14 January 2022

Attorney General's Department
by email: PrivacyActReview@ag.gov.au

Privacy Act Review, Discussion Paper

Thank you for the opportunity to comment on Privacy Act Review, Discussion Paper. This is a joint submission from the Financial Rights Legal Centre (**Financial Rights**) and Financial Counselling Australia (FCA).

Financial Rights and FCA supports the vast majority of the proposals put forward in the Discussion Paper to reform the *Privacy Act*, which, if adopted will go a long way to addressing the issues faced by consumers of the financial services industry.

While we do not provide comment on each of the proposals put forward, we provide the following responses to the specific questions posed on proposals where we can contribute or provide further insight.

2. Personal information, de-identification and sensitive information

- **In practice, what types of information would the proposed definition of personal information capture which are not presently covered?**

We support proposals 2.1, 2.2 and 2.3 to amend the definition of personal information to make clear that it includes technical and inferred information – in line with our previous recommendation.[1] We also support the proposed non-exhaustive list of technical and personal information examples listed in the paper factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person.).

Doing so will create greater regulatory oversight of the use and misuse of data to create detailed pictures of consumers exposing them to risks of re-identification, manipulation, exclusion and discrimination.

[1] Joint consumer submission to the Attorney-General's Department's Privacy Act Review: Issues Paper https://financialrights.org.au/wp-content/uploads/2020/12/201127_PrivacyActReview_IssuesPaper_FINAL.pdf

One sector steeped in personal information that is likely to use, and in fact is already using technical and inferred information regarding individuals, is the general insurance sector.

Insurers obtain a broad range of data for the purpose of assessing risk which is used in the process of underwriting, pricing and ongoing risk management. Insurers obtain the data from a range of sources. The data collected can include:

- consumer data
    - provided by consumers during the process of quotation
    - provided by other parties with consumer approval at the time of quotation (e.g. medical record for travel insurance)
    - collected following the process of sale, the most prominent example being telematics (e.g. telematics data acquired from customer)
- public data that is:
    - freely available to insurers and customers (e.g. data from Geoscience Australia)
    - available only to insurers (the national flood information database, NFID)
    - available at a cost (e.g. purchased by insurers)
- privately acquired data; that is acquired, and or generated, by the insurer. For example, the insurers may analyse the claims data they hold (or have access to) to assess risk.

A significant concurrent development is the increased role of insurers in undertaking risk management through monitoring of behaviour and risk. This is occurring most prominently in the case of motor vehicle insurance, whereby insurers use in-vehicle telematics to capture consumer data on behaviour, but could also arise from smart devices on home products, smart phones and fitness wearables (in the life insurance context)

In such cases the telematic services provider is usually the holder of the data and has an agreement with the vehicle user and the organisation monitoring the driving. Where the data has been used for insurance purposes, an aggregated measure (i.e. a driving score) has been passed to the insurer. Some telematic solutions are based on data captured using the mobile phone.

It is our view that most if not all of the information described above could potentially and should be captured by the new definition, including consumer telematics data, aggregated measures and other analyses used to identify behavioural characteristics of an insured person.

Public data relating to say the property of an individual or individuals that can be used to locate or identify an insured person should be captured. General information about a particular area that somebody lives – such as a flood plain or a postcode – can also potentially infer economic, cultural or social characteristic of a cohort to which an individual can be associated. If this information is linked to a specific individual in their risk profile then this link should be captured.

Privately acquired data that ultimately infers characteristics about an individual and which can be used to identify or associate an individual should also be included.

- **What do APP entities estimate are the costs and benefits of amending the definition of personal information in the manner suggested?**

- **Would the proposed definition of personal information pose any unintended consequences for APP entities? How could these be mitigated?**

We note that the Insurance Council of Australia have expressed concern that:

> *If a broadening of what constitutes 'personal information' results in less data being available for public use, this potentially limits the opportunities for insurers being able to draw on emerging data and trends to price for risk, undertake product innovation, engage with consumers and manage claims.*[2]

The aim of broadening what constitutes 'personal information' in an insurance context is not necessarily to limit the appropriate and socially valuable use of data analysis for identifying and measuring risk. It is to ensure that consumer protections are in place to collect, handle, store, and use this information in ways that improve safety and security of consumers, for consumers to access and understand this data and oversee potential uses that produce discriminatory or exclusionary outcomes. It simply creates a reasonable framework to provide certainty for industry and confidence for consumers that personal information will not be misused or exploited in harmful ways. It will not prevent the insurance sector from undertaking its important role in covering risks.

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

We recommend expanding the definition of sensitive information to ensure additional protections (including consent for collection and placing requirements on its use and disclosure) are applied to categories of information that act as proxies for already listed sensitive information.

Sensitive financial and/or transactional information can be used to:

- discriminate via proxy variables that stand in for omitted categories such as postcode for race and ethnic origin, the purchase of certain goods or services for sexual identity, religious or political affiliation etc.; and
- inappropriately discriminate on price where Australia's most vulnerable, disadvantaged and financially stressed households, or cultural and ethnic groups are identified and, for example, unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders.

[2] https://insurancecouncil.com.au/wp-content/uploads/resources/Submissions/2020/2020_12/2020_12_Privacy%20Act%20Issues%20Paper%20Submission.pdf

Sensitivity is contextual. Certain information in the hands of one party may be mundane and uncontroversial but highly sensitive and consequential in others. It can be used for good and it can be used for ill.

Analysing consumer financial data to, for example, identify that an individual is either a perpetrator or victim of financial or other abuse could be used to benefit the victim to provide actions or services that will assist that person. Lenders can and do use data analysis of transaction data to identify those who are experiencing financial hardship and provide appropriate support measures including offering to move people into basic bank accounts – as now required under the Banking Code of Practice.[3]

However correlative historical spending patterns from bank records, food data or grocery spending data could conceivably be analysed to assess risk in ways that could be inappropriate and discriminatory. For example, the purchasing of folate could infer that somebody is pregnant or seeking to become pregnant which may impact upon the willingness of a lender to provide credit, or provide credit at a higher price. Lenders could also use spending data to identify individuals with certain sensitive traits (such as ethnicity) and then target those individuals, to provide certain products at higher prices.

The increased application of the Consumer Data Right (**CDR**) to banking data will promote the use and analysis of financial transaction information to infer characteristics of consumers by CDR participants and non-participants including "trusted advisers."

It is critical therefore that this information is not used in ways that exploit or harm consumers. Increased protections and oversight should be explicitly extended under the *Privacy Act* to those areas including financial and transactional information that can either infer or act as a proxy for current categories of sensitive information.

- **What further information or guidance would assist APP entities when classifying biometric information, biometric templates or genetic information as 'sensitive information'?**

Two uses of biometric tools that need to be considered and incorporated under any expansion of the definition of sensitive information are:

- The use of Face ID and Touch ID for identification, security purposes in financial transactions, such as Tap Pay
- The capturing of information using biometric tools such as wearable health devices like Fitbits or Apple Watches in the life insurance space.

4. Small business exemption

The small business exemption must be removed.

[3] See paragraph 165 Banking Code of Practice, https://www.ausbanking.org.au/wp-content/uploads/2021/03/2021-Code-A4-Booklet-with-COVID-19-Special-Note-Web.pdf

We reiterate our concerns with respect to opening up financial data obtained under the CDR to so called "trusted advisers" (including small businesses not captured by the *Privacy Act*) under the latest iteration of the CDR rules.[4]

Recent amendments to the CDR Rules introduce the ability for CDR consumers to provide consent for the disclosure of their CDR Data to a "Trusted Adviser" including qualified accountants, persons who are admitted to the legal profession, registered tax agents, BAS agents and tax (financial) advisers, financial counselling agencies and mortgage brokers. Many of these are small businesses that would fall within the current exemption and therefore do not have to meet the standards required of them in the collection handling and use of consumer data either under the *Privacy Act* or the CDR with its strengthened privacy safeguards. This is a significant risk for consumers and for the confidence in the CDR regime itself.

We note that the Privacy Impact Assessment (**PIA**) for this new rule identified significant risks for consumers and recommended that Treasury mitigate these risks. They recommended (amongst other things) only allowing CDR Data to be disclosed outside of the CDR regime to Trusted Advisers who are APP entities for the purposes of the *Privacy Act* or only allowing CDR Data to be disclosed outside of the CDR regime to Trusted Advisers who have agreed (through a contractual arrangement with the Accredited Data Recipient) to effectively comply with the requirements of APP 1, APP 6 and APP 11, and the Notifiable Data Breach scheme.[5]

Treasury unfortunately did not accept these recommendations. In doing so they stated;

> *The classes of trusted adviser include professions that are regulated and subject to professional duties and oversight that provide an appropriate level of consumer protections. While many trusted advisers will be APP entities under the Privacy Act, requiring all trusted advisers to be subject to the Privacy Act may unduly impede consumer choice in circumstances where professional oversight and regulation exists*[6]

We respectfully disagree with Treasury's position. Professional duties and oversight may provide some protection for consumers but fiduciary and best interests rules are not the same in form or in substance as either strengthened CDR privacy safeguards, CDR accreditation standards or protections/requirements afforded under the *Privacy Act*. The PIA stated:

> *We do note that the limitation of the classes of entities who can be Trusted Advisers, where those classes will have fiduciary or regulatory obligations, does somewhat mitigate this risk. However, as was pointed out to us during stakeholder consultations, those obligations can offer*

[4] Joint consumer submission to the Attorney-General's Department's Privacy Act Review: Issues Paper https://financialrights.org.au/wp-content/uploads/2020/12/201127_PrivacyActReview_IssuesPaper_FINAL.pdf

[5] Page 36 Maddocks, Consumer Data Right Regime Update 3 to Privacy Impact Assessment Date of analysis: 17 September 2021 Report finalised on: 29 September 2021

[6] Page 5 Treasury, Consumer Data Right, Privacy Impact Assessment Agency Response October 2021

less protection for CDR Consumers than the strong privacy protections imposed under the CDR regime, or under the Privacy Act[7]

Under the current state of affairs – those consumers who port their financial data under the CDR to small businesses who do not meet the current thresholds under the *Privacy Act* will be provided few if any genuine preventative protections or protections after things go wrong.

Removing the small business exemption under the *Privacy Act* will, at the very least, provide a level playing field for consumers who currently face the risk that if a problem were to arise, they are not protected because the "trusted adviser" or small business happens to fall in the current loophole.

Finally, we agree with the Consumer Policy Research Centre (**CPRC**) that any complex system of exemptions, exceptions and loopholes is simply bad for business and bad for consumers. The current exemption and the alternatives to removing the exemption being considered place the onus on already overburdened consumers to learn, comprehend and understand the privacy, safety and security consequences of a decision to engage with a 'small business' no matter how defined. It assumes that consumers can inform themselves and consider complex data handling practices, unknown privacy harms that may materialise in the future and the many purposes for which their personal information may be handled, rather than allowing them to be confident that the business will simply protect their personal information. Simplicity, consistency and clarity should be principles that guide the design of the system.

If small businesses need support to get them up to speed with community expectations and new rules, this should be provided. We agree with the CPRC that Government should provide further resources to the Office of the Australian Information Commissioner (**OAIC**) to support this sector.

9. Consent to collection, use and disclosure of personal information

We support proposal 9.1 to strengthen what is required to demonstrate consent to apply to all APP entities.

- **Should entities be required to refresh or renew an individual's consent on a periodic basis where such consent is obtained for the collection, use or disclosure of sensitive information?**

Yes but that this should be for *all* consents including those related to sensitive information.

Current consent

We note that the Discussion Paper proposes to ensure that consent is "current" meaning "where the purpose for the collection, use or disclosure of personal information changes, consent should be obtained afresh" not "periodic renewal of consent to the collection, use or disclosure

[7] Page 36 Maddocks, Consumer Data Right Regime Update 3 to Privacy Impact Assessment Date of analysis: 17 September 2021 Report finalised on: 29 September 2021

of sensitive information, even where there is no material change to the purposes for use or disclosure, as contemplated by the Online Privacy code."[8]

This is a reflection of the current General Data Protection Regulation (**GPDR**) guidelines on Consent Article 29.[9] However we note that the WP29 states that:

> *WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights*

If consent were required to be "current" in the form proposed, it is conceivable that consents will be written in such a way that will ensure that "current" could be extended out to very long periods or, in some cases, in perpetuity decreasing consumer engagement with how their data is being used and how to exercise their rights.

While we acknowledge that over-burdening consumers with too many consent can reduce their effectiveness, decreasing consumer engagement with consents to the point of zero or "set and forget" can have a similar if not worse impact.

Where there are more regulatory protections in place to curtail and prohibit exploitative data practices, less engagement is required by consumers with their data, how it is used and any need to assert their rights. Consumers can in these circumstances have the confidence that the most egregious of use cases including for example, exploitative marketing practices or on-selling of data to third parties, will not generally impact them. Where there are fewer impediments, the balance needs to shift towards greater consumer engagement.

While we prefer the former to be the principle upon which the *Privacy Act* should be designed, we do not believe the balance has been struck here and that consents should be time-limited as they are under the CDR.

Withdrawal of consent

We note that while not included in proposal 9.1, proposal 14.1 recommends that:

> *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.*

We support this proposal however it should be strengthened to ensure that the consent should be able to be withdrawn as easy as it is to give consent.

Article 7(3) of the GDPR prescribes that the data collector (or controller)

---

[8] Page 77 Discussion Paper

[9] Article 29 Working Party Guidelines on consent under Regulation 2016/679 https://ec.europa.eu/newsroom/article29/redirection/document/51030

*must ensure that consent can be withdrawn by the data subject **as easy as giving consent** and at any given time*[10] *(**our emphasis**)*

We note that the CDR Rules employ the term "*easily* withdrawn" at Rule 4.9.

We also note that industry make processes to sign up to or subscribe and consent to services easy, while throwing in hurdles, dark patterns and multiple clicks to unsubscribe or withdraw from a service. Without expressly requiring consent to be "easily withdrawn" industry *will* comply with the requirement to allow one to withdraw consent but bury this withdrawal in websites, sub-menus, include pop-up alerts to ask whether you are sure you wish to withdraw, and other barriers to prevent the customer from withdrawing their consent.

- **Are there additional circumstances where entities should be required to seek consent?**

We agree with the OAIC that at a minimum the use of consent for situations in which the impact on an individual's privacy is greatest and "not require consent for uses of personal information for purposes that individuals would expect or consider reasonable."

It is important to note though that expectations have been eroded and altered over the preceding decade as businesses have vacuumed up personal data without express consent leading to dodgy data collection, handling and uses becoming the norm rather than the exception. Some consumers may have unfortunately become inured to these practices, and thus community expectations may have already shifted for the worse.

[10] https://gdpr-text.com/en/read/article-7/#:~:text=Article%207(3)%20of%20the,done%20through%20the%20same%20action.

10. Additional protections for collection, use and disclosure

- **Does the proposed fair and reasonable test strike the right balance between the interests of individuals, APP entities and the public interest?**

- **Does the proposed formulation of the fair and reasonable test strike the right balance between flexibility and certainty?**

We support proposal 10.1 so that a collection, use or disclosure of personal information must be fair and reasonable in the circumstances as an overarching requirement within the *Privacy Act*, with the list of legislated factors at proposal 10.2.

We also support the need to introduce an unfair trading prohibition more generally to complement this proposal and address the emerging range of unfair practices businesses adopt that are amplified in the digital age to complement these protections

With respect to the factors listed in proposal 10.2 we provide the following comments:

Reasonable expectations

We reiterate that certain consumer expectations may have been altered over the previous decade as businesses have pre-emptively collected, used and exploited without seeking the express, unbundled consent of consumers. Reasonable expectations would be very different if this proposal was made 10 years ago. The reasonable expectation factor therefore needs to be appropriately balanced with the risk of adverse impact or harm with this issue in mind.

Reasonably necessary to achieve functions and activities

We support this factor as proposed rather than the alternative regarding being reasonably necessary to achieve 'legitimate interests'.

However, we suggest that the collection, use or disclosure of personal information should be reasonably necessary to achieve the functions and activities of the entity's *in the provision of the product and/or service and its primary use (and legitimate secondary uses consented to).* Without this qualification the term could be interpreted so broadly as to capture all functions and activities that may take place within a business unrelated to the provision of the product and/or service.

- **Would the proposed definition of a secondary purpose inadvertently restrict socially beneficial uses and disclosures of personal information, such as public interest research?**

We support proposal 10.4 to define a 'primary purpose' as the purpose for the original collection, as notified to the individual and define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

If there is the chance that socially beneficial uses and disclosures of personal information, such as public interest research, are restricted – these should be included as exceptions as the GDPR does with respect to perform a task in the public interest.[11]

Alternatively we support the CPRC's proposal to develop a third tier (tertiary purpose) to clearly identify when personal information may be used for socially beneficial uses such as public interest research.

11. Restricted and prohibited practices

- **Would the introduction of specified restricted and prohibited practices be desirable?**
- **Should restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures, or should individuals be provided with more opportunities to self-manage their privacy in relation to such practices?**

We support the introduction of restricted and prohibited practices in the form outlined by Option 1 – that is APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks.

We note that the list of restricted practices references the concept of large scale processing as a limiting factor. It is important to clarify the meaning of large scale. In the UK[12] large scale can refer to

- t*he number of individuals concerned;*
- *the volume of data;*
- *the variety of data;*
- *the duration of the processing; and*
- *the geographical extent of the processing.*

Examples of large-scale processing include:

- *a hospital (but not an individual doctor) processing patient data;*
- *tracking individuals using a city's public transport system;*
- *a fast food chain tracking real-time location of its customers;*
- *an insurance company or bank processing customer data;*
- *a search engine processing data for behavioural advertising; or*
- *a telephone or internet service provider processing user data.*

It goes on to further clarify that:

---

[11] See Article 6 GPDR

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when12

Individual professionals processing patient or client data are not processing on a large scale.

One further point of clarification required is that processing by small and medium businesses should count as large scale. Otherwise, a loophole and exception will be created whereby some consumers will be protected and others not. They may also have a proportionately high impact on a significant proportion of a specific cohort – such as specific small businesses that serve specific ethnic or cultural groups.

- **What acts and practices should be categorised as a restricted and prohibited practice, respectively?**

We reiterate the list of practices listed in our previous submission[13] that need to either be restricted or prohibited altogether and separates them into the following categories:

Restricted

- the processing of data about minors
- AI informed decision-making including profiling
- the use of methods of tracking that individuals cannot control, for example, device fingerprinting
- the offering of incentives to consent to the commercial exploitation of personal data
- the secondary use of data for targeted/personalised marketing and the on-sale of personal data

Prohibited practices

- the collection of genetic test results as a requirement for providing goods and services or entering into a contract including life insurance;
- screen-scraping practices[14]
- concealed data practices[15]
- online tracking for targeted/personalised marketing purposes
- the for-profit trade in personal data through data brokers
- collection, use or disclosure that is otherwise unlawful

---

[13] Joint consumer submission to the Attorney-General's Department's Privacy Act Review: Issues Paper https://financialrights.org.au/wp-content/uploads/2020/12/201127_PrivacyActReview_IssuesPaper_FINAL.pdf

[14] For a full description of the problems with screen-scraping see Pages 10-18, Financial Rights Legal Centre and the Consumer Action Law Centre submission to the Senate Select Committee on Financial Technology and Regulatory Technology https://financialrights.org.au/wp-content/uploads/2020/02/191223_FinTechInquiry_Sub_FINAL-1.pdf

[15] as outlined in Page 2, Kemp, Nicholls https://www.accc.gov.au/system/files/Katharine%20Kemp%20%26%20Rob%20Nicholls%20%28March%202019%29.pdf

- profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law
- collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual
- publishing personal information with the intended purpose of charging individuals for its removal
- requiring passwords to social media accounts for the purpose of employee screening
- surveillance by an organisation through audio or video functionality of the individual's own device
- unfair trade practices such as dark patterns;
- the collection of location data unconnected to the fulfillment of a service

- **Should prohibited practices be legislated in the Act, or developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?**

Certain acts by businesses in collecting, handling, using personal data should be prohibited (as outlined above). This could be instituted through a combination of the two options being considered in the discussion paper – that is by embedding an inexhaustive list of specific prohibited practices into the legislation to send an explicit message to industry – complemented by Commissioner-issued guidance that interprets an overarching requirement of fair and reasonable personal information handling, providing further clarification to those listed practices, and articulating guidance on "proceed with caution" practices.

12. Pro-privacy default settings

- **Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access?**

Pro-privacy settings should be enabled by default, noting that there are some uses and circumstances where pro-privacy defaults may not be effective enough to avoid harm. These practices should be prohibited.

We note that Treasury has recently taken the opposite approach with respect to the sharing of joint account holder financial details under the CDR Rules. Treasury has introduced CDR rules that set as a default (under the pre-approval option) that CDR data relating to a joint account may be disclosed in response to a request by one Joint Account Holder (**JAH**) on the authority of that JAH *without* the approval of other JAHs.

This is a poor decision that will inevitably lead to consumer harm especially those vulnerable consumers subject to economic abuse. As the OAIC pointed out:

> *This is inconsistent with the fundamental principle of express consent for data sharing that is central to the operation of the CDR system. It would also appear contrary to both Australian*

and international best practice regarding consent, where the trend is towards requiring a positive act by an individual to indicate consent…[16]

Other stakeholders raised similar objections to the Treasury decision. The PIA found that:

> *The proposed change would have the impact of implementing an implied consent model, rather than the current express consent model. OAIC guidance indicates that an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, and that, generally, express consent should be sought where the personal information that will be handled has a degree of sensitivity.*
>
> *We are concerned that the proposed CDR Rules have serious consequences for the privacy rights of [the other] JAH. For example, even if JAH B later decides to change the disclosure option in DOMS, it is not clear that JAH B will be able to request that any previously shared joint account CDR Data be deleted by the relevant recipient.*
>
> *Removing the need for an active step that clearly indicates informed consent to the disclosure of CDR Data may be inconsistent with community expectations about the CDR regime.*

Treasury rejected the PIA's reasonable recommendations for mitigating the issues raised.

Requiring easily accessible privacy settings (as Treasury have relied on to mitigate problems) will not help the JAH B in the CDR context because the information would have already been shared. This is likely to be the case under option B in the discussion paper is adopted. By the time a consumer finds out about or realises they are uncomfortable with a particular form of data sharing, the damage is likely to have already taken place.

Option B also places all the onus on the consumer to engage with the consent process and disclosures–something that the Discussion Paper acknowledges throughout the paper places too heavy a burden on consumers.

- **If pro-privacy default settings are enabled by default, which types of personal information handling practices should be disabled by default?**

All privacy settings should be default to the pro-privacy position.

If businesses are expecting concerned consumers to engage with these settings, then they should similarly have no worries if they are set in a pro-privacy default since –following this logic - those same consumers will engage with the settings to express their wants. The truth however is that consumers rarely engage with these settings and are, at times, led not to engage with them through the use of dark patterns. The onus should be placed on the businesses to make the case to change the settings and obtain their express consent, rather than the other way round.

If pro-privacy settings are enabled by default for a limited set of circumstances then we would support the default settings referenced in the discussion paper including:

---

[16] Page 67, Maddocks, Consumer Data Right Regime Update 3 to Privacy Impact Assessment Date of analysis: 17 September 2021 Report finalised on: 29 September 2021

- geolocation options
- optional processing of personal data
- personal information handling for a purpose other than for the performance of a contract
- settings which allow third parties to process personal data

as well as the restricted uses we listed above.

We also support the CPRC's position that the following common data practices should also have pro-privacy defaults set (if they are not otherwise restricted or prohibited):

- Using personal information to make predictions about a consumer.
- Collecting information about consumers from other companies.
- Sharing personal information consumers have provided with other companies.
- Selling personal information consumers have provided to other companies.
- Requiring more personal information than necessary to deliver products/services.

13. Children and vulnerable individuals

- **Are there other contexts aside from children's use of social media services that pose privacy risks to children, which would warrant similar privacy protections to those proposed by the OP code?**

Children's engagement with the financial services sector – particularly their transactions and banking pose unique risks to children and warrants similar privacy protections to those proposed in the Online Privacy Code.

The banking sector's historical engagement with children is not a positive one.

With respect to School Banking Programs, for example, ASIC found that:

> *Young children are vulnerable consumers and are exposed to sophisticated advertising and marketing tactics by school banking program providers.*
>
> *School banking program providers fail to effectively disclose that a strategic objective of these programs is customer acquisition.*[17]

CHOICE awarded the Commonwealth Bank's Dollarmites a Shonky in 2020 for its relentless marketing to children. A number of states have now outlawed the practice.

With access to payment and transaction histories of children, the potential for harm to arise from the misuse and exploitation of this data is ever present. It is therefore critical that

[17] ASIC REP 676 Review of school banking programs

children are protected from poor data collection use and disclosure practices by the financial sector.

Should consent of a parent or guardian be required for *all* collections of a child's personal information, or only for the existing situations where consent is required under the APPs?

Consent of a parent or guardian be required for *all* collections of a child's personal information

Should the proposed assumed age of capacity of 16 years in the OP Bill apply to all APP entities?

Yes

- **Should APP entities also be permitted to assess capacity to consent on an individualised basis where appropriate, such as in the healthcare sector?**

Only in limited circumstances such as in healthcare.

14. Right to object and portability

We support proposal 14.1 that an individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.

The only qualifications to this is that the withdrawal be just as easy as the original consent (see above) and that this occur without the qualification that businesses take reasonable steps – a qualification not proposed under proposal 16.1 re: direct marketing.

15. Right to erasure of personal information

- **In light of submitter feedback, should a 'right to erasure' be introduced into the Act?**

Yes

- **Should an erasure request be only available on a limited number of grounds, as is the case under Article 17 of the GDPR?**

A right to erasure – to be acted upon by businesses without undue delay - based on Article 17 of the GPDR should be introduced where:

- the data is no longer necessary in relation to the purposes for which it was collected: Article 17(1)(a)
- the individual withdraws consent or the relevant storage period has expired and the data holder doesn't need to legally keep it (such as banking records for a seven year time period): Article 17(1)(b)
- the individual objects to the processing of data – including direct marketing purposes and profiling: Article 17(1)(c) & Article 21
- the data was unlawfully processed: Article 17(1)(d)
- there is a legal requirement for the data to be erased: Article 17(1)(e) •

- the consumer is a child at the time of collection: Article 17(1)(e) & Article 8

There are also exceptions to this right in the EU, which include:

- exercising the right of freedom of expression and information: Article 17(3)(a)
- for compliance with a legal obligation, e.g. again as mentioned above a bank keeping data for seven years: Article 17(3)(b)
- for reasons of public interest in the area of public health: Article 17(3)(c)
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes: Article 17(3)(d)
- for the establishment, exercise or defence of legal claims: Article 17(3)(e)

Consumers have the reasonable expectation that once a consumer withdraws consent or their consent is expired, that their information will be deleted or destroyed in order to protect their privacy.

16. Direct marketing, targeted advertising and profiling

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

Yes consumer should have the unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing.

This should be defaulted in such a way that consumers must expressly opt in to direct marketing and that this be separately identified (unbundled) from other use cases – primary or secondary.

We support businesses having to notify consumers of their right to object in relation to each marketing product provided and that this right to object can be carried out easily and *instantly*.

With respect to the proposal to enhance information on direct marketing in the APP privacy policy providing information on the details of third parties regarding the appropriate method of opting-out of those materials – this is not a straightforward method of withdrawing their consent for consumers. We reiterate our recommendation that withdrawing consent should be as easy as providing it. Expecting the average consumer to search through an APP entity's privacy policy to find third party details, to *then* find out how to opt out with that third party is cumbersome and places an unrealistic onus on the consumer to act.

If a business is making a profit from working with third parties who directly market, these businesses should provide an easy, one step/click solution to opting out of marketing materials distributed by the third parties they work with. If one click solutions can be adopted elsewhere – this is particularly the case in a sales context – they can be done so here. Any costs that arise in implementing such a system can be factored into the profits made by both the APP entity and the third parties.

17. Automated decision-making

We agree with the CPRC in urging the Government to look beyond the notification model and consider specific safeguards in ensuring fairness and safety of consumers in the context of artificial intelligence. Specifically the Government should introduce the right for consumers to 'not to be subject' to certain forms of AI informed decision-making and requires businesses to implement measures to enable individuals to obtain human review of an AI informed decision, to express their point of view and to contest the decision – in line with Article 22 of the GPDR.

18. Accessing and correcting personal information

- **Is there evidence that individuals are being refused access to personal information that has been inferred about them? In particular, is the exception at APP 12.3(j) being relied on to refuse individuals' requests to access inferred personal information?**

Financial Rights is currently undertaking research into the privacy practices of general insurers. As a part of this research we have worked with consumers to obtain their own personal information held by insurers by exercising their rights to access their data (i.e. the APP12 'data subject access' right). The research is not focusing on obtaining inferred material – simply having consumers ask for all material held.

While the research has not been completed, preliminary insights have shown that:

- obtaining personal data held by general insurers is not at all straight forward;
- approaches to providing personal data and its form are inconsistent; and
- the volume and quality of the information provide varies wildly with most providing basic, minimal information about a claim, and a handful providing voluminous, inaccessible, and at times incomprehensible material upwards of 150 pages long, including screenshots of databases.

It is not clear whether any of the information provided is inferred personal information however we note that in some there are notes and indicators of risk categories to which insured are tagged, and are a form of inferred data.

We are unable to answer the question as to whether consumers are being specifically refused access to inferred information, however it is clear that consumers either:

- are provided some of this information in a voluminous data dump to interpret and understand for themselves; or
- need to explicitly request the specific information (inferred or otherwise) that they are seeking, which the consumer may or may not be aware exists.

This research will be finalised in the first quarter of 2022 and we will be happy to provide further insights to the AGD once complete.

In the meantime, we support proposal 18.3 to clarify the existing access request process in APP 12 to the effect that:

- an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, and
- where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual

However where voluminous or not readily understandable material is made available, the required summaries should delineate and explicitly address the categories of information held including:

- sensitive information held (e.g. in insurance: information about health, criminal histories, location data etc)
- inferred information held (e.g. in insurance: insights into risk categories)
- financial information held (e.g. in insurance: credit card and payment details)

- **Is there evidence to suggest that organisations are taking longer than a reasonable period after a request is made to grant individuals access to their personal information?**

Again the unfinished research we are undertaking has provided Financial Rights with some preliminary insights into the timeframes and process it takes to receive personal information:

- Most participants obtained some basic information fairly quickly (between 1 and 5 days), but others took up to 30 days to receive their personal information – be it basic or more expansive. However we are aware of one participant waiting over 45 days and another participant who it took over 3 months to obtain the requested material.
- Participants variously found that they either did not receive or had delayed responses confirming their request.
- A number of participants had to engage multiple times with the insurer to clarify the request or seek further information.

24. Enforcement

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

We support Option 2 – creating a Federal Privacy Ombudsman (**FPO**).

When a consumer has an issue or complaint relating to a business and their practices - be it a privacy issue, a data handling issue or poor service issue – they want their complaint dealt with by the business quickly and efficiently. They generally do not conceive of the problem through the lens of categories or types of complaint – they simply see it as a complaint about the entity or its service/product.

When a consumer is unable to have their complaint resolved by the business directly (via internal dispute resolution (**IDR**) or some other front line service) consumers need to know who

they can turn to, to make a complaint. Where there are multiple external dispute resolution (**EDR**) schemes this can cause consumer confusion, delays and stress navigating the rules and processes.

In the financial services sector context much of this confusion was resolved by rolling three ombudsman services into the one service – the Australian Financial Complaints Authority (**AFCA**). However given the nature of complaints that are arising in the context of an increasingly digital economy, consumers still face confusion.

For example, if a consumer has an issue with respect to a phone banking application inappropriately inferring a characteristic about a consumer from their transaction history that has led to their being offered higher priced credit, a consumer not versed in the complexities of the EDR environment could think they need to complain to either:

- AFCA, because it is a financial service;
- the OAIC, because there may be a privacy issue related to misuse of personal information;
- the Australian Human Rights Commission, because of potential 'discrimination' issues; or
- the Australian Competition and Consumer Commission (**ACCC**) for potential price discrimination issues.

The productivity commission recommended in its *Data Access and Availability* report[18] that there be a 'no wrong door' approach to designing a regime for dealing with consumer data issues and complaints. This has for all intents and purposes been adopted under the CDR with the OAIC taking primarily responsible for consumer complaints about privacy and data handling in the CDR system but EDR schemes like AFCA being able to accept complaints under s35A of the *Privacy Act*.

Wherever a consumer goes to make a complaint, they should be triaged to the appropriate body in as efficient and simple a process as possible that does not lead to subsequent withdrawal of complaints borne of frustration with the bureaucracy.

We generally support ongoing recognition and use of EDR schemes requiring APP entities to participate or contribute to a complaints handling scheme. But this *should be combined* with establishing a more distinct and accessible privacy complaints handling system distinct and independent from the OAIC's regulatory and enforcement roles.

We therefore support Option 2 - splitting off the complaints handling function of the OAIC to triage and conciliate privacy complaints into a separate FPO service – working with other recognised Ombudsmen and EDR schemes.

The current model combining enforcement, investigations, regulatory, guidance and complaints handling and conciliation roles is not best practice.

---

[18] Page 20, Productivity Commission, *Data Availability and Use Inquiry Report*, No.82, 31 March 2017 https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

The Australian and New Zealand Ombudsman Association (**ANZOA**) have raised issues with blurring the complaint handling role of an Ombudsman with other roles. They state:

> *Where problems arise in an industry or an area of government services, the call for an Ombudsman commonly follows.*
>
> *This is a testament to the high level of public respect for the independence, integrity and impartiality of Ombudsman offices. However, there is concern about the inappropriate use of the term Ombudsman to describe bodies that do not conform to, or show an understanding of, the accepted Ombudsman model and its 200 year history. If the concept of Ombudsman is applied inappropriately, public confidence in the role and independence of the Ombudsman institution is at risk of being undermined and diminished. Using the term Ombudsman to describe an office with regulatory, disciplinary and/or prosecutorial functions confuses the role of Ombudsman with that of a regulatory body. An 'ombudsman' office under the direction or control of an industry sector or a government Minister is not independent. An office set up within a company or government agency as an 'internal ombudsman' is not independent.*[19]

Furthermore, ANZOA state:

> *An Ombudsman is not an advocate. An Ombudsman is not a regulator. The fundamental role of an Ombudsman is independent resolution, redress and prevention of disputes.*[20]

Continuing the status quo or adopting Option 3 will further undermine the confidence of Australian consumers in the role and independence of the OAIC and the ability to have their complaints dealt with in an appropriate manner, within an appropriate regime.

Consumers need to have confidence in an external dispute resolution system in the privacy and information space. To do so requires an Ombudsman to be

- independent of government and industry
- have a clearly defined jurisdiction,
- have appropriate powers to investigate individual complaints and systemic issues;
- accessible to all and free to the public
- procedurally fair; and
- accountable.[21]

There is also merit in extending the jurisdiction of an FPO to include other privacy related issues in the digital space and data and information space more generally. As the CPRC points out the ACCC has also recommended the establishment of an ombudsman scheme but only on issues relating to digital platforms.

---

[19] http://anzoa.com.au/about-ombudsmen.html

[20] http://www.anzoa.com.au/

[21] http://www.anzoa.com.au/assets/anzoa_media-release_essential-criteria-for-use-of-the-term-ombudsman_18may2010.pdf

In establishing an FPO we support this occurring in parallel to the proposed strengthening of the OAIC's enforcement roles including:

- creating tiers of civil penalties (proposal 24.1)
- clarifying what a serious or repeated interference with privacy (proposal 24.2)
- enhancing the OAIC's proactive investigation powers (proposal 24.3)
- empowering the OAIC to undertake public inquiries and reviews into specified matters (proposal 24.4)
- requiring an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss (proposal 24.5)
- giving the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established (proposal 24.6) and
- funding the OAIC through an industry funding arrangement (proposal 24.7)

With respect to the proposal (24.7) to fund the OAIC through an industry funding arrangement, this model should be extended to provide adequate funding to a new FPO.

With respect to amending the annual reporting requirements in the *AIC Act* to increase transparency about the outcome of all complaints lodged (proposal 24.8) this should also be applied to and incorporated into the establishment of a FPO.

25. A direct right of action

- **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?**

We support the model outlined at proposal 25.1 which strikes the right balance by encouraging conciliation but not strictly requiring it. However we note that in order to support this system access to free and independent advice and representation is essential to support consumers through the process, particularly for consumers experiencing vulnerability and disadvantage.

26. A statutory tort of privacy

We support proposal 26.1 Option 1 .re: introduction a statutory tort for invasion of privacy as recommended by the Australian Law Reform Commission Report 123. However this should be modified to the extent described by the Public Interest Advocacy Centre in its submission to the issues paper[22] – namely – including listing additional matters be included as to whether there is a reasonable expectation of privacy and extending the tort to negligent invasions of privacy, amongst others.

[22] https://www.ag.gov.au/sites/default/files/2021-01/public-interest-advocacy-centre.PDF

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact at via the details below

Kind Regards,

Drew MacRae
Senior Policy Officer
Financial Rights Legal Centre
Direct: (02) 8204 1386
E-mail: drew.macrae@financialrights.org.au