AUSTRALIAN
RETAIL
CREDIT
ASSOCIATION

Attorney-General's Department

privacyactreview@ag.gov.au

10 January 2022

Dear Sir/Madam,

PRIVACY ACT REVIEW – DISCUSSION PAPER

Thank you for the opportunity to provide a submission in respect to the above discussion paper.

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. Collectively, ARCA's Members 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 gives effect to Part IIIA of the Privacy Act (which, in turn, sets out the legislative framework for credit reporting in Australia[1]). ARCA is also the author and administrator of the Principles of Reciprocity and Data Exchange (PRDE) which sets out industry agreed rules and standards for participation in comprehensive credit reporting (CCR). As an industry agreement with potential impacts on competition, an application for authorisation of some aspects of the PRDE was made to the Australian Competition and Consumer Commission (ACCC) (most recently in June 2020) and a new authorisation took effect from 6 January 2021[2]. ARCA has a deep understanding of the operation of the Privacy Act, and particularly the operation of Part IIIA of the Privacy Act.

ARCA has previously provided a submission in response to the issues paper. A key component of ARCA's previous submission was the importance of including Part IIIA (credit

[1] For details on ARCA's most recent application to the OAIC to vary the CR Code see https://www.oaic.gov.au/engage-with-us/consultations/consultation-on-application-to-vary-the-cr-code

[2] https://www.accc.gov.au/public-registers/authorisations-and-notifications-registers/authorisations-register/australian-retail-credit-association

reporting) within the scope of the current review. The contents of the discussion paper have only increased our concern around the continued exclusion of Part IIIA from the current review, because some of the proposals suggested in the discussion paper have significant potential consequences for the operation of Part IIIA. Our submission below highlights these issues, and particularly how key concepts in the Privacy Act might apply within Part IIIA.

Despite our concerns, we appreciate that the evolution of social media and the use of data in ways previously unimagined has necessitated changes to the current privacy framework. However, we are concerned that the desire to respond to new challenges in the digital environment will interfere with the legitimate operation of businesses (including credit providers and CRBs both in terms of the broader Privacy Act and especially those practices enabled and governed by Part IIIA). That is, the increase in consumer protection to respond to the threats posed by the more dubious practices of some organisations may inhibit the legitimate practices incorporated in Part IIIA which deliver broad benefits to industry, consumers, and the wider economy.

In this regard we note that, until now, Part IIIA has set a highwater mark in terms of consumer protection within the privacy sphere, in that the types of data that may be collected and the disclosures and uses to which it may be put to by specific segments of industry are both specific and limited. Consumers also have explicit right to access and correct information held about them. The proposals in the discussion paper – while endeavouring to exclude Part IIIA – could lead to an outcome which sees the broader Privacy Act framework as more restrictive than Part IIIA, or certainly, at odds with the operation of Part IIIA and the otherwise legitimate and essential use of data (both Part IIIA data and other forms of personal information within the broader framework) to support consumer lending and credit risk management. Key concerns are the proposals to restrict the use of deidentified data, restrictions on use of alternative data, and prohibitions on risk based pricing and automated decision making. ARCA's submission clearly outlines that these proposals will significantly impact business practices to the detriment of both these businesses, consumers and the broader economy.

ARCA's recommendations are:

1. The objects of the Act allow for the privacy rights of individuals to be balanced against interests of entities which include the public interest. In doing so it should be recognised that the public interest may be served indirectly, and may also incorporate situations where the commercial interests of entities deliver benefits to both the entity and individual as well as having broader economy benefits
2. Technical information be clearly defined as a type of personal information
3. Inferred information be excluded from inclusion in the credit reporting system
4. The use of de-identified information by credit providers to aid credit risk management remain outside the scope of the Privacy Act
5. Financial transaction data is not included in the definition of sensitive information
6. Consideration be given to promotion of broader consumer education initiatives rather than resolving issues of consumer comprehension and understanding through the notification process alone
7. The consent framework be flexible (reflecting data type and use), grouped consents be enabled, alongside standardised consents
8. The Privacy Act should not restrict or prohibit automated decision making and risk-based pricing, with any additional regulation a matter for anti-discrimination law (not the Privacy Act)

9. Additional or different privacy protections should not be applied to a broad class of vulnerable individuals
10. Additional consumer protections enabling rights to withdraw consent and erasure of personal information should not apply to information (both credit information and APP data – and including de-identified information) used for credit risk management
11. The NDB scheme provide a clear framework for addressing multi-party breaches, with clearly identified roles and liabilities (and the ability to notify the OAIC where a relevant entity fails to notify a consumer). The NDB scheme also be supplemented by improvements to notifications provided to consumers
12. Any industry funding levy be fair and equitable, with measurable outcomes (including greater capacity within the OAIC to provide guidance on credit reporting issues)
13. The preferred alternative regulatory model be the establishment of a Deputy Information Commissioner
14. A working group be established to consider harmonisation of privacy laws, which would include consideration of inconsistencies between state legislation and Part IIIA

Objects of the Act

ARCA's previous submission recommended that the objects of the Act continue to maintain balance between privacy rights of individuals and interests of entities.

We note the AGD discussion paper proposes that the concept of 'public interest' be introduced into the objects, such that the privacy of individuals is balanced with the interests of entities carrying out functions or activities undertaken in the 'public interest'. While 'public interest' is not defined, we note the discussion paper refers to public health and safety, research, national security, freedom of expression, law enforcement and (for commercial entities) economic well-being of the country.

ARCA's concern is that balancing individual privacy rights only against the activity of entities that meets the public interest test may limit otherwise appropriate activities of entities. That is, applying this test ignores the activities of entities which may be beneficial to both individuals and the entity but cannot be classified as being undertaken in the broader 'public interest' (noting based on examples listed in the discussion paper it is evident the 'public interest' extends to impacts beyond the immediate relationship between entity and individual). For example, an entity may use an individual's personal information to build a risk model which may impact how that entity deals both with that individual but also other customers who display similar characteristics to that individual. The predominant interest driving the undertaking of the activity is the commercial interest of the entity and its own customers.

We would argue that the industry wide approach to using individual data to build entity level risk models also meets a "public interest" test in that it is a necessary component of a robust risk framework that promotes both responsible lending and economically efficient access to and pricing of credit. However, we are concerned that without very clear drafting, there is a risk that individual entities may be restricted in any activity which is not primarily driven by public interest. The preferred position would be recognition within the objects that the balancing of individual rights against entity interests should allow for interests beyond public interest and can include interests which may deliver benefits to entity and individual.

Recommendation 1: The objects of the Act allow for the privacy rights of individuals to be balanced against interests of entities which include the public

interest. In doing so it should be recognised that the public interest may be served indirectly, and may also incorporate situations where the commercial interests of entities deliver benefits to both the entity and individual as well as having broader economy benefits

Definition of personal information & collection of personal information – technical information & inferred information

To begin, we would observe that changes to extend the meaning of personal information will impact operation of Part IIIA (despite Part IIIA being outside the scope of this review). Personal information is currently defined as information or an opinion about an identified individual (section 6(1)). Credit information is personal information.

An example of how any change to the meaning of personal information (and related terms) impacts the credit reporting system includes the application of the 'identification information' definition. Identification information (defined in section 6(1)) is a type of personal information and is relevant to how an individual is identified through the broader privacy framework as well as through the credit reporting system (with identification information a type of credit information under section 6N).

Changing the definition to provide that an individual is 'reasonably identifiable if they are capable of being identified, directly or indirectly' would therefore enable inferred or technical information about an individual to be used in the operation of the credit reporting system. For example, an individual's address for the purposes of their credit report may be identified based on geolocation data[3] or, if inferred data were permitted, potentially based on the location of an IP address related to the individual.

The changed definitions are further reinforced by the proposal to change the 'collection' definition to enable inferred or generated information to be permitted.

ARCA's view is that the inclusion of technical information in the credit reporting system ought to be supported; however inferred information should be expressly excluded from the credit reporting system.

Technical information can be used to promote data quality, particularly in respect to accurate identification of an individual's address. The address dataset is one of the most problematic datasets as it can be prone to error (both in terms of data entry but also simply because address conventions, especially for overseas addresses, are not always consistent) but it can be critical for data matching (that is, matching information held as part of a credit reporting database to the correct and intended individual). Technical information, such as the geo-location of an individual, provides an infallible dataset, which is far less error prone than traditional address datasets. For this reason, ARCA would welcome the clear recognition that this type of data is a form of personal information (and, as identification information, a type of credit information).

By contrast, ARCA does not consider that inferred information should be included in the credit reporting system. This is because inferred information (if proven to be based on an incorrect inference) can easily undermine data quality which could, in turn, impact the

[3] For example, Geoscape G-NAF (https://data.gov.au/data/dataset/19432f89-dc3a-4ef3-b943-5326ef1dbecc) or a Delivery Point Identifier (https://auspost.com.au/content/dam/auspost_corp/media/documents/australia-post-data-guide.pdf)

reliability of credit reporting information. Using the above example of using an IP address to infer an individual's location, it could be that the IP address has been masked or imprecise (with precise location available only from an individual's internet service provider) such that inferring information about the individual's location could easily lead to inaccurate information being recorded.

Outside the credit reporting system, inferred information may be less problematic (and ARCA agrees that there is utility in ensuring some inferred information about an individual is captured as part of the broader Privacy Act framework). However, as concerns the credit reporting framework, it is critical that only personal information which directly identifies the individual is captured and any collection of inferred information is excluded.

Recommendation 2: Technical information be clearly defined as a type of personal information

Recommendation 3: Inferred information be excluded from inclusion in the credit reporting system

Anonymisation of data

ARCA refers to its previous submission which highlighted that de-identified data is partly regulated through Part IIIA (through credit reporting body use of this deidentified data for research purposes), and further that credit provider use of de-identified data is unregulated (whether obtained through the credit reporting system or more broadly under the APP framework), and should remain as such. ARCA's previous submission argued strongly for retaining the ability to deidentify data (and use it in that deidentified form), in preference to the anonymisation of data (which would render the data incapable of meaningful use).

We note the discussion paper proposes amending the Privacy Act to require personal information to be anonymous so that it is no longer protected by the Act[4]. As we understand it, this would remove the ability for data to be de-identified and used outside the scope of regulation.

This will have a significant impact on legitimate uses of de-identified data by credit providers to support analytics and credit risk management. Credit risk management analytics are inherently about comparing (and predicting) individual behaviour to (or from) the behaviour of all deidentified individuals in a group. Anonymisation means changing information so it is no longer possible to identify someone from that information – the "key" that enables an individual to be compared to the group is lost.

To illustrate our understanding of the differences in de-identification compared to anonymisation, we present the following example:

[4] We note the discussion paper proposes replacing de-identification with data anonymisation in a number of places, including introducing a 'reasonably identifiable' requirement to the definition of personal information (recommendation 2.3), and requirements around data destruction and anonymisation (recommendation 19.3) – in addition to the recommendation 2.5. ARCA's comments on de-identification and data anonymisation apply to each of these various proposals.

- Patricia Smith is a customer of ABC Bank. Patricia held a home loan with ABC Bank, and defaulted on that loan 5 years into a 30 year loan term. Following default, the home secured by the loan was sold, and ABC Bank suffered a loss of $25,000. As part of its collection recovery process, ABC Bank also obtained credit reports for Patricia which included default information and repayment history information recording unmet payment obligations with a number of other credit providers.
- ABC Bank created a 'risk' profile to capture information about this customer, and the loan default. This information was de-identified, and, for example, it no longer contained Patricia Smith's name, date of birth or residential address. However, the risk profile did record information reflecting the credit behaviour of a 25 year old female, living in the western suburbs of Sydney, working in the health care industry. That credit behaviour included information about the operation of Patricia's accounts with the bank and information obtained from credit reports obtained at different points in the home loan's life cycle.
- ABC Bank were able to compare this 'risk' profile (and a series of similar profiles) to its overall risk framework and credit management system. It identified a series of factors which were common to a number of risk profiles for individuals who all defaulted at a similar time period (and who held a similar range of credit products). It then was able to alter its decision analytical framework to identify new applicants who displayed similar characteristics, with a corresponding 'flag' requiring those applicants to have additional expense verification, or manual assessment.

To be clear, if de-identified information were to be regulated by the Privacy Act, ABC Bank would be unable to use the information in the manner set out in the above example. That is, by regulating de-identified information so it is treated similar to personal information, the use of that information would need to fit within the existing use categories.

In the above example, the information includes credit reporting information (albeit in a de-identified form). If the use of that information had to occur under the existing permitted uses, ABC Bank would be restricted in only being able to use the credit report it obtained for Patricia Smith when first assessing her application for credit for 'internal management purposes' (which may include development of a risk profile). Otherwise, and again applying the existing regulations, the subsequent credit reports that ABC Bank obtained for Patricia Smith could only be used to assist Patricia to avoid defaulting on her obligations with ABC Bank[5] but could not be used for any 'internal management purpose'.

Critically, because this information is currently able to be de-identified and sits outside the scope of regulation, ABC Bank are able to use this information to support the legitimate purpose of risk profiling.

If the discussion paper proposal proceeds and this information must be anonymised for it to be outside the scope of the Privacy Act, the requirement to anonymise the data would strip it of its value. The data may capture payment behaviour on the home loan, but any information about the type of individual who held the home loan (for instance, the individual's age, location, industry) would have to be removed so that it no longer identifies any type of individual.

In considering this example, it is evident that the anonymisation proposal fails to appreciate the very restricted use framework available to credit providers within Part IIIA. We again stress that even though Part IIIA does not sit within the scope of the review, the

[5] This outcome is the result of the application of the table contained in section 21H(b), Items 1 and 5

anonymisation proposal will directly impact the operations of all credit providers. It should be highlighted that risk profiles will also combine both Part IIIA and APP information held by credit providers, and de-coupling this information may then undermine the risk methodology relied on by the credit provider.

Removing the ability for credit providers to use de-identified information will have far reaching consequences. A properly functioning credit sector requires that data from an individual is able to be assessed in the context of the data aggregated for all individuals. Deriving insights from past performance of credit accounts is critical for all credit providers' ongoing risk management. For Authorised Deposit-taking Institutions (ADIs), having a robust risk management framework is a prudential requirement. Similarly for non-ADIs, a robust risk management will be required by their wholesale funding providers (which may be ADIs as well).

For both ADIs and non-ADIs, the inability to properly utilise the insights derived from customer performance can be the difference between success or failure of an organisation. Moreover, we are not aware of any evidence that deidentified data is currently systemically misused withing the credit management framework. We appreciate that there may be concern about how data may be used in other contexts - however it seems a perverse response to issues posed by the use of data in other contexts (and by other sectors) to then actively disable the credit industry in its ability to profile and analyse risk (and in doing so undermine the efficient access to and allocation of credit which has economy wide implications for both consumers and small businesses).

ARCA's recommendation is that the use of deidentified data to aid credit risk management must be preserved as part of the Privacy Act framework. In making this recommendation, ARCA recognises that data anonymisation may be preferred to deidentification for certain sectors or uses - however a specific carve out must exist for uses directly related to assessing and managing credit.

> **Recommendation 4: The use of de-identified information by credit providers to aid credit risk management remain outside the scope of the Privacy Act**

Sensitive information

We note the discussion paper raises questions about the expansion of the definition of sensitive information. Financial information including transaction data, is specifically identified as a type of information which may need to be included in the meaning of sensitive information. We also note that classifying information as sensitive information has the effect of restricting collection to a consent-based model and further restricting use and disclosure including prohibiting use and disclosure for secondary purposes.

The exchange of transaction data forms the basis of the consumer data right (CDR) for the banking sector. We are concerned that including transaction data within the meaning of sensitive information may inhibit the operation of CDR by placing a restriction on the exchange and use of that data within the CDR framework. We note the discussion paper does not appear to consider the adequacy of the CDR framework as concerns the exchange of transaction data, and particularly how additional restrictions on the use of this data as part of the Privacy Act would impact on the use of this data under the CDR rules.

CDR operates on a consent-based model, although as noted below, this can be problematic. CDR does enable transaction data to be used for both 'primary' and 'secondary' purposes

(i.e. general research purposes) although with express and separate consent. In the event that transaction data were classified as sensitive information under the Privacy Act, this may then mean an entity would lose the ability to use the information for a secondary purpose (as otherwise enabled by CDR). This has the effect of introducing an inconsistent regulatory overlay through the Privacy Act.

More broadly, we are concerned about the need for clarity as to how the various privacy and data frameworks interact, and the potential for this type of proposal to add to the complexity and uncertainty of various pieces of legislation. We note issues of complexity of financial service legislation has recently been considered by the Australian Law Reform Commission[6].

We are also concerned about the assumption that transaction data may infer sensitive information about an individual. The discussion paper suggests that an individual's financial transaction history may include clothes shops (which could indicate an individual's gender) or political or union organisation membership (which could indicate an individual's political opinions). We respectfully disagree that inferring sensitive information based on an individual's financial transaction history is a likely outcome, given this could easily prove unreliable. For instance, an individual's shopping history does not reveal their gender – as that individual may be shopping for other people (not just themselves) and may also unhelpfully reinforce misapplied or inappropriate gender norms.

ARCA submits that financial transaction data should not be included in the definition of sensitive information on the basis that financial transaction data is already adequately dealt with as part of existing frameworks such as CDR for open banking and Part IIIA for credit reporting. Adding a further layer of regulation through the classification as 'sensitive information' is likely to lead to inconsistency and potential overlap between regulation.

> **Recommendation 5: Financial transaction data is not included in the definition of sensitive information**

Privacy policy requirements

We note the discussion paper proposes introducing requirements to ensure privacy notices are clear, current and understandable, as well as consideration of the use of standardised notices.

We note the discussion paper does not appear to consider means to promote consumer understanding and avoid notice fatigue beyond consideration of the content and timing of notices.

As set out in ARCA's previous submission, having sought to promote consumer education in terms of the credit reporting system through our CreditSmart website (www.CreditSmart.org.au), our experience is customer notification is limited in its ability to achieve consumer understanding and awareness of privacy related issues. While we do not object to improvements to make notices easier for consumers to understand, the reality is that even the best drafted notice is unlikely to obtain more than a cursory glance from a consumer. Consumers are happy to transact using their data, often without choosing to

[6] See https://www.alrc.gov.au/inquiry/review-of-the-legislative-framework-for-corporations-and-financial-services-regulation/. We note the ALRC did not include the Privacy Act within its scope, but nonetheless the proposals raised in the first interim paper are relevant to this issue.

understand the overall framework in which that data is shared. It will often only be where an issue arises that a consumer will seek to understand the legal framework.

ARCA's view is that more can be gained by improving a consumer's access to timely and relevant privacy-related education material[7], and otherwise focusing on improving general consumer literacy on basic privacy and data rights and concepts. Repeating our earlier submission, we suggest that consideration continue to be given to promotion of broader consumer education initiatives rather than resolving issues of consumer comprehension and understanding through the notification process alone.

> **Recommendation 6: Consideration be given to promotion of broader consumer education initiatives rather than resolving issues of consumer comprehension and understanding through the notification process alone**

Consent requirements

We note the discussion paper proposes that consent requirements be strengthened by requiring consent to be defined as being voluntary, informed, current, specific and an unambiguous indication through clear action. The discussion paper also proposes the use of standardised consents.

ARCA notes that this proposed consent framework appears similar to that used under the CDR. However, as we noted in our previous submission, we remain concerned about the inflexibility that may be inherent in such a framework. That is, requiring a clear consent to attach to each data use may be difficult to implement. There is considerable difference between a situation in which a consumer shares data with an entity to give effect to a single transaction or interaction as opposed to the sharing of data in the context of an ongoing relationship between consumer and entity. Data may have more than 10 or 20 applications within an entity, the bulk of which may be necessary administrative or portfolio management activities, or activities consequential to that for which consent has been gained. Requiring clear and unambiguous consent to each and every activity is more than likely to be viewed as a bureaucratic annoyance and alienate customers.

ARCA's view remains that for consent to be effective and meaningful it must also import an element of flexibility, that is, the ability to dial up or dial down consent having regard to the type of information shared, and the proposed data use. It must also be possible to 'group' consents, so that the consumer consents to types of data uses rather than each single use. Standardisation of certain types of consents across industry participants would also be of benefit. This type of framework is more likely to promote responsible data use but, importantly, align with consumer expectations.

> **Recommendation 7: The consent framework be flexible (reflecting data type and use), grouped consents be enabled, alongside standardised consents**

Restricted and prohibited practices

We note the discussion paper raises concerns with particular practices and considers whether the law needs to do more to restrict or even prohibit these practices. Practices identified include the collection of geolocation data (which we have discussed above),

[7] That is, material that relates to the specific issue facing the customer and given *when* the customer needs it.

automated decision making and risk-based pricing. Different models are proposed for imposing restrictions on the use of automated decision making. In terms of risk-based pricing, it is suggested that the practice of using information about a person's financial vulnerability to cause harm or discrimination may be a prohibited practice (noting questions are then raised as to whether prohibited practices ought to be introduced into the Australian privacy framework).

ARCA is concerned that automated decision making and risk-based pricing, both practices which are widely utilised in the credit industry, are considered to raise the prospect of increased consumer harm and thus requiring restriction or prohibition as part of the Privacy Act without broader consideration of the legal framework, including the application of anti-discrimination laws.

Automated decision making, within an overall robust risk framework, promotes positive consumer experiences, including real time credit decisions, consistency in decisioning, auditability of processes, and lowers the overall cost of credit. The discussion paper recognises the benefits of automated decision making, but raises concerns about the transparency of decision-making, and the risk individuals will be subject to unlawful discrimination and unfair treatment.

It should be noted however that identifying what distinguishes between individuals who repay and those who do not is inherently the focus of credit risk assessment and management. Those who have the capacity to repay and do repay will tend to get better access to credit and on better terms compared to those who don't. The credit reporting system supports such "discrimination", but also has protections against enabling unlawful discrimination by ensuring that sensitive information cannot form part of credit information shared with credit reporting bodies.

An extension of being able to distinguish between different levels of credit risk is risk-based pricing[8]. Risk based pricing is generally thought of as charging different prices to the different consumers based on their relative risk. This form of pricing is growing within the Australian consumer credit market but is not as mature as in other markets. Certainly, competition for low-risk segments is growing.

But risk-based pricing of credit has always existed in Australia. Credit providers may charge exactly the same rate to all their customers, but their "risk appetite" determines that only certain individuals are within their target market. This may be expressed in terms of individuals who will be approved versus those who will be declined (e.g. income and serviceability, loan to value ratio). It may also be expressed in terms of the products they offer (e.g. secured versus unsecured).

There is no doubt that the Australian market has become increasingly stratified and differentiated in terms of credit providers and the consumer segments they are targeting. But imposition of regulation may actually increase the degree of stratification and differentiation (i.e. discrimination) in the market e.g. responsible lending laws may result in some credit providers being more risk averse, others may target higher risk consumers through less regulated products. Likewise, attempting to restrict access to and use of data for credit risk

[8] To be clear, we are referring to the concept of adjusting the price of credit based on the customer's risk of not repaying. We note that there may be other forms of variable pricing that are based on other factors, including a prospective customer's price elasticity. Whether those practices should be prohibited is a separate matter.

assessment and management may also have a perverse effect of making mainstream industry participants more risk adverse, reducing the options available to higher risk consumers and pushing them to credit providers offering even higher pricing.

Overall, rather than regulating the process and tools (automation, risk based pricing), it is suggested the focus of regulation should be the harm you seek to avoid e.g. credit providers being able to demonstrate that their processes do not discriminate based on protected attributes. This regulatory approach ought to focus on the application of anti-discrimination law, not the operation of the Privacy Act.

> **Recommendation 8: The Privacy Act should not restrict or prohibit automated decision making and risk-based pricing, with any additional regulation a matter for anti-discrimination law (not the Privacy Act)**

Vulnerable individuals

We note the discussion paper raises a question as to whether additional or different privacy protections are required for vulnerable individuals, although no specific recommendation is made.

ARCA would highlight that vulnerability is often broadly defined. For instance, the Australian Bankers' Association Code of Banking Practice defines vulnerability as including age-related impairment, cognitive impairment, elder abuse, family or domestic violence, financial abuse, mental illness, serious illness or any other personal, or financial, circumstance causing significant detriment (paragraph 38).

Given the broad scope of vulnerability, and the varying degrees of vulnerability potentially faced by individuals, additional or different privacy protections may be unwarranted, or may do little to aid the individual impacted by the vulnerability. On this basis, and without a clear understanding of what additional or different privacy protections may do to aid a specific vulnerable individual, ARCA does not support the provision of these additional or different privacy protections.

> **Recommendation 9: Additional or different privacy protections should not be applied to a broad class of vulnerable individuals**

Rights to object and portability, erasure of personal information

We note the discussion paper proposes increasing consumer rights in respect to handling of personal information, including rights to withdraw consent and also erase personal information. Notionally, ARCA considers that increasing consumer protections in the digital age and in response to the challenges posed by the increased sharing of personal information, particularly in the context of social media, has merit.

However, ARCA's concern is to ensure that these measures are clearly restricted in their operation so that they do not unduly interfere or restrict credit risk management, both through the credit reporting system but also through the use of APP-data to aid credit risk management. A robust system of credit risk management is reliant on the ability to successfully address information asymmetry. An information asymmetry will arise, for instance, in a situation where one party (the consumer) holds the relevant information and the other party (the credit provider) is inhibited in its decision-making based on its ability to access that information. Information asymmetry for credit risk assessment and management

has been reduced through the credit reporting system, benefiting consumers and credit providers both individually and collectively. Strict rules prevent the removal or destruction of information in the credit reporting system; information can only be de-identified or destroyed if it is incorrect or is otherwise at the end of its retention period. More recently, through the Mandatory CCR legislation, the largest credit providers are required to contribute information on all their consumer credit accounts into the credit reporting system.

ARCA's firm view is that allowing consumers to withdraw consent to access of data, or even erase data, has the potential to introduce significant information asymmetries. This will undermine the operation and integrity of the credit reporting system, which could, in turn, impact the quality of credit decisions. Poor credit decisions lead to poor outcomes for both credit providers and consumers.

We also note the right to erasure is proposed to extend to the right to erase de-identified data. In this regard, we repeat the concerns raised in our submission above, particularly the need to ensure that credit providers continue to be able to use de-identified data to aid credit risk management, including the development of analytical models. If consumers had the right to erase data which would otherwise be deidentified and used as part of development of risk profiles, it could seriously undermine this ability.

> **Recommendation 10: Additional consumer protections enabling rights to withdraw consent and erasure of personal information should not apply to information (both credit information and APP data – and including de-identified information) used for credit risk management**

Notifiable Data Breach (NDB) scheme

ARCA's previous submission highlighted the key issue with the operation of the NDB scheme is the handling of multi-party breaches, and the need for clear rules to identify which party is responsible for making the appropriate notification. ARCA also noted the General Data Protection Regulation (GDPR) model of data controllers and processors, and suggested such a model ought to be adopted in Australia.

The discussion paper has rejected this suggestion; the view was that such an approach would remove consumer protections as it could mean that (where a data controller fails to notify an individual) the consumer does not receive a notification.

The only recommendation made in the discussion paper to improve operation of the NDB scheme is for the consumer notification to include information about the steps taken by the entity to respond to the data breach, including the steps to reduce adverse impact on the consumer.

ARCA remains concerned that, in the absence of a clear approach to managing multi-party data breaches, the NDB scheme remains at risk of 'over notification' to consumers, as well as delays or even an inability to assess the significance of harm caused by the data breach. While we appreciate concerns about removing consumer protections, without a clear framework for addressing multi-party data breaches, these protections may not be operating effectively (in any case).

Clearly identifying roles and liabilities could ensure that affected entities communicate amongst each other who is responsible, who has communicated with the consumer, and what has been communicated. In that manner, this ensures that entities can identify

themselves where there has been a failure to notify a consumer, and steps taken (by that entity) to rectify (as well as notifying the OAIC of the failure by the relevant entity to notify). This embeds appropriate checks and balances within the NDB scheme but, importantly, ensures clear, singular notifications are provided to the consumer.

We would suggest that this system could be supplemented by improvements in the notification provided to consumers, including providing a list of other parties involved in the relevant data breach, steps being taken by those entities and how the consumer, if they choose to, may contact those entities to obtain further information.

> **Recommendation 11: The NDB scheme provide a clear framework for addressing multi-party breaches, with clearly identified roles and liabilities (and the ability to notify the OAIC where a relevant entity fails to notify a consumer). The NDB scheme also be supplemented by improvements to notifications provided to consumers**

Regulation and enforcement

We note the discussion paper includes proposals which would provide more enforcement tools to the OAIC, as well as the introduction of an industry levy to fund OAIC to provide guidance, undertake systemic reviews and enforcement action. We also note the discussion paper seeks feedback on different regulatory models being either increased use of external dispute resolution (EDR) schemes, creation of a Federal Privacy Ombudsman or establishment of a Deputy Information Commissioner.

ARCA's observation in its dealings with the OAIC is that the breadth of its responsibility has been increased (including CCR, consumer data right, COVID-19 privacy issues etc) but without commensurate changes to resourcing. ARCA has particular concern about the level of ongoing specialist support within the OAIC for credit reporting.

If imposition of an industry funding model was preferred, any levy would need to be applied fairly and equitably across industry, and the outcomes associated with the imposition of the levy would need to be clearly measurable e.g. if levies were imposed on participants in credit reporting then all participants should be included in the levy, and industry should see greater capacity within the OAIC to undertake their role including providing guidance on credit reporting issues.

In terms of the alternative regulatory models, ARCA's view is that the establishment of a Deputy Information Commissioner is the preferable option, as it ensures that the OAIC remains the appropriate home for specialist privacy knowledge and advice. It is also preferable to establishing a Federal Privacy Ombudsman, as this may simply duplicate parts of the operation of the OAIC, but with the added overhead of having to establish a separate organisation.

> **Recommendation 12: Any industry funding levy be fair and equitable, with measurable outcomes (including greater capacity within the OAIC to provide guidance on credit reporting issues**

> **Recommendation 13: The preferred alternative regulatory model be the establishment of a Deputy Information Commissioner**

Interaction with state and territory laws

We note the discussion paper recommends that a working group be established to harmonise privacy laws.

ARCA would welcome this initiative. We note we are aware of two examples of potential inconsistency between state legislation and operation of Part IIIA of the Privacy Act, as follows:

- Victoria: Under Part 4.1, section 45 (2)(m) of the Australian Consumer Law and Fair Trading Act 2012, credit providers may be unable to issue notices to a Victorian customer, once the customer advises in writing that no further communication should be made about that debt. ARCA notes this appears to impact operation of default listing under sections 6Q and 21 of the Privacy Act (and also paragraph 9 of the Privacy (Credit Reporting) Code (CR Code)).
- Northern Territory: Part 8 (Fair Reporting) of the Consumer Affairs and Fair Trading Act imposes a series of obligations on reporting agencies which appear to go beyond requirements imposed by Privacy Act/ CR Code.

Recommendation 14: A working group be established to consider harmonisation of privacy laws, which would include consideration of inconsistencies between state legislation and Part IIIA

We would welcome the opportunity to discuss this submission further. Please contact our Executive Director, Regulatory, Elsa Markula, on 03 9863 7863 or emarkula@arca.asn.au with any queries.

Yours sincerely

Mike Laing
Chief Executive Officer