AUSTRALIAN COLLECTORS & DEBT BUYERS ASSOCIATION

24 January 2022

The Secretary
Australian Attorney General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

By email: PrivacyActReview@ag.gov.au

Dear Sir,

Submission in response to Discussion Paper: Privacy Act Review

The Australian Collectors & Debt Buyers Association is pleased to provide the attached Submission in response to the Privacy Act Review Discussion Paper.

Please do not hesitate to contact the writer to discuss any aspect of the Submission.

Yours sincerely
AUSTRALIAN COLLECTORS & DEBT BUYERS ASSOCIATION

Alan Harries
CEO
Email: akh@acdba.com

Submission in response to Attorney General's Department Privacy Act Review Discussion Paper

January 2022

Australian Collectors & Debt Buyers Association (ACDBA) welcomes this opportunity to respond to the Privacy Act Review Discussion Paper released 25 October 2021.

About ACDBA

Established in 2009 for the benefit of companies who collect, buy and/or sell debt – ACDBA's members (refer Appendix 1) represent the majority of the collection market in Australia.

The core business of our members within the financial services industry is in the credit impaired consumer segment, whether as collectors or debt purchasers, working with consumers who for various reasons, have found themselves in default of their credit obligations.

Contingent collectors pursue the recovery of accounts on behalf of a creditor under a "principal and agent" agreement for an agreed fee, with the debt at all times being owned by the creditor. Creditors issuing instructions for contingent collections include governments, statutory authorities, financiers, insurers, telcos, utility providers, other corporations, strata body corporates, small business and individuals.

ACDBA members purchasing debt, each hold an Australian Credit Licence and are members of the Australian Financial Complaints Authority (AFCA). An explanation of how debt purchasing operates in Australia is included at Appendix 2.

Overview

Changes outlined in the Discussion Paper aimed at clarifying the scope and application of the *Privacy Act 1988 (Cth)* (the Act) and removing ambiguity from existing provisions are in principle generally supported by ACDBA.

Although changes intended to strengthen requirements around the use and handling the personal information of children and other vulnerable groups are also supported, cautious concern is raised around the rationale for wider changes to current provisions in the absence of evidence widely supporting the existence and extent of specific privacy issues.

Establishment of a general direct right of action is not supported – instead ACDBA supports a limited direct right of action for a narrow range of highly offensive breaches such as intimate image abuse, bullying, perpetrating domestic violence, blackmail or inappropriately influencing family court proceedings.

The Discussion Paper extensively references overseas jurisdictions. It is appropriate to highlight any significant overhaul of Australia's privacy laws to align for example with the European Union's General Data Protection Regulation (GDPR) will add significant cost burdens to industry, which should not be underestimated.

Where restrictions are to be further imposed upon business entities, the case for change should be clearly supported by empirical data evidencing the extent of the privacy issue together with cost burden benefit modelling to ensure compliance costs are commensurate to the actual risk posed.

These concerns are particularly relevant at this time as many businesses in Australia struggle to survive through the health pandemic and adjust to the ongoing challenges of changed work and life expectations post COVID.

Our members report much of the existing framework of privacy legislation in Australia remains fit for purpose and functions appropriately, maintaining a fair balance of the rights of individuals and commercial realities for Australian businesses.

The Collections Industry

The Collections Industry differs from the wider business community in that the relationships, firms have with consumers are not established by each individual initiating contact or willingly electing to engage with the firm.

Instead, an individual is typically contacted by a collection firm following an alleged breach of a financial agreement between that individual and a third party credit provider. The response of individuals to such contact varies with some very resistant towards participating cooperatively to resolve or discuss their financial dispute.

The Collections Industry in FY2021[1] made 113 million contacts with Australians by way of calls, texts, letters and emails in relation to 8 million consumer accounts. Any proposed restrictions introducing enhanced privacy controls which fail to take account of the basis of the relationship individuals typically have with collection firms will potentially unreasonably interfere with the rights of the other party to a financial agreement allegedly breached by an individual.

The nature of this relationship between individuals and collection firms underpins collection related exemptions in respect to obligations under other Commonwealth legislation[2] for example, the *Do Not Call Register Act 2006* and the *Do Not Call Register Regulations 2017*:

> ***Part 2 – Do Not Call Register***
>
> *6 Calls that are not telemarketing calls*
>
> *…*
>
> *(6) A voice call is not a telemarketing call if the primary purpose of the call relates to payment for goods or services ordered by, requested by or supplied to a customer.*

ACDBA respectfully submits there is a compelling case for providing a similar exemption for the Collections Industry in any amendments to the Act and associated regulations.

Responses

Our responses below are to proposals and questions relevant for the Australian collection industry rather than to any other wider privacy issues raised. For ease of navigation, our responses reference the page numbering from the Discussion Paper.

Pages 18-20 **Objects of the Act**

Proposal 1.1: Amend the objects in section 2A

This proposal is supported. The inclusion under (b) of the following words is essential: *"to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions"*

[1] ACDBA Data Snapshot 2021 – www.acdba.com
[2] Do Not Call Register Regulations 2017

Pages 33-35 **Definition of sensitive information**

Question: What would be the benefits and risks of amending the definition of sensitive information, or expanding it to include other types of personal information?

Noting the suggestion that the categories of sensitive information be reviewed to consider such things as location, financial, health, genomic and biometric information, we submit that any change to "location information" should make clear this relates to information generated from an App, IP address or mobile phone location and specifically ensure an individual's physical address is not inadvertently and inappropriately categorised as "sensitive Information".

Further, we submit given the pace of technological change, care should be exercised to ensure any amended definition of "sensitive information" does not stifle innovation.

Emerging use of voice print technology to identify an individual is expected to improve the customer experience and the efficiency of call handling, by identifying customers in real time. In the future, technology such as a fraud voiceprint database offers the potential to assist with fraud mitigation especially for identity theft.

These examples highlight why the definition of "sensitive information" must balance individual privacy with both current and emerging risks.

Pages 36-39 **Flexibility of the APPs**

ACDBA supports the general view that flexibility is a key benefit of the APPs and that a more prescriptive approach would increase the regulatory burden for businesses and limit the effectiveness of the Act in protecting the privacy of individuals - the current APPs work very well.

Significant change to the APP framework appears unwarranted in the absence of compelling data to identify and quantify actual privacy risks as there do not appear to be any fundamental shortfalls in the existing regime.

Pages 40-49 **Small business exemption**

ACDBA supports the retention of a small business exemption for the wider business community on the basis the cost of compliance would be beyond the resources of many smaller firms.

An exemption for small businesses in the Collections Industry however is somewhat of a moot point as most clients particularly those in the financial services industry require their service providers to meet the obligations of the Act as an essential condition of their contract of engagement.

Pages 50-57 **Employee records exemption**

We note the Discussion Paper does not include any proposals relating to the employee records exemption nor are any examples cited of poor privacy outcomes based on the employee records exemption – consequently, a significant actual privacy risk posed by retaining the exemption is not evident.

On this basis, we submit the status quo should be maintained to avoid imposing an unwarranted compliance burden and costs on industry.

In response to the various questions around the issue in the Discussion Paper, we offer the following perspectives:

- Private sector business entities are regulated by workplace relations legislation imposing obligations on employers, including in relation to employee record keeping requirements
- In the absence of compelling evidence to the contrary, most private entities already treat employee records as if regulated personal information, applying high protection standards – understandably, the motivation to do so is high as those managing and administering such records have their own individual details recorded in those systems
- The principal purpose for maintaining employee records is to manage the many and varied aspects constituting the employment relationship. Limits on access by an individual to all the information contained in their employment record should be maintained to preserve that employment relationship.

  Currently, individuals with an employment grievance may access information from their employer as part of proceedings and processes pursuant to workplace relations legislation with such legislation providing appropriate safeguards having regard to the respective rights of the parties.

The current employee records exemption should remain, but if varied in response to compelling evidence, we submit as a minimum the exemption should be maintained in relation to APP 12 and APP 13 as both would be problematic if implemented and would adversely impact the employment relationship.

Pages 67-73 **Notice of collection of personal information**

Proposal 8.3: Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

ACDBA strongly supports the notion of introducing the option of entities using a standardised format of privacy notices, given the cost impost on industry to keep notices updated.

To address concerns regarding the limitation of a single standardised notice format, one member suggested the OAIC develop model forms which firms could tailor for their specific use by way of an online drop down selection based engine, similar to New Zealand's Privacy Statement Generator[3].

[3] NZ Privacy Commissioner - www.privacy.org.nz/tools/privacy-statement-generator

Proposal 8.4: Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless:

- **the individual has already been made aware of the APP 5 matters; or**
- **notification would be impossible or would involve disproportionate effort.**

Noting the following commentary in the Discussion Paper around proposal 8.4:

> *"While there is merit in enhancing transparency by placing a heavier obligation on APP entities to provide notice, some flexibility in the requirement to provide notice should be retained for situations where notice is unnecessary as the individual is already aware of the matters that would be notified and where providing notice would be impossible or would involve disproportionate effort, or may actually be harmful."*

it is appropriate, as a further example of situations where providing notice would be impossible, impractical and/or potentially impact the privacy of others, to again reference the work of collectors to establish and verify current contact details for individuals to allow contact to resolve their account issues.

Issuing an APP 5 notice to a third party from whom personal information about an individual is collected, either directly or indirectly, would reveal to the third party that the individual concerned was to be contacted by a debt collector – such a disclosure would be a breach of that individual's privacy.

Additionally, a notice to a third party might trigger adverse consequences for the individual, for example, by way of family violence; reputational harm; the eligibility for rights, benefits or privileges in employment, credit or housing.

ACDBA respectfully submits an APP 5 collection notice to a third party from whom personal information about an individual is collected, should continue to not be required where the collection relates to debt collection.

Pages 80-93 **Additional protections for collection, use and disclosure of personal information**

Proposal 10.3: Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

We support the proposal that guidelines be issued by the Commissioner to assist entities with examples of reasonable steps.

In doing so, we submit the Commissioner should take into account the concerns we have identified immediately above in relation to proposal 8.4 - that is, the difficulties encountered in dealing with the collection of personal information from a third party individual where debt collection is the primary purpose for collection of such personal information.

Pages 98-99 **Pro-privacy default settings**

Proposal 12.1: Introduce pro-privacy defaults on a sectoral or other specified basis.

Option 1 – Pro-privacy settings enabled by default
Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.

Option 2 – Require easily accessible privacy settings
Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

As outlined in the Discussion Paper there are pros and cons to both options. We submit a hybrid solution may be more appropriate requiring entities providing social media services, relevant electronic services and designated internet services to:

a) Enable pro-privacy settings by default for children; and
b) Provide easily accessible privacy settings for individual users either through a portal or single click functionality.

Pages 111-114 **Right to object and portability**

Proposal 14.1: An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

In the Discussion Paper there is reference to the following circumstances where further collection, use or disclosure is required:

"• to complete a transaction or give effect to a contract
- *to provide a service or product the individual has requested*
- *due to the application of an Australian law, court or tribunal order*
- *due to a permitted general or health situation, or*
- *to assist a law enforcement body undertake an enforcement-related activity."*

For the sake of clarity, we respectfully submit the first circumstance should be suitably amended to:

*"• to complete a transaction or give effect to **or enforce rights under** a contract"*

A further circumstance should also be added to the list, being:

"• to meet credit reporting obligations"

Pages 115-123 Right to erasure of personal information

Proposal 15.2: Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.

We support the provision of exceptions to the right to erasure but respectfully submit the possible exceptions should also include:

"• *where the information relates to existing or anticipated disputes or proceedings between the entity and the individual which are to be resolved through internal dispute resolution, an external dispute resolution scheme or an ombudsman service"*

It is relevant to raise the issue of practicality and costs of erasure of an individual record. We respectfully submit there should not be any requirement for an entity to delete an individual information record from backup tapes:

a) in circumstances where it is costly or burdensome to do so, unless and except where the risks significantly outweigh the cost/burden; or

b) where it is impossible to delete any individual record from the backup dataset

Page 124-136 Direct marketing, targeted advertising and profiling

We agree with the observations in the Discussion Paper that targeted advertising is increasingly integral and critical to marketing strategies for businesses allowing them to direct advertising at the customer pool most likely to purchase their goods and services – this is equally important for large and small businesses in the digital economy.

Targeted advertising is also beneficial to consumers, ensuring they hear about goods and services that are more relevant to them, and supporting richer online experiences.

Question: Should express consent be required for any collection, use or disclosure of personal information for the purpose of direct marketing?

What is the extent of any real privacy concern to be addressed here, given users already have the ability to: opt out of unwanted marketing; set their emails to block direct marketing or other unwanted emails; and set their browser not to accept cookies from any or all websites? Is there an actual issue warranting the risk of notice fatigue for users and otherwise complicating what already works?

Question: What are some of the practical challenges of implementing a global opt-out process, to enable individuals to opt out of all online tracking in one click?

It is not evident from the Discussion Paper how a "global opt-out process" would actually operate. Is it envisaged to be similar to the Do Not Call Register?

A practical obstacle to a viable "global opt-out process" is the reality individuals often use multiple devices with multiple logins and/or no login to connect to the internet. In such circumstances, how would an entity be able to identify with any accuracy whether a connected user had previously opted out?

To illustrate, consider this scenario:

- Customer A exercises their right to request an entity to not use their information for marketing purposes
- Customer A then uses an unknown device to access the entity's website
- Customer A when later accessing Google on that same device sees the entity's targeted advertisement
- How was the entity to know not to present this advertisement to Customer A in such a scenario?

Similarly, the above scenario will impede entities in meeting the below obligation detailed in proposal 16.1:

> *"On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection."*

Pages 140-143 Accessing and correcting personal information

Proposal 18.1: An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

In the context of debt collection, proposal 18.1 may potentially lead to adverse consequences for a third party disclosed as the source of personal information about an individual.

The situation is the flip side to the situation detailed in response to proposal 8.4 - disclosing the identity of a third party may lead to personal or family violence; reputational harm; or other retaliatory actions by the individual to whom the source is disclosed.

We therefore respectfully submit that the following words be added to the end of proposal 18.1:

> ***"or might adversely impact the privacy or safety of another individual."***

Proposal 18.2: Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

- **the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.**

This proposal is supported by ACDBA.

Pages 168-172 Cross-Border Privacy Rules and domestic certification

Proposal 23.1: Continue to progress implementation of the CBPR system.

The benefits of yet another compliance certification system for Australia, given the likely significant associated costs for entities is not apparent.

Many Australian entities are ISO-27001 accredited[4], representing a significant investment by each entity to attain and maintain accreditation. Introducing a further compliance standard reliant upon engagement of a third party Accountability Agent will be unreasonable given the likely significant overlap in accreditation standards and processes and the costs involved.

Additionally, outsourcing to a third party to manage customer privacy complaints is unlikely to be an attractive or viable proposition for many entities and in some cases would be contractually prohibited by their clients.

The CBPR system might theoretically be appropriate but in practical reality, another certification standard and practice will only add further costs to business for little, if any real benefit to the entity and little, if any corresponding benefit for consumers. This is manifestly the case for entities not trading outside Australia.

Proposal 23.2: Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.

We refer to the above comments in relation to proposal 23.1 and similarly note the absence of any significant benefit to entities for participating in a voluntary domestic privacy certification scheme which would be additional to existing certification schemes supported, such as ISO-27001.

A more viable proposition for business, we submit would be for the OAIC to work with Standards Australia in respect to its ISO-27001 standard to facilitate inclusion of any missing elements that a domestic privacy certification scheme would offer, thereby allowing Australian businesses to make best use of their existing commitment to the ISO-27001 standard.

Costs borne by business entities are ultimately costs passed onto consumers – for this reason, any certification scheme should be introduced reluctantly and only where it provides demonstrable benefits to consumers and is carefully designed to prevent any duplication with existing certification schemes.

[4] ISO 27001 Information Security Management System - www.standards.org.au/standards-catalogue/sa-snz/communication/it-012/as--iso-slash-iec--27001-colon-2015

Pages 173-185 Enforcement

Question: Is it necessary and appropriate to give the Federal Court the express power to make any orders it sees fit or should the amendment only enable the Federal Court to make compensation orders in addition to an order imposing a pecuniary penalty?

In respect to the above question regarding proposal 24.6, ACDBA submits the better option would be to only enable the Federal Court to make compensation orders in addition to an order imposing a pecuniary penalty - this is a more measured and balanced solution to obviate the need to file two separate applications for the purpose of ordering a respondent to pay compensation.

Proposal 24.7: Introduce an industry funding model similar to ASIC's incorporating two different levies:

- **A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and**
- **A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.**

This proposal is not supported. There are already many taxes and levies imposed upon industry – those imposts are not on government enterprises. The extent and quantum of existing cost recoveries from industry is overwhelming and oppressive for many businesses struggling to survive through the health pandemic and now attempting to regroup as Australia adjusts to changed work and life expectations post COVID. Business can ill afford a further industry funding levy.

In any event the rationale for industry funding requires deeper consideration than set out in the Discussion Paper. For example, why should compliant industry participants in any funding recovery model, be responsible for costs which relate to poor conduct by others?

A fairer and more reasonable approach is for the OAIC to recover the costs of enforcement in any proceedings initiated against non-compliant entities, rather than there being any expectation or reliance on compliant industry participants to fund such enforcement.

A more balanced approach is for Australia's privacy framework, including its OAIC oversight, to continue being from consolidated tax revenues on the basis privacy protection from non-compliant conduct is extended to all Australians, regardless of whether the non-compliant conduct is by government, industry, non-for-profits or any other entity. This is a fairer and more equitable basis for funding.

The Discussion Paper references "cost recovery levies and statutory levies have been successfully implemented by other regulators including ASIC". What is the basis for measuring and claiming such successful implementation?

Is the only measure of success simply that industry is paying over funds?

Any assessment of successful implementation requires consideration of what benefits the levy has brought to consumers, and whether such benefits outweigh the cost impost on industry, ultimately passed onto consumers in the form of higher costs for credit or services.

Proposal 24.9: Alternative regulatory models

Question: Which option would most improve the complaints handling process for complainants and allow the OAIC to focus on more strategic enforcement of the Act?

As an overarching observation, our members report that the current processes relating to privacy complaints, particularly the early resolution process, are highly effective and ask is there a compelling need for change?

Early resolution delivers positive consumer outcomes with most issues resolved promptly between the parties - benefiting consumers who as a cohort do not want a lengthy complaints process but simply want their concern resolved.

Our members are of the view nothing further appears warranted at this time and view having another ombudsman scheme involved in complaint processes as unhelpful and certain to add costs for participants.

In these circumstances, the benefits of any proposed change need to be clearly quantified and articulated before implementation so as to ensure the aspirant outcomes justify the cost impost.

Our opposition to the creation of another ombudsman scheme is that to require multiple memberships will only lead to duplication and increased costs which would ultimately be passed on to consumers in the pricing of credit or services.

Multiple schemes additionally run the real risk that for resolution of privacy complaints, consumers may be tempted to forum shop.

As a general premise, we submit no entity should be required to be a member of more than one EDR or Ombudsman scheme in order to meet their privacy obligations.

Further, the rationale advocated by the Federal Government to streamline external dispute resolution has been to replace a number of predecessor schemes by creating AFCA to act as a "One Stop Shop" for consumers in resolving their financial complaints.

In November 2021 the Government confirmed its strategy when responding to Treasury's Review of AFCA by welcoming the overall finding that AFCA is performing well and providing an effective dispute resolution service for consumers and small businesses.

While we submit there is no imperative for change at this time, in the event the Government elects to create a further Ombudsman scheme for privacy complaints, we respectfully submit it should apply only for entities not already members or agents of members of AFCA or other EDR scheme and that the jurisdictions of those existing schemes be extended where necessary to include privacy complaints.

Further, the design of any special purpose Ombudsman scheme established for privacy complaints should address such valid considerations as:

- Avoidance of excessive delays in the resolution of complaints including by expeditious use of reasonable offers made by the member during early complaint stages
- Minimisation of costs to members for complaint resolution

- Avoidance of misuse of complaint processes by for-profit intermediaries adopting manipulation of such processes in their business model
- Ensuring the basis of complaints is not unreasonably expanded during resolution processes
- Ensuring non-meritorious complaints and vexatious complaints are promptly closed down

Pages 186-190 A direct right of action

Question: Is each element of the proposed model fit for purpose? In particular, does the proposed gateway to actions strike the right balance between protecting the court's resources and providing individuals a more direct avenue for seeking judicial consideration and compensation?

The Discussion Paper signals significant support for a direct right of action but it is appropriate to note establishing such a right will almost certainly lead to the emergence of a cottage industry of professional plaintiffs and their solicitors/for profit representatives similar to the US experience for the various private rights of action in that jurisdiction.

If this occurs, Australia is likely to similarly experience frivolous claims and/or class claims filed solely to elicit settlements or force capitulation on the removal of credit defaults.

The scale of the US problem is enormous although the true extent is somewhat hidden with many claims being threatened including unfiled draft court proceedings being sent to would be defendants and the targeted defendants then settling the purported dispute without proceedings being filed.

The business model being pursued in the US is that opportunistic plaintiffs and their representatives works on the basis businesses will generally prefer to settle claims rather than to risk significant costs to establish their compliance with the law.

Unfortunately, Australia already has a significant existing problem with poor actors within the for-profit debt management space engaged in credit repair and debt negotiation – the issues they create being well understood by ASIC[5], AFCA, OAIC, Treasury, consumer advocates[6] and the business entities targeted.

Currently in Australia the financial services sector is significantly exposed to vexatious complaints and spurious claims. Adding another opportunity to pursue direct rights of action for purported privacy complaints is likely to add to the problems caused by the for-profit intermediaries and ultimately will result in consumer detriment, as those poor actors, in pursuit of their commissions inevitably will encourage additional spurious actions to be filed.

[5] Handling complaints and paid representatives: ASIC provides financial firms with guidance, 28 August 2020 - asic.gov.au/about-asic/news-centre/articles/handling-complaints-and-paid-representatives-asic-provides-financial-firms-with-guidance

[6] Consumer Action Law Centre Media Release, 4 May 2021 - consumeraction.org.au/asic-must-reject-licence-applications-from-predatory-debt-vultures

For these reasons we do not support the creation of a general private right of action, but instead support the establishment of a very limited right of action for a narrow range of highly offensive breaches such as intimate image abuse, bullying, perpetrating domestic violence, blackmail or inappropriately influencing family court proceedings.

Noting the concurrent proposals in this Discussion Paper to increase the powers of OAIC, to allow the courts to order compensation in OAIC actions and to provide for new civil penalties, we submit a broader private right is not warranted.

Pages 191-197 A statutory tort of privacy

Proposals 26.1-26.4:

Option 1: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

Option 2: Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

Option 3: Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

Option 4: In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

We do not support the introduction of a statutory tort of privacy.

Instead, Option 3 is preferred on the basis the extension of the Act to cover "information which would be highly offensive to an objective reasonable person" will provide an appropriate avenue of redress for the collection, use or disclosure of personal information leading to situations of intimate image abuse, bullying or perpetration of domestic violence.

Pages 198-206 Notifiable Data Breaches Scheme – impact and effectiveness

Question: What aspects of other data breach notification schemes might be beneficial to incorporate into the NDB scheme?

The current NDB scheme appears to be working well and achieving the main objectives of informing OAIC and individuals of breaches that are likely to lead to significant harm, whilst not causing notification fatigue though the adoption of the sensible standard of "likely serious harm" before reporting is required.

The Discussion Paper does not articulate any issues with the scheme other than the delay of some entities in reporting. On this basis, there does not currently appear to be any imperative to amend the NDB scheme that would justify the costs to industry of amending policies, procedures, training, controls and governance.

Contact

For any enquiry in relation to this Submission, please contact:

Mr Alan Harries
CEO
Australian Collectors & Debt Buyers Association
PO Box 295
WARATAH NSW 2298

Telephone: 02 4925 2099
Email: akh@acdba.com

Appendix 1 - Members of Australian Collectors & Debt Buyers Association

- Axess Australia Pty Ltd
- CCC Financial Solutions Pty Ltd
- CFMG Pty Ltd t/as reminda
- Charter Mercantile Pty Ltd
- CollectAU Pty Ltd
- Collection House Limited (ASX: CLH)
- Complete Credit Solutions Pty Ltd
- Credit Collection Services Group Pty Ltd
- Credit Corp Group Limited (ASX: CCP)
- Debt Force Pty Ltd
- Lyndon Peak Pty Ltd t/as Access Mercantile Services
- PF Australia Pty Ltd
- Pioneer Credit Limited
- PRA Australia Pty Ltd
- Prushka Fast Debt Recovery Pty Ltd
- Recoveries Corporation Holdings Pty Ltd
- Shield Mercantile Pty Ltd
- Standard8 Advisory Pty Ltd
- Strategic Collections Pty Ltd

Appendix 2 - Debt Purchasing explained

Debt sale contracts exhibit the features of outsourced service provision rather than asset divestment - the contracts contain substantial ongoing conduct obligations and restrictions imposed on the purchaser, which are supported by warranties, indemnities and other potential penalties. The conduct obligations deal with matters such as ongoing compliance with laws, codes, guidelines, data security, principles of fairness and policy directives of the seller.

These contractual requirements are supported by ongoing reporting obligations for matters including breaches, complaints and the identification of customers in sensitive circumstances. There are provisions for extensive auditing, on-site visits and regular review meetings to share emerging issues. Sellers retain substantial discretion to recall individual customer accounts at any time.

The contractual elements create an outsourcing relationship granting the seller substantial control over the ongoing conduct of the purchaser and the experience of individual consumers.

It is appropriate to note ASIC as the regulator for the financial services industry provides guidance in respect to conduct relating to a debt[7]:

> *A creditor may also remain liable for conduct regarding a debt despite having sold or assigned the debt. Liability will generally remain for misconduct occurring before the sale or assignment of the debt.*

Accounts assigned to debt purchasers by original credit providers typically involve debts where an acceleration clause in the financial agreement has been triggered by the consumer's default in making repayments. Once a debt has been accelerated, the amount owing is immediately due and payable.

Many, if not most consumers with accelerated debts are likely to be in hardship giving rise to complex, contested and unresolved issues.

Debt purchasers are specialists in dealing with and managing hardship as they almost exclusively interact with customers in some form of financial difficulty.

Debt purchasers do not establish separate hardship teams and do not need to implement protocols and systems to identify hardship. Rather, they proceed on the basis that every customer is in hardship. This means that every customer receives an empathetic and understanding experience designed to reach mutual agreement on a sustainable repayment arrangement.

The debt purchase business model includes two key features being:

a. The model is uniquely suited to the promotion of affordable and flexible long-term payment arrangements which most effectively respond to individual customer circumstances

b. Debt purchasing involves the assignment of permanent tenure to defaulted loans at prices which represent a substantial discount to the face value outstanding

The benefit of these two features is allowing debt purchasers to agree to longer-term payment arrangements with lower and more affordable repayments for the customer in hardship and to take a patient approach to understanding and accommodating individual customer circumstances.

[7] Equifax Default Information Guide version 23.0 - February 2019

Each year ACDBA members and other industry firms participate in a data survey to provide industry wide demographics. Reviewing the data survey for FY2021 reveals there were 2.98 million accounts with a total face value of $13.9 billion under collection that had been purchased from originating credit providers.

These aggregated figures reveal a low average value per account of only $4,664.

Debt purchasers handle a range of debt values in their portfolios from lesser amounts in respect to telecommunication debts through to larger amounts for higher value credit card and other banking product debts.

Survey respondents in FY2021, reported for both debt purchase and contingent collections collecting $1.55 billion of defaulted consumer credit obligations, restructuring $3.06 billion into sustainable repayment arrangements together with a $1.16 billion in hardship arrangements and waiving a further $54.7 million owed by vulnerable customers in financial hardship.