities of that data recipient. Our members have assessed the likelihood of this type of attack (under risk 5.4) to be higher than Treasury's assessment of 'unlikely'.

The ABA considers that the following additional measures will be critical in mitigating these risks:

- Information security requirements in the accreditation criteria, to be included in the Rules.
- Threat monitoring and intelligence sharing arrangements between data holders to help data recipients to defend against cyber-attacks targeting consumer data.

3. PIA recommendations

The ABA supports all of the recommendations of the PIA to ensure the risk mitigation strategies outlined work as they are intended. We suggest that the following recommendations could be strengthened by:

- Recommendation 4 – Requiring a Privacy by Design approach with consumer privacy set as a default state. Doing so ensures that there is no 'privacy trade off' per se.
- Recommendation 8 – Making a requirement to leverage complaints/breach data to address any newly identified privacy risks or vulnerabilities in those data sets.
- Recommendation 9 – Clarifying what constitutes a "significant change to the CDR legislation or Rules" to trigger further PIAs being completed.

In relation to recommendation 7, the PIA indicates that consumer education should be focused on in the period around 1 July 2019. This timing may need to be reconsidered in light of the Treasurer's announcement on the timeline for open banking, and the ABA would be happy to work with government on this[7].

4. Other issues

Authorised disclosure to non-accredited entities

The PIA discusses[8] the potential for CDR data to be disclosed, with the consumer's consent, to a non-accredited entity. We understand that this disclosure could occur under proposed section 56BC (2) of the Treasury Laws Amendment (Consumer Data Rights) Bill 2018 (**CDR Bill**). We note that this section would allow rules authorising 'CDR participants' to disclose CDR data. This is broader than the PIA's implication that it would be 'accredited data recipients' which would disclose CDR data in accordance with this mechanism[9]. The ABA suggests that, when CDR is disclosed to a non-accredited recipient, it

[7] See http://jaf.ministers.treasury.gov.au/media-release/077-2018/.
[8] See p.111.
[9] See second last paragraph of p.111.

may be appropriate to require the recipient to provide a warning to the consumer, including that the information will be going to a recipient who may not be required to comply with the Privacy Act if applicable. This would be in addition, or an alternative to, the CDR participant providing the consumer with a warning[10].

Who is bound by the privacy safeguards

There is discussion[11] in the PIA about who is bound by the privacy safeguards. The PIA states that:

a) those who purport to be accredited but are not will be bound; and

b) privacy safeguards 6 and 8 will apply to data holders.

We could not see support for these propositions in the CDR Bill, and request clarification accordingly.

We would also suggest that a key risk is that non-accredited third parties who hold the CDR data mishandle, misuse or fail to appropriately protect this data. Under the framework to be established by the CDR Bill, accredited data recipients are liable for the behaviour of these third parties. It may be appropriate for Treasury to consider whether the privacy safeguards should also be applied by law to these third parties, rather than just relying on accredited data recipients to impose and police data security standards.

Yours faithfully

Signed by

Denise Hang
Policy Director
02 8298 0414
Denise.Hang@ausbanking.org.au

[10] As proposed on page 112.
[11] See p.124.