AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

Attorney-General's Department

By Email:

31 March 2023

Dear Sir/Madam

Privacy Act Review Report 2022

Thank you for the opportunity to provide a submission in response to the Privacy Act Review Report 2022 (the Report).

The Australian Retail Credit Association (ARCA) is the peak industry association for businesses using consumer information for risk and credit management. Our Members include banks, mutual ADIs, finance companies and fintech credit providers, as well as all of the major credit reporting bodies (CRBs) and, through our Associate Members, many other types of related businesses providing services to the industry. ARCA's Members collectively account for well over 95% of all consumer lending in Australia.

ARCA, upon request of the Office of the Australian Information Commissioner (OAIC), has acted as Code Developer for the Privacy (Credit Reporting) Code 2014 (the CR Code) which supports the operation of the legislative framework for credit reporting contained in Part IIIA of the Privacy Act. ARCA's role in respect of credit reporting means we have a deep understanding of the operation of the Privacy Act, and particularly the operation of Part IIIA.

ARCA has previously provided submissions in response to the issues paper and discussion paper prepared as part of the Privacy Act Review.[1] Although Part IIIA was not within scope of the review, ARCA is providing a submission in response to the Privacy Act Review Report as several proposals could, if implemented, have implications for our Members and credit reporting more generally.

ARCA's submission focuses primarily on credit management and reporting issues, and provides specific feedback relating to:

1. The definition of de-identified data and the obligations that apply in respect of such data (Proposals 4.5-4.8);
2. The definition of consent (Proposal 11.1);
3. Consent withdrawal and information erasure (Proposals 11.3 and 18.3);

[1] ARCA's submission in response to the issues paper is available here; ARCA's submission in response to the discussion paper is available here.

4. Obligations and rights associated with automated decision making (Proposals 19.1-19.3);
5. Obligations associated with direct marketing and targeting (Proposals 20.8 and 20.9);
6. Retention periods for personal information and a review of other laws giving rise to obligations or incentives to retain personal information (Proposals 21.6 and 21.7);
7. Creation of a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs (Proposal 23.2); and
8. Timeframes in respect of the notifiable data breaches scheme (Proposal 28.2).

The Report contains many proposals, most of which would require a substantial amount of work to implement. This work will require entities throughout the economy to scope, design and deliver changes to existing documents, systems and processes, upskill staff, and develop risk and compliance monitoring frameworks. It is essential that there is a significant transition period (e.g. 24 months) from when any laws and guidance are put in place to when those laws start to take effect. Additionally, the proposals should be put in place in tranches, where the tranches chosen effectively spread the work out (and do not require new laws, guidance and practices to be re-worked multiple times).

1. The definition of de-identified data and the obligations that apply in respect of such data (Proposals 4.5-4.8)

We support the Report's conclusion that requiring data to be anonymised in order for the Privacy Act protections to no longer apply would be impractical. As acknowledged by the Report, we also consider that the use of de-identified information by entities presents a range of benefits, such as the potential to use data to improve their services or conduct research with very significantly reduced privacy risks.

As outlined in our submission to the discussion paper, de-identified data is used widely in the credit management context, including to compare (and predict) individual behaviour to (or from) the behaviour of all de-identified individuals in a group. Deriving insights from past performance of credit accounts is critical for all credit providers' ongoing risk management, as well as their financial viability. To that end, the continued ability to appropriately and safely use de-identified information is critical to credit providers and the broader credit market.

We note the proposals relating to de-identified information would have a very broad scope and effect. In order to implement these proposals, entities would need to apply protections to all information, including any information stored with de-identified information which was never personal information in the first place, and in any situations where there are negligible risks of re-identification or disclosure. It may be worth considering whether more specific proposals, focused on the risks of re-identification and where such risks may occur, would address the primary concerns articulated by the Report while reducing the cost and burden of changes for entities throughout the economy.

Should the proposals proceed to law reform and implementation, we note that the 'reasonable steps' expected of entities in relation to de-identified information should be made clear well in advance of commencement.

2. The definition of consent (Proposal 11.1)

Although we welcome some indications of flexibility within the proposed concepts that would apply to a 'consent', we remain concerned about the potential degree of inflexibility that may result from Proposal 11.1. As outlined in our submission to the discussion paper, if specific

consents were needed for e.g. even administrative or consequential activities, then this would require a substantial number of requests and, in our view, is likely to be viewed by consumers as of limited benefit and primarily a bureaucratic annoyance.

We continue to support an element of flexibility underpinning the framework around consents – that is, the requirements on entities depending in part on the types of information shared and the proposed data use(s). Data types and uses that create greater risks to individual privacy would lead to additional requirements (e.g. more specific consents). We also consider that it should be possible to 'group' consents, so that the consumer consents to types of data uses rather than each single use. This kind of framework is more likely to promote responsible data use while aligning with consumer expectations.

3. Consent withdrawal and information erasure (Proposals 11.3, 18.3 and 18.6)

ARCA notes that it conceptually follows that consent that is provided should generally be capable of being withdrawn, and that Proposal 11.3 is intended to make express the ability to withdraw a consent which exists under the current framework.

Nonetheless, in relation to this proposal, and the proposals about information erasure, ARCA makes the following comments:

- The credit reporting framework operates on the basis that information is retained with the credit reporting system for the specified periods set out in Part IIIA of the Privacy Act. This is essential to the overarching purpose of credit reporting: giving credit providers objective, easily accessible information about the consumer's creditworthiness, and helping them make appropriate lending decisions that are in the interests of both parties. Undermining this principle to allow information to be withdrawn at will would significantly reduce the macroeconomic benefits from credit reporting, and increase the risk that less creditworthy consumers receive loans they cannot afford (i.e. because their status is obscured by removal of information from the credit reporting system). The retention periods for personal information in Part IIIA balance the competing objectives of the benefits from credit reporting against the effect on a consumer's privacy, and any changes that would affect these periods should be carefully considered through the upcoming review of those provisions.[2]

- Many other laws require entities to retain substantial amounts of information, for instance to demonstrate compliance with non-privacy-related legal obligations. We do not consider that entities should be required to delete information where doing so would place them in breach of other obligations or expose them to significant legal risk. In that regard we consider the types of exceptions mentioned in Proposal 18.6 would appear to be appropriate. We also note that if the exceptions to e.g. the right to seek erasure are particularly significant, then there is a risk that consumers' expectations about their ability to seek to erase information may be out step when what can be deleted.

- If a right to request erasure of personal information were implemented, we would support that right not applying to information that has been de-identified. Although we

[2] Section 25B requires that a review of Part IIIA of the Privacy Act be completed by 1 October 2024.

acknowledge that de-identified information that was subsequently re-identified would then need to be treated in line with the consumer's erasure request, policymakers will need to consider the practical challenges of such a regime (including that it would appear to require entities to retain erasure requests in perpetuity).

4. **Obligations and rights associated with automated decision making (Proposals 19.1-19.3)**

It is difficult for ARCA to comment on the proposals relating to automated decision making in the absence of further information, particularly about:

- how specific the descriptions in privacy policies would need to be; and
- the types of matters which could be requested under Proposal 19.3.

We consider that these two matters should themselves be the subject of detailed consultation (along with the proposed consultation around the scope of 'substantially automated decision' proposed in the Report). However, we can make the following general comments:

- In the credit context, automated decision provides significant benefits to consumers and the economy. Appropriate uses of substantially automated decision making within an overall robust risk framework allows for faster credit decisions, as well as increased consistency in decisions, auditability of processes, all while lowering the overall cost of credit for consumers.

- Although credit providers may be able to provide a general description of the types of information used in automated decisions, there are substantial risks and unintended consequences associated with the proposals (particularly Proposal 19.3) if the requirements are too granular, as:
    - credit algorithms are proprietary in nature, and the mechanisms could be mis-used by competitor firms; and
    - there are risks of moral hazard (i.e. where consumers seek to falsify information based on what is used in credit decisioning processes). Given the size of the potential loans this could create outsized risks for the consumers (if the loan is ultimately unaffordable) or for lenders (if they are exposed to excessive credit risk outside their risk appetite or that tolerated by their regulators).

  To that end ARCA would not support an implementation – particularly of Proposal 19.3 – that involved requirements to disclose very detailed information in a manner that presents the risks we have identified.

5. **Obligations associated with direct marketing and targeting (Proposals 20.1, 20.2, 20.8 and 20.9)**

In relation to direct marketing, the credit reporting framework already contains restrictions intended to prevent the use of credit information for marketing purposes. In particular:

- CRBS are prohibited from using or disclosing credit reporting information for direct marketing (s 20G), with a limited exception where CRBs can use credit information to assist CPs to pre-screen an individual to determine if there are eligible for a certain consumer credit products.

- The CR Code:
    - limits the power of a CRB to use credit reporting information to develop tools that could help it (or a CP) assess the likelihood of the individual accepting specific credit or credit variation, or to target an individual to accept specific offers;
    - prohibits CPs from using eligibility requirements that indicate that the individual has/may have difficulties in meeting repayments under their existing credit contracts; and
    - gives individuals the right to ask a CRB not to use credit reporting information about them for direct marketing purposes.

ARCA supports the restrictions described above, and notes their apparent consistency with the policy goals expressed in the Report. On that basis we support the retention of current settings under the credit reporting framework.

In relation to targeting, our understanding of the discussion in the Report is that these proposals are primarily focused on harms from e.g. social media content selection, distribution and advertising. However, we note that definition outlined in Proposal 20.1 would apply to the credit industry – including who may obtain credit on what terms (e.g. with/without a guarantee or at what interest rate).[3] We consider that any definition of 'targeting' should be sufficiently focused to ensure it addresses the specific risks of harm identified without unduly broad application.

In relation to proposal 20.8, while we consider that few stakeholders would express explicit support for unfair or unreasonable targeting, we note that these concepts can be difficult to apply in practice. Additionally, notwithstanding the discussion in the Report, such a requirement would lead to increased uncertainty and legal risk for entities (particularly if implementation and expectations are unclear). We consider that there should be express consideration and consultation about whether any tailoring is required to the factors listed in Chapter 12 for the targeting context. We also consider that there should be opportunity to provide input on the desired policy outcomes relevant to particular scenarios etc with policymakers and regulators before any new obligations are finalised.

In relation to Proposal 20.9, we note our concerns above about requirements under Proposals 19.1 and 19.3 to provide very detailed information potentially leading to unintended consequences and risks of harm for credit providers and consumers. This could be relevant here if targeting were to include offers to enter credit on certain terms, and the expectation was that explicit information about how, for instance, the interest rate was determined would need to be disclosed.

6. Retention periods for personal information and review of other laws giving rise to obligations or incentives to retain personal information (Proposals 21.6 and 21.7))

[3] In the credit industry some lenders vary the price (e.g. interest rate) of a loan based on the credit risk associated with the potential borrower. This 'risk-based pricing' is conceptually distinct from e.g. differential pricing based solely on what a consumer would be *willing to* pay for a product or service. As noted in our earlier submissions, we consider that the Privacy Act should not restrict or prohibit risk-based pricing.

ARCA supports this proposal. Many ARCA Members are subject to laws administered by other regulators which require records and information to be retained to demonstrate that regulatory obligations have been complied with / goods and services have been provided in a compliant way. Although the retention of that information may serve to ensure that the policy outcomes sought by those other laws are demonstrably achieved, the retention of information does create privacy and cyber security risks. Entities subject to multiple laws with competing objectives are not in a position to address those issues; as such a clear signal from Government about the balancing of privacy and cyber security objectives against other policy goals is essential.

Additionally, we note that some entities may keep information that is either not subject to a specific retention period, or where the retention period has expired, because of ongoing legal or commercial risks. For instance, entities may need to prove they complied with other laws in response to proceedings by consumers or regulators, or EDR disputes. These ongoing risks should be factored into the Government's work on retention of personal information, as the risks mentioned above can mean that entities seeking to mitigate their risk exposure retain documents containing personal information for a substantial period (in turn increasing privacy/cyber security risks).

7. **Creating a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs (Proposal 23.2)**

ARCA supports this proposal, which would provide an alternative to different APP entities separately considering whether certain countries or certification schemes provide substantial similar protection under APP 8.2(a). The proposal has the potential to very substantially reduce the amount of work needed to rely on the mechanism in the relevant part of the APPs, while also leading to increased certainty and consistency of treatment. Entities may also be able to avoid costs associated with taking 'reasonable steps' that would be unnecessary due to the protections provided under the prescribed countries/certification schemes.

8. **Timeframes in respect of the notifiable data breaches scheme (Proposal 28.2)**

If statements about a data breach must be given to the Commissioner within 72 hours, institutions may not have adequate time to assess and mitigate the breach, particularly where external advice is needed. Although assessing and mitigating data breaches should be a priority for all entities, an 'as soon as practicable' reporting requirement may be more appropriate. Situations where the existing obligation is more suitable include where:

- the additional time would allow for one of the exceptions in s26WF to apply, removing the need for the statement (and therefore providing an adequate outcome to the situation and reducing burden for both entities and the Commissioner); and

- much or all of the 72 hour timeframe would elapse outside business hours.

If you have any questions about this submission, please feel free to contact me.

Yours sincerely,

Richard McMahon

General Manager – Government & Regulatory