Financial Rights LEGAL CENTRE

Submission by the Financial Rights Legal Centre

Senate Economics Legislation Committee

Inquiry into Treasury Laws Amendment (Consumer Data Right) Bill 2018

February 2019

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 |
info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Financial Rights took close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to
www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

Introduction and Executive Summary

Thank you for the opportunity to comment on Treasury Laws Amendment (Consumer Data Right) Bill 2018.

Financial Rights has made a series of submissions to the Productivity Commission's Data Availability and Use Report, Open Banking Review, Treasury's Consumer Data Right legislative development, the ACCC CDR Rules and Treasury' Privacy Impact Assessment.[1] These submissions outline fundamental concerns that we have held and continue to hold with respect to the development of an open banking regime and consumer data right. In summary these concerns are:

- **Increased complexity and choice:** Greater choice, increased competition and new products may bring some efficiencies and benefits to some people, however greater complexity, choice and transaction speeds in open banking and consumer data products and services will likely result in information overload and too little time to make decisions, less consumer understanding and market inefficiencies.
- **Increased economic inequality and financial exclusion:** Risk segmentation, profiling for profit, price discrimination and the delivery of poor, unsuitable products are all likely outcomes of greater access to consumer data by FinTechs. Those experiencing financial hardship are often very profitable to debt management firms and fringe financial service providers and therefore most vulnerable to exploitation. Those in more precarious financial situations are more likely to be unfairly charged higher amounts or pushed to second tier and high cost fringe lenders.
- **Increased information asymmetry and predatory marketing:** Access to data and continuous monitoring are likely to lead to predatory practices, for example by payday

[1] Submission to Treasury's Consumer Data Right, Privacy Impact Assessment, January 2019, https://financialrights.org.au/wp-content/uploads/2019/02/190118_CDRPIA_Sub_FINAL.pdf Submission to the Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation https://financialrights.org.au/wp-content/uploads/2018/10/181012_CDR-Second-Round_submission_FINAL.pdf; Consumer Data Right (CDR) Rules Framework, Sept. 2018 https://financialrights.org.au/wp-content/uploads/2018/10/181003_ACCC_CDRRULES_Submission_FINAL.pdf; Submission to the Treasury Laws Amendment (Consumer Data Right) Bill 2018; https://financialrights.org.au/wp-content/uploads/2018/09/180907_CDRLegislation_Submission_FINAL.pdf Joint consumer submission on the Open Banking: customers, choice, convenience, confidence Final Report, March 2018 http://financialrights.org.au/wp-content/uploads/2018/03/180323_OpenBanking_FinalReport_Sub_FINAL.pdf; Joint supplementary submission by the Financial Rights Legal Centre and Consumer Action Legal Centre Treasury Open Banking: customers, choice, convenience, confidence, December 2017 http://financialrights.org.au/wp-content/uploads/2017/10/171025-Open-Banking-Supplementary-Submission-FINAL.pdf, Joint submission by the Financial Rights Legal Centre and Consumer Action Legal Centre Treasury Open Banking: customers, choice, convenience, confidence, October 2017, http://financialrights.org.au/wp-content/uploads/2017/09/170922-FINAL-submission-open-banking-issues-paper.pdf; Submission by the Financial Rights Legal Centre Productivity Commission Draft Report: Data Availability and Use, October 2016 http://financialrights.org.au/wp-content/uploads/2016/12/161216_FRLCSubmission_draft-report-Data-Availability-use.pdf

lenders. There is also an increasing asymmetry of power in consent provision and contracting.

- **Increased unconscionable practices:** Closed proprietary algorithms could potentially lead to situations where consumers are denied access to crucial products and services based on inaccurate data without the ability to determine why or to correct underlying assumptions**.** Increased use of non-transparent, black box technology could also lead to poor consumer outcomes through the creation of potentially biased and discriminatory algorithms.
- **The use of inaccurate or flawed data with few avenues for individuals to correct errors in an efficient and prompt manner:** An economy increasingly reliant on data is wholly dependent on that data to be accurate. If there are roadblocks in place for consumers to get incorrect data corrected this will create serious problems for consumers
- **Increased privacy concerns relating to the security, portability and use of financial and personal data.** Consumers are more and more aware of the impact of the data that they are providing to digital platforms and services and are increasingly concerned about the impact upon their privacy rights and the protections in place about the use or their data.

The current Consumer Data Right (**CDR**) legislation addresses few of these concerns and those concerns that is does seek to deal with, it fails to address in any comprehensive manner.

Consequently, Financial Rights believes that the draft CDR legislation (and approach) is flawed in a significant number of ways.

The CDR is limited in scope and misleads consumers

The "Consumer Data Right" has been named and presented in a way that seems like it is establishing an all-encompassing, comprehensive consumer right. It is not. The "Consumer Data Right" is a misnomer. It is a Consumer Data *Portability* Right. It is not the introduction of a comprehensive set of consumer data rights like the European Union's General Data Protection Right (**GDPR**)**.** This is implicitly acknowledged in the *Explanatory Materials*[2] but not in its name.

The CDR is merely a collection of rights with respect to porting or transferring consumer data. It provides no further rights to more broadly access, restrict processing, object, delete, correct, and rectify one's data. The CDR is therefore misleading as consumers are being sold the idea of a "consumer data right" to protect consumers in their access to and use of their own financial data. Once CDR data inevitably falls outside of the system, lower or non-existent privacy rights apply.

[2] Para 1.1 "*The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties.*"

The CDR is piecemeal and expedites Australia falling behind the rest of the world

The portability rights created by the CDR will only apply to designated sectors as approved by the Minister. Currently this will be applied to the banking sector but will expand to cover other sectors such as energy, telecommunications, insurance, even social media. Given the timelines proposed, the application of strengthened privacy standards will take decades to spread to all aspects of the economy.[3]

Compare this to the approach being taken by the EU. The new EU GDPR has established a list of 20 Data Protection Rights that applies to all individuals and businesses across the entire economy including the Right to Access, Right to Deletion, Right to Rectification, etc. One of those rights is the Right to Portability. In this sense this "Consumer Data Right" will be one twentieth of the rights being provided to EU citizens, leaving Australian industry and consumers well behind.

Australian FinTechs wishing to work and compete internationally will have to establish multiple privacy safeguards and systems, placing our businesses at a strategic disadvantage.

The CDR is symptomatic of a lack of an integrated, holistic framework for consumer data management and regulation

The CDR legislation is one of at least four interrelated policy development processes underway that relate directly to the treatment of consumer data and the establishment of increased consumer protections in this regard. These policy processes are the Consumer Data Rights legislation (currently being considered by this committee);[4] the Data Sharing and Release Reforms,[5] the ACCC Digital Platforms Inquiry[6], and the Human Rights Commission's Technology and Human Rights project.[7] There appears to little if any coordination amongst these processes and the privacy protections being recommended in each of these vary in strength and at times contradict each other. This fractured approach poses significant challenges to both consumers and businesses.

What is required is a holistic approach that places consumers' right to privacy their interests in security front and centre of the establishment of a broad Consumer Data Right and

---

[3] The EDEM only states that: "*Over time it is expected that these same benefits will be rolled out to other sectors of the economy.*[3]

[4] The CDR is being established to allow consumers to ask for data to be safely shared with trusted recipients in specific sectors such as banking, energy and telecommunication services, and eventually for other services across the economy.

[5] The Data Sharing and Release Reforms ostensibly seek to promote better sharing of public sector data, build trust in use of public data, maintain the integrity of the data system, and establish institutional arrangements. https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms

[6] The Digital Platforms Inquiry is examining digital search engines, social media platforms and digital content aggregators.

[7] the Human Rights Commission is undertaking a significant project exploring the rapid rise of new technology and what it means for our human rights. The project aims to identify the practical issues at stake; undertake research and public consultation on how best to respond to the human rights challenges and opportunities presented by new technology, and finally develop a practical and innovative roadmap for reform

strengthened privacy regime. This means reviewing the out of date *Privacy Act* and Australian Privacy Principles (**APP**) first and then implementing a consumer data portability right.

The CDR establishes multiple privacy standards, confusing consumers and placing them at risk

The CDR creates a third privacy standard that applies to consumers seeking protection, security and redress when something goes wrong with their data. The CDR Data Privacy Safeguards as envisioned under this draft legislation will be an addition to the current *Privacy Act* safeguards as detailed under the APPs. Then there are the general consumer protections and laws that apply to those situations where holders of consumer data are *not* "APP entities" as defined under the APPs.[8]

The introduction of the CDR is an explicit acknowledgement that the current APPs are out of date, no longer fit for purpose, and are generally weaker than what is required for a modern data-based economy, ie the APPs are not good enough to provide the privacy protections that consumers require.[9]

Implementing the CDR alongside the APPs therefore implements multiple privacy standards. This will be confusing for consumers and industry alike. It also leaves consumers vulnerable to lower protections in different situations given the inevitability if non-accredited parties accessing consumers' CDR data.

The CDR facilitates leaking of sensitive financial data to entities that provide lower privacy protections

One of the key aims of the CDR is to create a safe and secure environment in which consumers will be able to trust and have confidence that they will be able to transfer or port their data from one data holder or participant to another.

However the CDR legislation has the potential to facilitate non-accredited parties obtaining CDR information, leaving these consumers, who were led into a system on the promise of higher privacy protections, vulnerable to the lower privacy standards of the APPs.

We note that the concerns of consumer representatives with respect to these leaks outside of the system have been somewhat ameliorated temporarily under the first iteration of the ACCC rules.[10] However there is no guarantee moving into the future that this will remain the case. Indeed it is highly likely that they will at some point available to non-accredited parties in future iterations of the ACCC CDR Rules. Nor is it strictly able to be curtailed under the first iteration of the rules because non-accredited parties will gain access to CDR data through

[8] ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million

[9] Pages 54-56, Recommendation 4.2 – modifications to privacy protections.

[10] Rule 8.8, ACCC CDR Rules Outline, December 2018, "*The ACCC does not propose to include sharing of CDR data with a non-accredited entity in version one of the Rules. This is in light of concerns from stakeholders that transfer of CDR data to a non-accredited entity risks undermining the consumer protection that the accreditation process is designed to provide. The ability for consumers to direct the sharing of CDR data to certain non-accredited entities (including professional advisors such as accountants and lawyers) will be considered for inclusion in the next version of the Rules.*"

other means such as screen-scraping, or simply demanding the provision of the data in exchange for a service.

This is a fundamental flaw to the legislation and needs to be reconsidered.

The CDR establishes flawed and incomplete privacy safeguards

Even when a consumer is subject to the CDR privacy safeguards which match to the APPs, the stronger safeguards are limited and incomplete. They:

- do not provide a legislated right to deletion or erasure;
- do not embed privacy by design;
- do not provide a legislated right to restrict purposes;
- do not provide a legislated right to object to processing; and
- do not provide a legislated right to not be evaluated on the basis of automated processing.

Again we acknowledge that the ACCC Rules have taken some steps to ameliorate these concerns under the first iteration of the CDR rules. However these are not permanent and do not apply to consumer's financial data held by data holder. These should be legislated rights.

The CDR institutes two very different FinTech sectors

In addition to the multiple privacy standards, the CDR embeds two very different FinTech sectors by not banning screen scraping and other unsafe technologies. Screen-scraping involves a consumer providing their log-in credentials to a third party who use them to access the data held by another party via a customer-facing website. Consumer data is then collected from the website. These unsafe data access technologies have been banned in other countries. Providing access to one's data using 'screen scraping' technology can amount to a breach of the terms and conditions of a customer's bank account, and can put customers at risk of losing their protections under the E-Payments Code[11] This will impact harshly upon financially vulnerable consumers. Without a ban on these technologies, there is very little incentive for businesses such as pay day lenders and debt management firms to become accredited. The higher regulatory hurdles will in fact be a disincentive to these businesses from joining. Financially vulnerable people, for example, will continue to be desperate to access credit and will not concern themselves with the nuances of privacy protections to so. If that means engaging with non-CDR accredited entities like pay day loan operators, those financially vulnerable people will end up with lower privacy protections than their middle-class counterparts.

[11] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

The CDR Privacy Impact Assessment process was flawed and failed to address a number of concerns.

Treasury decided not to outsource the development of its Privacy Impact Assessment to external consultants. While we acknowledge there is no strict requirement for Treasury to have undertaken an independent assessment, we believe that the approach taken to undertake the PIA is flawed, conflicted in nature and not in keeping with the recommendations of the OAIC in its Privacy Impact Assessment guidelines. Because of this Treasury has failed to address a number of core consumer concerns.

Key Recommendations

Given the above, Financial Rights recommends a complete re-think in the approach the Government has taken with respect to the implementation of the CDR:

1. The CDR legislation should not be finalised nor implemented until the *Privacy Act* and the Australian Privacy Principles are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.
2. If the approach to developing a CDR is to proceed then a number of significant changes to the legislation are required, as detailed in this submission.
3. The CDR legislation needs to be re-named to the Consumer Data Portability/Transfer Right to reflect the intent of its operation.
4. As recommended by the Open Banking Review, the CDR legislation should be a closed system to prevent any CDR data being provided to non-accredited entities. All handlers of CDR data from banks and credit unions (data holders), FinTechs and software developers (data participants) to accountants, financial advisors, mortgage brokers, insurance brokers, landlords or any other entity with even a remote interest in gaining access to sensitive, personal financial data should be accredited. This accreditation should be appropriately scalable.
5. The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies as has occurred in the UK and elsewhere.
6. The CDR must implement stronger privacy safeguards to those currently proposed and introduce further safeguards and security measures currently not conceived of under the APPs but which are necessary for a modern, forward looking, consumer data transfer regime that will build genuine consumer trust and confidence.
7. The government should establish a coordinated approach to privacy reform incorporating consideration of all of the proposed reforms under the CDR, the ACCC Digital Platforms Inquiry, the Data Sharing and Release Reforms and the Human Rights Commission's Technology and Human Rights project.
8. A genuinely independent privacy impact assessment should be carried out and its recommendations implemented.

Treasury Laws Amendment (Consumer Data Right) Bill 2018

This section of our submission expresses our concerns with respect to the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* currently under consideration.

Designating sectors for increased privacy protections

By design, the draft CDR legislation will apply to different sectors of the economy that have been designated by the Minister.

Under the CDR regime, individuals and businesses can directly access or direct that their data be shared with certain CDR participants and seemingly non participants under certain circumstances.

The development of this legislation and the CDR model more broadly emerges from the government's response to both the *Productivity Commission's Inquiry into Data Availability and Use Report* and the *Review into Open Banking in Australia 2017* which recommended that Open Banking be implemented through a broader CDR framework.

While this approach may be appropriate to developing consistent application programming interfaces (**APIs**) and data standards for vastly different sectors of the economy and their unique data sets (banking and financial information versus energy, telecommunications, social media, insurance and other sectors yet to be identified), it fails to address standard privacy and security expectations that apply equally across the economy across all sectors.

Financial Rights notes that there are currently a number of concurrent processes taking place in developing various new legal frameworks for the handling and use of consumer data. These are:

- the Consumer Data Rights legislation (currently being considered by this committee);[12]
- the Data Sharing and Release Reforms[13]
- the ACCC Digital Platforms Inquiry[14], and
- the Human Rights Commission's Technology and Human Rights process[15]

[12] The CDR is being established to allow consumers to ask for data to be safely shared with trusted recipients in specific sectors such as banking, energy and telecommunication services, and eventually for other services across the economy.

[13] The Data Sharing and Release Reforms ostensibly seek to promote better sharing of public sector data, build trust in use of public data, maintain the integrity of the data system, and establish institutional arrangements. https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms

[14] The Digital Platforms Inquiry is examining digital search engines, social media platforms and digital content aggregators.

[15] The Human Rights Commission is undertaking a significant project exploring the rapid rise of new technology and what it means for our human rights. The project aims to identify the practical issues at

Despite all the current policy developments and inquiries dealing with slightly different issues there is significant crossover in their impact upon consumers, their data and privacy (and other consumer) protections. For example, the ACCC Digital Platforms Preliminary Report identifies major flaws in the regulatory framework over the collection, use and disclosure of user data and personal information. Many of these flaws have similarly been identified by the Open Banking Report[16] and sought to be addressed under the CDR regime but not the wider economy. The ACCC Preliminary Report also makes a number of recommendations in ensuring that consumers are better protected. Most of these recommendations align with consumer representative recommendations with respect to data collection and use practices in the financial services and FinTech sectors that will be subject to the CDR and Open Banking.

By taking a limited approach, the CDR regime creates a new set of strengthened privacy safeguards that will only apply to certain designated sets of financial data in certain limited circumstances. In reality, these strengthened privacy safeguards are required in all situations where consumer data is handled.

Over time it is expected that the CDR will expand to cover certain other sectors in further limited circumstances. This approach in providing privacy safeguards for sensitive data use is therefore by its nature, limited and piecemeal.

The approach also stands in stark contrast with the EU who has established a list of 20 Data Protection Rights that applies to all individuals and businesses across the entire economy including the Right to Access, Right to Deletion, Right to Rectification, etc. The EU has established this baseline set of safeguards and is also systematically developing rules and data standards for every sector to more appropriately implement consumer facing data products and services such as open banking.

The draft CDR legislation however only implements one of the rights that the EU has implemented - the right to portability. In this sense then the CDR is a misnomer as it is merely a Consumer Data Portability/Transfer Right.

While this is implicitly acknowledged in the *Exposure Draft Explanatory Materials*[17] the Government is selling the CDR in such a way that suggests that the CDR is a broader right*:*

> *This Bill is a game changer for Australians. The Consumer Data Right will empower customers to use their data for their own benefit. … Customers will determine which data is shared, on what terms and with whom. The Consumer Data Right is a right for customers and not for those who wish to access or use a customer's data. …The Government is committed to ensuring that high levels of privacy protection and information security for customer data is*

---

stake; undertake research and public consultation on how best to respond to the human rights challenges and opportunities presented by new technology, and finally develop a practical and innovative roadmap for reform

[16] https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

[17] Para 1.1 "*The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties.*"

> *embedded in the new regulatory framework. This Bill delivers enhanced protections, backed by well-resourced regulators with strong powers.* [18]

Counter to the sales pitch, the CDR is merely a collection of rights with respect to porting or transferring consumer data in certain designated sectors. It provides no further rights to more broadly access consumer data, restrict processing, object, delete, correct, or rectify your data. The CDR is therefore misleading as consumers are being sold the idea of a "consumer data right" to protect consumers in their access to and use of their own financial data.

All that is being created is a set of standards to be applied to the portability of consumer data with some strengthened privacy safeguards in specific designated sectors.

A third set of privacy safeguards

While these strengthened privacy safeguards in Open Banking are welcome, the CDR is in essence establishing a third set of privacy standards for specific designated sectors that applies to consumers seeking protection, security and redress when something goes wrong with their data.

The CDR Data Privacy Safeguards as envisioned under this draft legislation for specific designated sectors will be an addition to the current *Privacy Act* safeguards as detailed under the APPs.

The APPs are also in addition to general consumer protections and law that apply to those situations where holders of consumer data are *not* "APP entities" as defined under the APPs[19].

The introduction of the CDR for designated sectors are an explicit acknowledgement that the current APPs are out of date, no longer fit for purpose, and are generally weaker than required for a modern data based economy, ie the APPs are not good enough to provide the privacy protections that consumers require.[20] The CDR Legislation institutes a number of modified privacy safeguards to boost the protections under the APPs. Currently the APPs:

- do not require informed and express consent: APP3;
- merely require reasonable steps be taken to notify consumers rather than having to notify: APP 5; and
- do not require express and informed consent for direct marketing: APP 7.

Implementing the CDR alongside the APPs therefore implements multiple privacy standards. This will be confusing for consumers and industry alike. This is especially the case given the fact that as envisioned under the Bill, sensitive personal financial data will be subject to these different standards in different circumstances and different stages of the data lifecycle: this is explained further below regarding financial data under the non-accredited data recipients section.

---

[18] The Hon. Scott Morrison, Treasurer, Media Release *More power in the hands of consumers,* 21 September 2018, http://sjm.ministers.treasury.gov.au/media-release/087-2018/

[19] ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million

[20] Pages 54-56, Recommendation 4.2 – modifications to privacy protections.

Financial Rights therefore believes that while designating sectors to establish and introduce data standards for the purposes of portability is sensible, the limited approach being taken by the Treasury to designate sectors for increased privacy protections needs to be reconsidered.

The CDR legislation should not be finalised nor implemented until the *Privacy Act* and the APPs are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.

In addition to the problems identified by the Open Banking review which demonstrate how the APPs are inappropriate for a modern, data based economy, there are other issues with the APPs. The last time privacy laws in Australia were comprehensively reviewed was ten years ago.[21] The way Australian consumers and businesses use and supply data has changed dramatically since then. Australians' expectations for privacy have also increased markedly, in line with increased awareness of the importance of personal data and increased breaches in their personal data. The ACCC Digital Platforms Preliminary Report has also identified serious issues with respect to consumer's privacy and recommends a serious upgrading of privacy protections for all consumers across the economy.[22] Add to this, significant international developments in privacy protections and the APPs stand as a relic of a former time and are in no way fit to address community expectations with respect to the use, security and protection of their data.

If the Government insists on proceeding with the current draft CDR legislation and approach then a number of significant changes to the current draft need to be implemented.

The CDR legislation needs to be re-named to the Consumer Data Portability/Transfer Right to reflect the intent and reality of its operation. Without this change consumers will continue to be misled about the scope and reach of the CDR and may fall into a false sense of security.

As clearly recommended by the Open Banking Review, the CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity. All handlers of CDR data from banks and credit unions (data holders), FinTechs and software developers (data participants) to accountants, financial advisors, mortgage brokers, insurance brokers, landlords or any other entity with even a remote interest in gaining access to sensitive, personal financial data should be accredited. This accreditation can be appropriate to their use and be implemented on a sliding scale if need be. See further information on this under the Participants in the CDR System, below.

[21] ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 , 12 August 2008. Available at: https://www.alrc.gov.au/publications/report-108

[22] These recommendations include: Strengthen notification requirements; Introduce an independent third-party certification scheme; Enable the erasure of personal information; Increase the penalties for breach; Introduce direct rights of action for individuals; Expand resourcing for the OAIC to support further enforcement activities; introduce a statutory cause of action for serious invasions of privacy.

Recommendations

1. **The CDR legislation should not be finalised nor implemented until the *Privacy Act* and the Australian Privacy Principles are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.**

2. **If the Government insists on proceeding with the current draft CDR legislation and approach then a number of significant changes need to be implemented:**

   a) **The CDR legislation needs to be re-named to the Consumer Data Portability/Transfer Right to reflect the actuality and intent of its operation.**

   b) **The CDR legislation should be a closed system to prevent any CDR data being provided to any non-accredited entity.**

   c) **All handlers of CDR data should be accredited. This accreditation should be appropriate to their use and be implemented on a sliding scale if need be.**

Participants in the Consumer Data Right System

Non-accredited data recipients

The EM states that there will be circumstances where non-accredited entities will be able to access CDR data:

> *1.29 The Bill establishes a framework to enable the CDR to be applied to various sectors of the economy over time. The framework relies on four key participants – consumers, data holders, accredited persons and accredited data recipients, and designated gateways. However, the system is flexible and may also provide via the consumer data rules, for interactions between consumers and non-accredited entities.*

This is a fundamental flaw to the CDR regime and should be reconsidered.

We note that the first iteration of the ACCC rules prevent the sharing of CDR data with a non-accredited entity in Version 1 of the Rules.[23] While non-accredited parties currently will not have access to CDR data for at least the initial period it is highly likely that they will at some point be able to access CDR data, be it through future iterations of the ACCC CDR Rules, some form of regulatory arbitrage or it may simply be accessed by non-accredited parties through other means such as screen-scraping.

[23] Rule 8.8, ACCC CDR Rules Outline, December 2018,

Access by non-accredited parties is *not* what was recommended under the Open Banking Report. The Open Banking Report explicitly recommends:

> *Recommendation 2.7 accreditation*
>
> *Only accredited parties should be able to receive Open Banking data. The ACCC should determine the criteria for, and method of, accreditation.*

The reason? The Open Banking Report states that:

> *For customers to have confidence in Open Banking they will need assurance that other participants — data holders and recipients — are accredited entities that will adhere to appropriate security and privacy standards and have the capacity to provide financial compensation if things go wrong and they are found liable.*
>
> *…Other participating entities should be required to establish that they can safely deal with their obligations in relation to data (which may not necessarily be as stringent as the prudential obligations for banks). The standard that non-ADIs may be required to meet should be based on the potential harm to customers, and risk to the Open Banking system, that the relevant data set and that participant pose.* [24]

Consumer confidence in Open Banking and the CDR is crucial if it has any chance of succeeding.

The decision to create legislation that has the potential to allow non-accredited entities to access sensitive CDR data is incredibly dangerous. It is dangerous because consumers are being led to assume their data will be protected under a "Consumer Data Right" but in fact it has the potential to facilitate the movement of this data outside of a strengthened privacy framework to one with lower privacy protections.

As mentioned above, the introduction of the CDR regime will create multiple levels of privacy standards that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

- CDR Privacy Safeguards as envisioned under this draft legislation – essentially strengthened versions of the APPs;
- the *Privacy Act* safeguards as detailed under the APPs; and
- general consumer protections and law applying to those holders of consumer data that are *not* "APP entities" as defined under the APPs, ie all private sector and not-for-profit organisations with an annual turnover of less than $3 million.

To demonstrate the complexity being proposed by the draft CDR legislation, a consumer could potentially be subject to the following array of high and low protections:

1. Transactional data held by a bank that may at some point in the future be CDR data (a data holder) but has yet to be requested to be ported, is currently and will continue to be subject to the APPs only.

[24] Pages 44-5, Open Banking Report https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

2. This transaction data becomes "CDR data" once requested to be transferred to an accredited Data Participant where its transfer and use will be subject to the CDR Privacy Safeguards.
3. The transactional data continuing to be held by the original bank remains subject to the APPs.
4. CDR data collected and held by an accredited Data Participant will be subject to the CDR Privacy Safeguards.
5. Non-CDR Data held by Accredited CDR Participant small businesses will be subject to the APPs.
6. CDR data accessed and held by non-accredited parties who are "APP entities"[25] will be subject to the APPs, not the CDR privacy safeguards.
7. CDR data accessed and held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

The introduction of the concept of providing non-accredited CDR participants the ability to access CDR against the recommendation of the Open Banking Report provides a significant leakage point for CDR data to fall outside of the system, whereby consumers will, at a minimum, be provided fewer or lower standard protections or in some cases, no realistic privacy protections at all if or when a breach or problem arises out of the use or misuse of this CDR data.

In fact, the draft CDR legislation is designed to encourage consumers to engage with the CDR regime with the promise of increased protections, all the while allowing this data to leak out of the CDR regime where lower or no privacy standards at all apply. In other words, the draft CDR legislation has the potential to facilitate incredibly sensitive financial and personal data to be handled by non-accredited parties with lower or no protections for consumers.

This is unacceptable.

There are likely to be a significant number of parties who will seek access to CDR data as a non-accredited entity. These include:

- accountants
- financial advisors
- insurance brokers
- mortgage brokers
- debt management firms
- debt collectors

[25] Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses

- pay day loan and consumer lease operators
- real estate agents
- landlords
- book-up providers

Generally speaking any sole trader or small businesses who provides "middleman" or advice services are likely to seek to gain access to CDR data and will not be in a position (financially or otherwise) to become an accredited party as foreseen under the draft legislation and EM. Nor will they be incentivised to be an accredited member.

Non-accreditation and consent of a consumer

Even if a consumer consents to a transfer out of the CDR regime to a non-accredited entity by, for example downloading their own data and handing it to a third party, this could result in significant problems.

Firstly, it is unclear how a consumer will be expected to understand what privacy protections will be available to them even if they were told that they are being subjected to CDR privacy safeguards, the *Privacy Act*, the APPs or none of the above. Even if the consumer was told explicitly what the arrangement was, how is the consumer expected to know that the *Privacy Act* and APPs are weaker forms of protection to the CDR privacy safeguards, and not very effective privacy protections. Will these higher, lower and lowest forms of protection be made explicit to consumers?

Second, what will prevent a consumer from signing up for a service that will include data handled by a non-accredited party, where there is a willingness on the consumer's part to sign up to just about anything, even with lower privacy standards. Financially vulnerable consumers will sign up to any service if they are desperate enough, or perceive no real choice. And Financial Rights knows from its work on the National Debt Helpline that many Australian consumers are vulnerable to the promises of debt management firms, quick-cash payday lenders, and online companies that promise to solve all of their financial problems for a fee or in exchange for their personal information.

Think about consumers applying for a financial check to obtain a rental property, struggling consumers who want to sign up with a debt consolidation service or pay day loan operator, or rural and regional Australians using the only store in town handing their details over.

The result is that the people who are most in need of protection – the financially vulnerable - will inevitably be provided the fewest protections under the CDR legislation.

This is particularly the case with respect to pay day lenders.

The CDR legislation does not ban screen scraping and other technologies. These incredibly unsafe data access technologies have been banned in other countries. Without a ban on these technologies, there is very little incentive for businesses such as pay day lenders and debt management firms to become accredited. The higher regulatory hurdles will be a disincentive to these businesses from joining. Financially vulnerable people will of course continue to be desperate to access credit and will not concern themselves with the nuances of privacy

protections to so. If that means engaging with non-CDR accredited entities like pay day loan operators, financially vulnerable people will do just that.

Even non-financially vulnerable consumers may hold misplaced trust in a financial advisor or accountant that they know. Indeed there is significant research that trust increases when a financial advisor provides information on conflicts of interest because the consumer believes they are being transparent and is therefore more deserving of trust.[26] The same principle could very well apply with respect to greater disclosure and transparency with respect to the application or lack thereof of privacy safeguards. If the scandals in financial advice, mortgage and insurance broking that led to the current Royal Commission are anything to go by, this will continue to the be the case.

It has been put to Financial Rights in CDR consultations that consumers won't need to know which set of privacy standards they will be subject to since there will be an "any door approach" to EDR and complaints handling and the appropriate EDR will figure it out. This dismisses the fact that people will be afforded fewer safeguards depending on where they happen to fall in the process.

As we read the legislation, there is nothing preventing the ACCC from developing rules of accreditation for all potential small businesses and sole traders who are currently conceived to possibly gain access to CDR data as a "non-accredited entity". In other words, the ACCC could very well introduce accredited rules and standards not simply to FinTechs to be accredited, but for all accountants, financial advisors, and mortgage brokers on a sliding scale, to ensure that consumers are protected under the CDR privacy safeguards. We do not believe that this would onerous. Accessing huge amounts of personal financial information is not a right and should be a privilege one that comes with obligations to protect the privacy of individuals and meet expected security standards. Providing people with access to huge amounts of private financial information under the CDR is *not* business as usual.

If the Government proceeds with the legislation in its current form then the accreditation for these data recipients should be mandated.

There is also nothing preventing the legislation from being re-drafted to ensure that all CDR data, wherever and whoever it is held by, will be subject to CDR privacy safeguards. This was, in our view, the original intent of the Open Banking Report.

The reason, for example, why the UK does not have to worry about leakages outside of their own Open Banking regime is because the GPDR rules are in place for all citizens and their data across the economy. These general protections do not exist in Australia.

The simplest solution, as recommended above, would be to delay the introduction of the CDR regime until the *Privacy Act* and the APPs are modernised to meet community standards and

[26] James Lacko and Janis Pappalardo, *The effect of mortgage broker compensation disclosures on consumers and competition: A controlled experiment*, *Federal Trade Commission Bureau of Economics Staff Report*, 2008 referenced in Financial Services Authority, Financial Capability: A Behavioural Economics Perspective, 2008*: "Even if the disclosure is noticed by consumers, it may have the effect of increasing trust in advisers rather than making consumers more wary."*

requirements arising from technological development. In this way consumers will be protected by the general law if their consumer data right data falls out of the CDR system.

In the absence of any such review Financial Rights recommends that the CDR legislation should be legislated to be a closed system to prevent any CDR data being provided to any non-accredited entity. All handlers of CDR data from banks and credit unions (data holders), FinTechs and software developers (data participants) to accountants, financial advisors, mortgage brokers, insurance brokers, landlords or any other entity with even a remote interest in gaining access to sensitive, personal financial data should be accredited. This accreditation can be appropriate to their use and be implemented on a sliding scale if need be.

The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies as has occurred in the UK and elsewhere.

Accreditation process

Financial Rights supports the establishment and implementation of a strong accreditation process and accreditation criteria to ensure consumer protections are built into the system from the start.

Accreditation is crucial to the success of the CDR. As the Open Banking Report stated:

> *Accreditation would allow customers to determine with greater ease which data recipients meet the Standards and may, as a result, be considered trustworthy. An accreditation process should inspire confidence amongst customers to share their data with recipients that the customer has chosen to trust. An accreditation process would also provide some level of customer protection from malicious third parties.*[27]

Without accreditation, trust and confidence falls away.

Financial Rights has stated emphatically that all entities seeking to use or hold CDR data must be accredited – with no exceptions.

This means that accreditation needs to be implemented for those potential financial services users who are currently conceived under the legislation to be "non-accredited," but in our strong view should be accredited. At a minimum these entities – including accountants, financial advisors, mortgage brokers, etc should afford consumers CDR privacy safeguards and protections and adhere to most if not all of the accreditation criteria in the Rules.

Financial Rights recommends a tiered model for accrediting entities based on differing levels of risk and potential harm and we would support a system that varies the obligations as to a FinTech company, a neo-bank or a financial advisor or accountant.

But it is critical that *all* of these entities (companies and individuals) handling CDR data must be accredited.

[27] Page 22, Open Banking Report https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

Protecting sensitive information

Financial Rights notes that actually defining high risk versus low risk for the purposes of a tiered accreditation system may be difficult.

A person's financial circumstance is highly sensitive since a breach opens them up to exploitation by unscrupulous operators, price discrimination and other risks. There are many forms of personal financial data that are highly sensitive due to the serious risks of hacking (account details, passwords), material theft, and identity theft (credit card numbers, ccv numbers).

Currently "sensitive information" is defined under the *Privacy Act* to mean information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record;
- health information; or
- genetic information.

Sensitive information in this context is information that could be used as the basis of unjustified discrimination. This is appropriate.

It is our view that there is a likelihood that CDR data can and likely will be used to discriminate. Sensitive financial information can and will be used to both:

- discriminate via the use of black box algorithmic biases that contain 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
- price and risk discrimination where Australia's most vulnerable, disadvantaged and financially stressed households are identified and for example unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders.

Sensitivity is therefore contextual. Certain information in the hands of one party may be mundane and uncontroversial but highly sensitive and consequential in others. The current definition of sensitive information in the *Privacy Act* does not include financial information, which is surprising and disappointing given the new ways discrimination may arise through the misuse of data analysis and black box algorithms.

It is our view that their needs to be a full reconsideration of the concept of sensitivity under the *Privacy Act* to ensure that financial data is also considered sensitive, both because of the chance of discrimination and because if the data were to be breached, and not handled with appropriately high standards, it will lead to serious financial consequences.

Given the move to an economy based on the use of personal data in almost every aspect of life, there needs to be greater protections under the *Privacy Act* and that involves consideration of further shades of sensitivity to cover the multiplicity of problems that can arise that are incongruent with the current binary approach.

In the meantime, the current CDR legislation and CDR rules should include accreditation criteria that bans, and regulates, any price discrimination, algorithmic discrimination and black box algorithms inaccessible to regulators.

Problematic business models

One key concern of Financial Rights is the business model of FinTechs particularly "Freemium" models that in part will make money from advertising or the sale of data and information to "fourth parties"[28] in Australia or overseas.

Any business model dependent upon the on-sale of personal data to fourth party entities (be they CDR accredited or non CDR accredited) is one that has the potential to sell this data to any and all entities including unscrupulous or disreputable international or Australian parties who have a history of misuse of data through spamming, hacking or other activities that don't comply with the law or meet community expectations.

We note that the first iteration of the ACCC CDR Rules prevents the on-sale of data. This is a positive step however this practice needs to be banned outright under the legislation.

Screen-scraping, the CDR regime and accreditation

Establishing an accreditation process without banning other unsafe forms of accessing personal financial transactions such as screen-scraping creates a multitude of issues.

By not banning screen scraping and other unsafe access technologies – as has occurred in other jurisdictions including the UK - two very distinct FinTech sectors will be created: a sector that will adhere to higher privacy safeguards and standards and a sector that will not. It is unclear what the incentives are to seek accreditation under the CDR for, say, a screen-scraping pay day lender. While there are many pay day lenders or debt management firms, for example, who may seek reputational legitimacy, many others do not. The additional hurdles, regulations, obligations introduced by an accreditation process will remain unattractive to many of these businesses, some of whom already skirt the regulations in place. With a steady stream of desperate and vulnerable clientele willing to do anything for a speedy solution or fast cash, there is no financial, reputational or other incentive for them to seek accreditation,

[28] If the consumer is the first party, the bank data-holder is the second party, the data recipient is the third party, then we refer to other parties to which data is on-sold or provided to by the third party data holder as "fourth parties". This is an important distinction to make when considering the downstream uses and potential abuses of data and data breaches.

Financially vulnerable people *will* continue to be desperate to access credit and will not concern themselves with the nuances of privacy protections to so. If that means engaging with non-CDR accredited entities like pay day loan operators they will. The result will be financially vulnerable people will ending up with lower privacy protections than their middle-class counterparts. Screen-scraping can amount to a breach of the terms and conditions of a customer's bank account, and can put customers at risk of losing their protections under the E-Payments Code.[29]

Recommendations

3. **Accreditation criteria should ban and/or regulate any price discrimination, algorithmic discrimination and black box algorithms inaccessible to regulators.**
4. **The on-sale of CDR data needs to be banned.**
5. **The concept of sensitive information, as defined under the *Privacy Act 1988* needs to be re-considered to ensure that financial information is appropriately protected.**
6. **The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies.**

Consumer Data Rules

Disclosure, use, accuracy, storage, security or deletion of CDR data

Consent

The EM states:

> *1.71 Consumer data rules will be set out for CDR consumers, data holders, accredited data recipients and designated gateways the matters that have to be satisfied in order to demonstrate that consent was obtained and the CDR consumer understood what it was they were consenting to. The rules will prescribe the process for obtaining consent and how to ensure that consent it genuine. However, it is not intended to make this element of the CDR system so complex as to discourage participation. The role of the consumer data rules is to balance the sensitivity of the CDR data with the need for security, efficiency and convenience.*

Genuine consent is not simply an important feature of the CDR it is the entire lynchpin upon which the CDR succeeds or fails. Genuine consent should, and inevitably will be, the central

[29] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

feature for all data arrangements and privacy standards across the economy moving into future – not simply for designated sectors.

The ACCC have established the following requirement for consent in its first iteration CDR rules:

> a. Consent must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.
>
> > *Consent must be voluntary and consistent with the OAIC's Australian Privacy Principles guidelines on voluntary consent. Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where duress, coercion or pressure is applied by any party involved in the transaction. Factors relevant to deciding whether consent is voluntary include:*
> >
> > - *the alternatives open to the individual if they choose not to consent*
> > - *the seriousness of any consequences to the individual if they choose not to consent*
> > - *any adverse consequences for family members or associates of the individual if the individual chooses not to consent.*
>
> b. An accredited data recipient must not make consent a precondition to obtaining another unrelated product or service. The collection of CDR data must be reasonably necessary or required to provide the service the accredited data recipient is offering.
>
> c. An accredited data recipient must not bundle consent with other directions, permissions, consents or agreements.
>
> d. An accredited data recipient must present each consumer with an active choice to give consent, and consent must not be the result of default settings, pre-selected options, inactivity or silence.

Financial Rights generally supports these requirements but makes the following observations and recommendations.

it is important to ensure that the lack of consent for a particular use should not limit the ability to receive a service unless the data is fundamentally necessary for a particular product or service to work.

The EU guidance on consent[30] acknowledges that there are a number of situations where genuine consent cannot be freely given – for example in situations where there is a significant imbalance of power. This needs to be incorporated into any notion of voluntariness. To this end consent must be freely given, absent of any element of inappropriate pressure or influence upon the consumer preventing them from exercising their free will including:

- any imbalance of power;

30

- the presence of any conditions via for example, the bundling of consent of necessary and unnecessary uses;
- the conflation of several purposes without consent for each specific use; and/or
- detriment to the consumer if consent is withdrawn or refused;

Some of these elements have been taken up by the ACCC – other have not.

Consent should also be able to be constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data. Entities must be obliged to only collect the minimum amount of personal information that the business actually needs. This means not collecting extra information simply for marketing purposes at some later date for example.

Finally APP entities must explain in simple, clear, terms *why* information is being collected and for what it is being used.

The key point here is that while outlining consent in the way the ACCC does under the rules is a positive step, the conception of consent and data use need to be embedded under the *Privacy Act* and APPs for all consumers in all situations.

Financial Rights supports amending the *Privacy Act* to define 'consent' to include only *express* consent and that the current non-binding elements of the OAIC's guidance regarding consent be binding requirements under the APPs, to ensure that:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

The *Privacy Act* was drafted during a period where the use of digital terms and conditions that are bundled and lengthy were relatively new. Their use has led to a significant asymmetry of information and power, working against the interests of consumers. They are unfair and have led to lower levels of product, service and data literacy.

The APPs (including APP3, 7 and 8) must be modernised and future-proofed with clear requirements on all companies (not just digital platforms and financial services) to gain express, fully informed consent from a consumer.

Recommendations

7. Genuine consent must be defined under the *Privacy Act* and APPs as:

a) freely given, absent of any element of inappropriate pressure or influence upon the consumer preventing them from exercising their free will including:

i. any imbalance of power;

ii. the presence of any conditions via for example, the bundling of consent of necessary and unnecessary uses;

iii. the conflation of several purposes without consent for each specific use; and/or

iv. detriment to the consumer if consent is withdrawn or refused;

b) specific including clear separation of information related to the obtain of consent for different data processing activities;

c) able to be constrained according to the customer's instructions including easily withdrawn with immediate effect and deletion of data;

d) fully informed, transparent and fair,

e) time limited, and

f) an unambiguous indication of wishes via an affirmative act from the consumer.

Deletion

Financial Rights notes that the consumer data rules, accreditation and data standards may develop rules on the deletion of CDR data: subsections 56BB, 56BC, 56BD, 56BE, 56BF.

The ACCC CDR rules have introduced the concept of redundant data and assert that redundant data must be deleted.

> *8.15 If CDR data becomes redundant data (as specified in that clause)2, an accredited data recipient must ensure that the redundant CDR data is either destroyed or de-identified and apply the OAIC and Data61's 'De-identification Decision-making Framework' in determining which treatment is appropriate in the circumstances.*

Further:

> *7.15 Withdrawal of consent by a consumer to collect and use data will have the consequence that the CDR data becomes redundant data for the purposes of Privacy Safeguard 12*

These rules however can be changed in the future, depending on pressure from business interests. This pressure is inevitable in a regime where data is more valuable.

The EU's GDPR Article 17 provides for the "Right to Erasure" where an individual will hold the right to request the erasure, *without undue delay*, of any links to, copy or replication of the data in question, under the circumstances 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. This needs to be a legislated right – not one that can be taken away.

Consumers do not want the situation where their data has been used by a company – with or without consent – and that company holds on to that data to use for secondary purposes, either in aggregated or de-identified form where there is any possibility of re-identification.

This expectation is also increasing as consumers become more and more aware of and literate regarding the extent their own personal data is being used and misused by companies.

The recent news that UK company Cambridge Analytica legitimately gathered some personal data from Facebook accounts and concurrently illegitimately gathered other people's data, and then, when found out and were requested to delete the data, did not, has raised public consciousness over the potential for data to be misused. Combined with the never-ending list of significant and high-profile data breaches at Equifax, Ashley Madison, Yahoo, Red Cross to name a few and the privacy concerns raised in the context of the recent census and MyHealth Data controversies, the desire on the part of consumers to control their data via strengthened regulations is becoming stronger and stronger every day.

The Government will be opening consumers up to serious consequences if the right to delete is not embedded in the legislation. It risks undermining trust and confidence in a system it is promoting as the future. If a right to erasure is not included future headlines will likely include the names of accredited and non-accredited CDR entities rather than Facebook and Cambridge Analytica.

Financial Rights strongly recommends that in line with its recommendation that the APPs be reviewed with stronger privacy protections created, that as a part of this review that a right to deletion/right to erasure be introduced into the privacy laws. This would include a thorough re-think of APP 11 with the removal of the "reasonable steps" test removed as a minimum.

Further Financial Rights recommends that a right to deletion be embedded or hardcoded in to the CDR legislation, not as a part of the set of rules but as a fundamental Privacy Safeguard, built into the legislation not the CDR rules developed by the ACCC. We believe that the EU GPDR standard sets a solid benchmark from which to implement such a safeguard.

Recommendation

8. **If the CDR regime is to be implemented without a general right to deletion existing under the *Privacy Act* or APPs, a privacy safeguard should be implemented to establish such a right.**

CDR Privacy Framework

Privacy Safeguard 1 – open and transparent management of CDR data

Privacy Safeguard 1 is essentially the requirement to have a privacy policy (similar to APP 1). There is really is no significant difference that bolsters the APP 1 requirement.

We believe that this needs to be strengthened to include the following information in a CDR data management policy:

- ***confirmation of where the CDR participant is processing their personal data.*** This means explicitly stating where a consumer's CDR will be *held* – not just in the case where the information is disclosed to a overseas accredited or non accredited entity under section 56ED(5)(f). Information held in certain countries, such as the US will automatically allow another countries access to that data. It is important that information about international storage is provided explicitly to a consumer in order to choose whether they wish to have that information stored overseas.
- ***the categories of recipients with whom the data may be shared.***
- ***the period for which the data will be stored (or the criteria used to determine that period).*** Given it is foreseen that there will be rules including time limits - it is essential that this be embedded in the privacy safeguards
- ***information about the existence of the rights to correction and other privacy rights including a right to deletion, a rights to restrict of processing and to object to processing as proposed by Financial Rights.*** It is critical that for the sake of transparency that consumers are provided with transparent information on their rights in the privacy policy.
- ***information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the consumer.*** This is critical for

consumers to know how their data will be treated in an era of algorithmic bias and potential discrimination.

Recommendations

9. **Privacy Safeguard 1 should be strengthened to include:**
   a) **confirmation of where the CDR participant is processing their personal data.**
   b) **the categories of recipients with whom the data may be shared.**
   c) **the period for which the data will be stored (or the criteria used to determine that period)**
   d) **information about the existence of the rights to correction and other privacy rights including a right to deletion, a rights to restrict of processing and to object to processing as proposed by Financial Rights.**
   e) **information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the consumer.**

Privacy Safeguard 7 – Use or disclosure of CDR data for direct marketing by accredited data recipients

Financial Rights believes that significant restraints must be placed upon CDR data holders, accredited CDR participants and accredited CDR participants on the disclosure or use of CDR data for direct marketing purposes. This has been accepted by the ACCC in its rules

> *Privacy safeguard 7: use or disclosure of CDR data for direct marketing*
>
> *An accredited data recipient will be prohibited from using CDR data for the direct marketing of products or services unrelated to the product or service a consumer has consented to the collection and use of their CDR data for.*
>
> *This prohibition is not intended to prevent an accredited data recipient from providing a service the consumer has specifically consented to receiving (for example, a comparison service that gives a consumer tailored quotes for better products or services), including an improved version of that service.*

While we strongly support this decision, the practice should be banned altogether under the legislation not the rules, since it is again highly likely that there will be pressure on the ACCC to loosen this up.

Recommendation

10. The use of CDR data for direct marketing purposes should be banned under the legislation.

Privacy Safeguard 8 – Cross border disclosure

Financial Rights believes that consent must be sought and received by a data participant before sending a customer's banking data overseas.

We believe that there should be an obligation on a CDR data participant to take steps to ensure that the overseas recipient does not breach the APPs in relation to CDR data.

Outside of leaking CDR out of the regime to non-accredited parties in Australia, sending data overseas will be the biggest and most obvious chink in the safety and security regime in handling personal data collection. If any breaches were to occur in an overseas jurisdiction it may be more difficult to access justice for somebody in Australia, particularly if that data is being on-sold to a fourth party based solely in another jurisdiction.

The refusal of consent should not be used to punish or penalize a customer, nor should it be used to refuse service to a customer. It should not be presented in such a way also that skews the consumer in favour of consenting.

Recommendation

11. CDR data participants should be obliged to take steps to ensure that overseas recipients do not breach the APPs in relation to CDR data.

12. Consent must be sought and received by a data participant before sending a customer's banking data oversea for storage, collection or use.

Correction of CDR data

Privacy Safeguard 12 – correction of CDR data

Financial Rights can attest to a general ongoing failure to amend or correct personal information in a speedy or good faith manner. Seeking amendments to credit reports, as an example, is frustrating and difficult. Seeking corrections is important as inaccurate information can lead to say, losses under the CDR regime, notices being sent to incorrect addresses and the

consequent losses that arise from that. The difficulties in seeking amendments have led to a boom in unregulated and predatory 'credit repair' businesses

This becomes even more problematic under a liability regime where a data participant will *not* be held liable for not making the changes to inaccurate, incomplete or misleading information, and merely be responsible for correcting the data (presumably in a reasonable time).

It is critical that Privacy Safeguard 12 ensure that a CDR participant must take *immediate* steps to correct information once it becomes aware (by learning itself or being told by the consumer) that personal information they hold is inaccurate, out of date incomplete, irrelevant or misleading. If they do not they should be held liable for any reliance on this information that leads to a loss.

We note too that there is the possibility for the inclusion of a statement but it remains unclear whether this is a statement from the company or the consumer? We would want the Consumer Data Rules to allow consumers to provide a statement if they do not agree with the assessment of the data participant.

Recommendations

13. **CDR participants must take immediate steps to correct information once it becomes aware (by learning itself or being told by the consumer) that personal information they hold is inaccurate, out of date incomplete, irrelevant or misleading. If they do not they should be held liable for any reliance on this information that leads to a loss.**

14. **The Consumer Data Rules should allow consumers to provide a statement if they do not agree with the assessment of the data participant.**

Further privacy safeguards

Financial Rights believes that the CDR legislation should include the following further privacy safeguards:

- ***The right to deletion/erasure/right to be forgotten***

The right to deletion should be a standalone privacy safeguard. Financial Rights goes into more detail above under the Deletion section above.

- ***Privacy by design***

Article 25 of the GDPR implements rules for data protection by design and by default.[31] Privacy by design is a proactive approach to protecting privacy during the design of a project and as well as throughout its life.

[31] Art. 25 GDPR Data protection by design and by default

Privacy by Design was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian,[32] The principles were a part of a Resolution by International Data Protection and Privacy Commissioners in 2010; followed by the U.S. Federal Trade Commission's recognition of Privacy by Design in 2012 as one of its three recommended practices for protecting online privacy; and as mentioned, incorporated into the European Commission plans to unify data protection within the European Union.

There are seven foundation principles to privacy by design are summarised by the CPRC summarises as follows:

1. ***Proactive not reactive; preventative not remedial:*** *Be proactive rather than reactive, to anticipate and prevent privacy problems in advance.*
2. ***Privacy as the Default Setting:*** *Personal data is automatically provided with the maximum degree of privacy protection in IT systems or business practices.*
3. ***Privacy Embedded into Design*** *Consider how to embed privacy in the design and architecture of IT systems and business practices rather than a treating privacy protection as a subsequent add-on feature*
4. ***Full functionality – Positive-sum, not Zero-Sum:*** *Accommodate all legitimate interests and objectives in a win-win manner, where privacy and security can both be achieved without unnecessary trade-offs.*
5. ***End-to-End Security – Full Life-cycle Projection****: Ensuring strong security measures prior to collecting the first element of information, as well as securely retaining data, and destroying data at the end of the process.*
6. ***Visibility and Transparency – Keep it Open:*** *Businesses practices and technology involved should be subject to independent verification, to assure stakeholders they are operating according to stated promises and objectives.*
7. ***Respect for User Privacy – Keep it User-Centric:*** *Take a user-centric approach by protecting the interest of individuals, for example: offering strong privacy defaults, appropriate notice, and user-friendly options.*

Embedding this approach into the CDR and any other broader re-thinking of the Privacy Act and the APPs is critical to ensure that all businesses demonstrates their respect for consumer data and personal information to provide greater security and privacy protections from day one.

- ***Right to restrict purposes***

Article 18 of the GDPR[33] gives Europeans the right to restrict the processing of their personal data in certain circumstances. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction, for example they may have an issue with the content of the information held by a company or how they

[32] Information & Privacy Commissioner of Ontario, Privacy by Design, https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

[33] Art. 18 GDPR Right to restriction of processing

have processed their data. While there may be rights conferred via the CDR rules, a right to restrict purposes should be afforded the status of key privacy safeguard.

- ***Right to object to processing***

Article 21 of GDPR[34] gives Europeans the right to object to the processing of their personal data in certain circumstances. Currently this is materialised under the CDR in part under the direct marketing Privacy Safeguards, but needs to be applied more broadly to the on-sale of data and any other purposes secondary to the primary purpose of the provision of CDR data.

- ***Right to not be evaluated on the basis of automated processing***

Article 22 of GDPR gives Europeans restricts the ability of companies to automatically profile consumers. Article 4 (4) defines profiling as:

> *Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

Obviously there are a many useful things that can take place by automating some of these processes leading to quicker and consistent decision but it may also lead to serious issues for consumers.

CDR participants should only carry out automated decision-making or profiling if it is:

- necessary for the performance of the contract for the product or service;
- authorised by law; or
- based on the consumer genuine and express consent.

CDR participants should also be required to:

- to give consumer information about the automated processing or profiling;
- take steps to prevent errors, bias and discrimination; and
- gives consumer the ability to challenge the processing.

Recommendations

15. Further privacy safeguards need to be included in the CDR regime including:

a) The right to deletion/erasure/right to be forgotten

b) Privacy by design

c) Right to restrict purposes

d) Right to object to processing

[34] Art. 21 GDPR Right to object

e) Right to not be evaluated on the basis of automated processing

Treatment of minors

We note that the ACCC had originally planned to include minors in the CDR but has:

> *changed its position on including minors in version one of the Rules given that stakeholders did not support their inclusion.*[35]

We agree with this position and believe that the application of the CDR to minors and their treatment more broadly under the privacy regime as it pertains to their data needs serious consideration and review.

Children are particularly vulnerable to the allure of new technology and new apps and may not fully understand the consequences of any consents required nor the full range of contractual obligations.

We note that the EU's GDPR restricts the ability to consent to those 16 years (or potentially 13 years and above) depending on the State. Article 8 states:

> ***Art. 8 GDPR Conditions applicable to child's consent in relation to information society services***
>
> 1. *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*
> 2. *The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*

As noted we believe that minors are particularly vulnerable to exploitation and the risks versus potential benefits are high.

For example, the Dollarmites program run by Commonwealth Bank in schools received a SHONKY Award this year from CHOICE. The Dollarmites program works by offering commissions to primary schools in exchange for running the school banking scheme. The commissions include a one-off payment of $200 when the first student makes their initial deposit as well as annual rewards of up to $600 per year.[36] Recent investigations from Fairfax

[35] Para 3.5, page 6, ACCC CDR Rules outline, Version 1., December 2018

[36] https://www.commbank.com.au/personal/kids/school-banking/information-for-schools.html?ei=bld2-btn-information-for-schools

found that Commonwealth Bank staff fraudulently activated Dollarmite accounts for personal gain.[37]

We cannot see what would stop a bank, FinTech or any other data recipient from instigating similar marketing programs directed at children.

This is particularly a concern in the FinTech sector since technologies provide the ability for individual consumers to retreat into private, hidden, digital spaces to transact with FinTech providers. For example, a person who uses a pay day loan once will be targeted for more pay day loans via the advertising on their browser as well as text, email or other forms of spam. Given the ease, speed and inherently private nature of applying for a new loan on an app, the usual social cues and hurdles that would work to potentially stop someone from accessing further predatory finance are simply no longer there. As someone falls further and further into the spiral of debt and shame, people will retreat further into the private sphere using their mobile phones away from other people (family and friends) only serving to exacerbate the problem over time.

These issues are exacerbated when we consider the use of phones by minors and a willingness to hide activities from guardians and parents.[38]

Data recipients should be required to demonstrate that they have verified someone's age and identity before acquiring consent to share CDR data. We recommend at the very least ACCC reach out to Youth Action NSW who has done advocacy on young person consent issues.

Recommendation

16. Restrictions similar to Article 8 of the EU GPDR should be implemented with consent rules specific to minors considered.

[37] https://www.smh.com.au/business/banking-and-finance/dollarmites-bites-the-scandal-behind-the-commonwealth-bank-s-junior-savings-program-20180517-p4zfyr.html

[38] Just as one example, Madhumita Murgia The secret lives of children and their phones, October 6, 2017 https://www.ft.com/content/7c972e2e-a88f-11e7-ab55-27219df83c97

The development of the Treasury Laws Amendment (Consumer Data Right) Bill 2018

Treasury's Consumer Data Right Privacy Impact Assessment

Conduct of the Privacy Impact Assessment

Treasury decided not to outsource the development of the Privacy Impact Assessment[39] to external consultants. Financial Rights is disappointed in this decision.

While we acknowledge there is no strict requirement for Treasury to have undertaken an independent assessment, we believe that the approach taken to undertake the PIA is flawed, conflicted in nature and not in keeping with the recommendations of the OAIC in its Privacy Impact Assessment guidelines.

We note that Treasury explains the decision to undertake the PIA internally in a number of ways.

First, the PIA states:

> *The CDR regime as a whole is largely directed at protecting the data of consumers, including individual's data. It was therefore not appropriate to separate the assessment of privacy impacts and proposals to address privacy risks from the core policy development function being undertaken by Treasury.*[40]

We acknowledge that it is clearly the case that Treasury have a policy development function in implementing the CDR regime. In implementing and developing this policy though there is a fundamental balancing act that needs to take place between the protection of personal information of Australians with the interests of business in carrying on or innovating their profit driven activities. The regime being proposed is therefore not solely directed at protecting the data of consumers– it is directed at balancing the specific interests of consumers in accessing their own data with the specific interests of business to innovate and create new business models based on the use of that data. This economic element has always been an integral part of the data bargain, and remains a key underlying assumption to its implementation. As the Productivity Commission stated in its Inquiry into Data Availability and Use Report:

> *Effective use of data is increasingly integral to the efficient functioning of the economy. Improved availability of reliable data, combined with the tools to use it, is creating new economic opportunities. Increasing availability of data can facilitate development of new products and services, enhance consumer and business outcomes, better inform decision*

[39] Privacy Impact Assessment Consumer Data Right December 2018, https://static.treasury.gov.au/uploads/sites/1/2018/12/CDR-PIA.pdf

[40] Page 30 Privacy Impact Assessment Consumer Data Right December 2018,

> *making and policy development, and facilitate greater efficiency and innovation in the economy.*[41]

We also note that this economic element is downplayed in the PIA, with benefits to privacy highlighted. The Objectives of the Consumer Data Right section states:

> *It is partially intended to enable the development of third party services that may enhance privacy rights, by helping individuals to understand what data is held by businesses and understand and manage collection, use and disclosure permissions.*[42]

The use of the word partially, in our view, understates the case. The creation of new FinTech services is a fundamental part of the CDR, without which it would not even be viable. The object of the Act is to create more choice and competition,[43] the only way this can occur is if there are new FinTech services to assist people to do compare.

The policy development process in implementing the CDR can therefore lead to greater or lower privacy protections depending where this balance is judged to be. It is for this reason that the privacy impact assessment should be completed by an independent body. The OAIC guidelines state that:

> *Some projects will have substantially more privacy impact than others. A robust and independent PIA conducted by external assessors may be preferable in those instances. This independent assessment may also help the organisation to develop community trust in the PIA findings and the project's intent. Footnote: A number of privacy consultancies and law firms offer PIAs as a service.*[44]

The decision not to in this case gives rise to a possible perceived or actual conflict of interest. Given Treasury's mandate by government to implement a Consumer Data Right in a very short period, it could be seen to be in Treasury's interest to downplay any privacy issues that may arise from consideration of the CDR and therefore delay the implementation. A poor *independent* privacy impact assessment may, for example, recommend a re-think of the legislation to bolster privacy protections, which may have obvious policy development implications. The current assessment in our view does downplay many risks. This will ultimately go to undermining community trust in the CDR and the Government's role in implementing it. Given increasing community concerns with respect to Government data initiatives such as the My Health Record and the most recent Census, this lack of trust is likely to be considerable – especially when the first sign of problems arise.

Second, the PIA states:

---

[41] Page v. Productivity Commission, Inquiry into Data Availability and Use Report, https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf

[42] Page 18, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[43] Section 56AA(c) *Treasury Laws Amendment (Consumer Data Right) Bill 2018*

[44] Page 10, Office of the Australian Information Commissioner, Guide to undertaking privacy impact assessments https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf

> *This development process took place over approximately 18 months, in an iterative way, involving multiple consultations. This did not lend itself to a point in time assessment by external consultants.*[45]

Any point in time along this process – particularly after the exposure draft bill was developed could have been an appropriate time to begin. Given the delay in the implementation timeframe, now would be a good time too.

Third, the PIA states:

> *The internal development of the PIA also reflects Treasury's recognition of the importance of developing internal capability in relation to PIAs and a better understanding of the privacy issues and risks raised by the CDR as part of its design. This was a secondary factor in the decision to conduct the PIA internally and had little influence on the decision.*[46]

Using the development and implementation of legislation that will have a profound impact upon Australian's privacy as a training ground for PIA capabilities seems inappropriate. If there is any case that requires experience and expertise it would be this one.

As we understand it, Treasury's consideration of many of the privacy risks was limited to internal brainstorming sessions with no specific external consultations or surveys. Without specific privacy expertise, nor expertise in the behaviours of the financial services sector and the burgeoning FinTech and IT sectors that external, independent perspectives could provide, we believe the approach taken is flawed.

Finally, given OAIC's role in the CDR, the decision by Treasury to go against the explicit advice of the co-regulator is problematic and does not provide any more confidence in the process or the OAIC advice.

Recommendation

17. Treasury should engage an external consultant to finalise the development of the current PIA.

Examining the substance of Treasury's PIA, Financial Rights has raised a series of concerns with Treasury. It is worth repeating these concerns for the Committee here in order that these concerns be addressed either in the Privacy Impact Assessment itself or in the legislation.

[45] Page 30, Treasury, Consumer Data Right, Privacy Impact Assessment, December 2018

[46] Page 30, Treasury, Consumer Data Right, Privacy Impact Assessment, December 2018

Mapping of personal information flows

The PIA attempts to describe the personal information flow using the example of Naomi.[47] While this describes the complexity of the data flow and is somewhat useful – what remains missing is a description of what privacy protections will be available to a consumer at every step of this flow.

The complexity of what is being proposed with respect to the application of APPs, CDR Privacy protections and general law at different stages remains obscure and difficult for industry, lawyers, and consumer representatives to understand, let alone a consumer.

An explanation, flowchart or visualisation of what privacy protections apply at what stage should be a central feature of the Privacy Impact Assessment. Understanding what protections are available when and applying to whom would be in our view critical for a comprehensive privacy assessment to be undertaken. Without it, the privacy assessment is incomplete.

Consumers need to be aware of their privacy rights at different stages of the process in order to build confidence in the CDR. This is because there are higher and lower levels of protection at different stages and the level of protection should influence their decision making process. Simply asserting that consumers can simply complain to External Dispute Resolution (**EDR**) after the fact and find out what protections apply is inadequate and fundamentally undermines the stated aim that consumers be educated in their consumer data rights.

If it is too complicated for Treasury to create a simple explanation it will be too complicated for consumers to understand.

Recommendation

18. An explanation, flowchart or visualisation of what privacy protections apply at what stage should be included in the Privacy Impact Assessment.

Vulnerable and Disadvantaged Individuals

Financial Rights commends Treasury on the inclusion of a section on vulnerable and disadvantaged individuals and the inclusion of vulnerability considerations in Recommendations 1 and 3.

We wish to make one comment though. Further categories of vulnerability and disadvantage should be listed explicitly in this section, including:

- People suffering from mental health issues

[47] Stages 1-6 at Pages 41-42, Consumer Data Right Privacy Impact Assessment.

- Older Australians
- Aboriginal and Torres Strait Islander peoples

While the first two groups have been appropriately mentioned in the consent section, this is not enough. These groups have unique experiences and issues that will mean the CDR will impact upon them in different ways and they will experience Open Banking and their Consumer Data Rights in ways very different to other Australians.

Recommendation

19. People suffering from mental health issues, Older Australians, Aboriginal and Torres Strait Islander peoples should be explicitly listed in the section addressing Vulnerable and Disadvantaged Individuals.

Mitigants that were not adopted - Banning other forms of sharing of CDR data

We note that the PIA raises the issue of screen scraping. In part the PIA states:

> *There are a broad range of data sharing arrangements currently in place. The CDR regime cannot meet all of the different tailored requirements of these arrangements. Prohibiting them would have significant negative impacts on consumers and business. As the CDR develops it is expected that it will meet the needs of many of these arrangements. If the CDR is designed and implemented in a way that is efficient, convenient and that inspires confidence in consumers and businesses, it is expected that consumers and business will choose to use the 'safe pipe' that it represents.*[48]

The position that if there is a safer more trusted option then consumers will use this service rather than the unsafe service, fundamentally misunderstands both the incentives of bad financial services actors to avoid the safe pipes altogether, and the real world incentives for consumers to submit to these bad actors and use the unsafe pipes.

A number of points need to be made. Firstly, the higher regulatory hurdles of CDR accreditation will be a significant disincentive for these businesses, particularly fringe financial services, from joining.

Second, financially vulnerable people will continue to be desperate enough to seek fringe financial services and will do anything, including signing up to a service that uses unsafe screen-scraping practices in order to gain access to these services. Many of these consumers will not concern themselves with the nuances of privacy protections to do so. If it means engaging with and submitting to the requests or demands of non-CDR accredited entities like pay day loan operators or other emergent services, financially vulnerable consumers will do so.

[48] Page 107

This will result in financially vulnerable people ending up with lower privacy protections and at greater risk to harm due to lack of protection from existing protections. For example, accessing data via 'screen scraping' technology amounts to a breach of the terms and conditions of a customer's bank account, as the consumer is handing over their PIN or access to their online account. If they were then to have funds taken from their account the customers is at risk of losing their protections under the E-Payments Code as they have, by allowing access to a third to their account[49]

The PIA does not address the outcomes from this inevitable regulatory arbitrage. While the CDR Bill includes the offences of misleading or deceiving a CDR consumer and holding out as an accredited person, it does not address the situation where the consumer is pressured to provide the CDR data to an entity using screen scraping technology who is clearly stating that they are not an accredited entity, whereby gaining inappropriate access to the consumer's CDR data. This remains the case, despite the new ACCC rules preventing the sharing of CDR data with a non-accredited entity in version one of the Rules.[50] This is because consumers will be able to still access their own data and pass this on to the non-accredited entity in a form that they will be able to use.

We note again that screen-scraping has been banned in other countries such as the UK.

Recommendation

20. The PIA needs to address the issue of screen-scraping and makes recommendations that mitigate the problems that arise from its interaction with the CDR regime.

Other possible mitigants as yet unconsidered.

Financial Rights has previously put forward risk mitigation strategies for some of the privacy risks that arise. Many of these have now been considered in the PIA. However others have yet to be addressed and we believe need to be. While we accept that they may be rejected we believe Treasury needs to specifically and explicitly explain why these obvious risk mitigation strategies have been rejected. These include:

- A legislated prohibition of on-selling as opposed to leaving this to the ACCC rules;
- An outcomes-based regulatory approach that could include post-purchase/post-initiation audit surveys to find out what consumers believe that they have consented to and whether this aligns with the consents as formulated by the data

[49] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

[50] Rule 8.8, ACCC CDR Rules Outline, December 2018,

recipient. These audits would be compulsory, conducted independently and require a certain percentage of consumers to have understood the consents, otherwise, data recipients will need to improve their consent and have increased monitoring to ensure their consent process meets best practice. Such an approach will give industry the ability to innovate, while ensuring that they meet regulatory expectations.

- The use of RegTech to develop market analyses of CDR products and services to examine actual consumer outcomes in the finance services market. Regulators should be provided with detailed market monitoring tools with transaction detail data for everything from default data, claims, sales and quotes data to transaction information;
- Introducing concepts of anonymised data (where re-identification is impossible by any party by any means) and pseudonymous data (except re-identification techniques are reasonably likely to be used) be embedded in the Consumer Data Right and the Open Banking regime.
- Strengthening of CDR privacy protections as recommended in our previous submission

Recommendation

21. The PIA needs to address a number of mitigation strategies put forward by consumer representatives including:

a) a legislated prohibition of on-selling data;

b) the introduction of an outcomes-based regulatory approach that includes post-purchase/post-initiation audit surveys;

c) the use of RegTech to develop market analyses of CDR products and services to examine actual consumer outcomes;

d) introducing concepts of anonymised data and pseudonymous data to improve controls over the subsequent use of data;

e) further strengthening CDR privacy protections.

Risk Rating Matrix

The Risk Rating Matrix as presented in the PIA is problematic. The risk severity is as we understand determined by the typical case rather than the extreme case.

This leads to the strange outcome seen at Scenario 2.1[51] where the example provided regarding political views is leaked, the likelihood of that leaking happening as highly likely and the risk severity is deemed minor. Political views are one of the categories of sensitivity under the *Privacy Act*. The breach and misuse of political views drawn from data farming on Facebook has arguably led to major impacts upon western democracy. This is not a minor privacy breach for either the individual or society as a whole.

It also leads to similarly absurd outcomes at Scenario 1.3, which states:

> *The individual may engage an accredited data recipient who instead seeks data outside the CDR system. E.g. Naomi may engage with a tech company believing that access is obtained through the regulated framework of the CDR. The data recipient instead obtains her personal information through screen scraping.*[52]

The risk severity here is deemed "minor" despite the fact that screen-scraping takes away all the persons rights under the terms and conditions of the data-holder and can involve severe subsequent problems (see above on page 8).

Scenario 4.5 states:

> *The data holder may intentionally or unintentionally send inaccurate data. E.g. NN Bank sends transaction data to BetterDeals containing transactions processed by NN Bank in error.*[53]

This is however deemed a minor severity despite the fact that the wrong details will feed into algorithms producing significant flow on impacts upon an individual's credit worthiness, credit ratings or be prevented from accessing certain services at all. This is not a minor consequence for most people.

By developing a risk severity rating based upon a probability distribution ensures that the severe consequences that impact upon an individual will be nullified by the breadth of the population or reference to a typical case.

We recommend that if Treasury are stuck with the format, at the very least for each Potential Risk that at least 5 examples be provided – extreme, major, moderate, minor and insignificant scenarios. An extreme example leads to extreme outcomes, a minor risk, minor outcomes. It is misleading to present a generalised description of severity given the multiplicity of cases.

We recommend too that a full description of the process Treasury undertook to determine risk severity be included in the PIA for transparency's sake and for the public to better understand how Treasury came up with the determination.

Subsequently we recommend that Treasury consult widely on risk severity. While we are sure Treasury is diverse there is no way Treasury employees could be in any way seen to be representative of the broader community and they can not reflect general attitudes towards privacy matters.

---

[51] Page 55, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[52] Page 54, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[53] Page 60, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

Recommendation

22. Treasury should reconsider the use of the risk matrix and consult widely on risk severity of the scenarios listed.

Treasury judgements as to likelihood

As with risk severity, we do not agree with many of the judgements made by Treasury with respect to the likelihood of a risk.

For example scenario 4.10 is deemed "unlikely":

> *A third person may pose as the accredited data recipient to gain access to the individual's raw transaction data from the data holder. E.g. A third person could pose as BetterDeals to request and obtain Naomi's raw transaction data from her bank, NN Bank.*[54]

This however is highly likely in a great number of scenarios including many in-store sales scenarios, in scenarios involving aged parents and their children, with parents and their young children; as well as non-English speaking consumers and their English speaking relatives.

Scenario 5.2 states

> *The accredited data recipient may misuse the information provided by the individual in a way technically consistent with their authorisations. E.g. BetterDeals may use information such as emails, telephone numbers, and other personal details in a way that, while technically consistent with an authorisation, is improper or abusive.*[55]

This is deemed "possible" by Treasury. It is our expectation that data collector's will regularly seek to use data that may be technically consistent with consent but are used in ways not necessarily understood by the consumer or not conceived of by the consumer. This use (or misuse) of data seems to us to be the entire business model of data harvesters.

Recommendation

23. Treasury should reconsider the likelihood ratings and consult widely on the likelihood of the scenarios listed.

Non-accredited parties

[54] Page 61, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[55] Page 61, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

We note that the PIA states, in part:

> *The CDR does not create rights for consumers to direct accredited entities (or original data holders) to transfer their data to non-accredited entities. It may allow accredited persons to voluntarily do so at the direction of the consumer. Therefore the potential is limited for non-accredited entities to pressure individuals to provide their personal information outside of CDR frameworks as a condition of receiving a service.*[56]

While the CDR does not create rights for consumers to direct accredited entities (or original data holders) to transfer their data to non-accredited entities, consumers do have the ability to request their own data and this can be in a format that could be read by a computer program – whether it is in a pdf or other machine readable or screen scrapable format. It is this ability that enables non-accredited entities to potentially pressure individual consumers to provide the personal information outside of the CDR regime - not necessarily the consumer's direction to an accredited party.

This issue is actually raised later under the *Preventing the consumer from accessing their own data* section[57]. The PIA states:

> *Some stakeholders have raised concerns that if consumers have the right to access their own data, with the data provided in a useable form, unscrupulous actors will use the consumer to bypass the accreditation requirement.*
>
> *It has been suggested that this skirting of the CDR framework could be achieved, for example, by the third party not receiving the data themselves but instead providing the consumer with the software that enables the consumer to download the data via an API. CDR data would then be stored on the consumer's device or on cloud storage under an account that is owned by the consumer, but accessed by the non-accredited third party.*[58]

This still does not quite capture the concern described above but gets close.

In rejecting a closed system, the PIA suggests that there will be risk mitigants available. The PIA suggests that:

> *this risk could be mitigated by ensuring data holders are not required to provide this access through an API in standardised formats. Data holders could instead be enabled to determine the format in which this information is provided to the consumer, so long as it is provided in a user-friendly digital format.*[59]

A user-friendly digital format is easily "screen scrapable" to gain access to the consumer data – again, a process not prohibited under the CDR regime.

The PIA goes on to state:

---

[56] Page 66, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[57] Page 100, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[58] Page 110, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[59] Page 110, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

> *Greater friction would be introduced if the consumer accessed this information themselves rather than disclosing it to an accredited person.*[60]

This friction may exist but given the opportunities and incentives involved in a particular transaction with a desperate consumer, facing financial hardship and a bad actor financial services entity, this friction is a minor hurdle and easily overcome.

Then the PIA states:

> *Additionally, education and clear branding of CDR transfers would ensure consumers know that when they are transferring this way, they are no longer using the CDR (see below for further discussion of branding).*[61]

While helpful, a desperate consumer, facing financial hardship will be willing to ignore all advice.

Finally the PIA states:

> *While this would not prevent consumers being used as a funnel in every instance, and as such would not eliminate this risk, it would act as a de facto barrier for the majority of consumers who are considering sharing their data with a non-accredited third party.*[62]

Ultimately we agree with Treasury on this point. It may very well prevent most people from engaging in risky behaviour but it will be the vulnerable consumer, the consumer experiencing financial hardship that will be most at risk under the CDR regime as currently designed.

Treasury Privacy Recommendation 1 - Behavioural research

Financial Rights supports the proposal to have the Data Standards Body to have regard to vulnerable groups and that

> *Test groups should be of sufficient size and diversity to provide justified confidence in the safety of consent processes.*[63]

We note that

> *Initial research will be undertaken in three stages. There will be at least 20 participants in the first stage, a further 50 in the second stage, and a further 20 in the third stage. Participants will be recruited by CHOICE. It is expected that further research will be undertaken throughout the implementation of the CDR*

We are not entirely confident that the full range of vulnerabilities will be able to be represented in a sample size of 90 and consideration should be given to increasing this sample size as appropriate. While we presume they will be, we recommend the full results of these tests be made public.

---

[60] Page 111, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[61] Page 111, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[62] Page 111, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

[63] Page 117, Treasury, Consumer Data Right Privacy Impact Assessment, December 2018

Treasury Privacy Recommendation 4 – preventing undue weight on the benefits of competition and innovation

Financial Rights supports this recommendation except that it is incredibly vague. What defines undue weight? When will we know undue weight has been given by a regulator on competition issues? It is a subjective test that will provide the opportunity to claim that they did not provide undue weight to these factors. It needs to be further defined and should be quantified.

Treasury Privacy Recommendation 7 – consumer education

We recommend that any education about the CDR should be less a sales pitch for the benefits of open banking and open data generally but specifically raising awareness about the risks and provide warnings to consumers of the potential negative consequences of breaches etc.

Recommendations

24. **Treasury should consider resourcing an increase to the sample size in consumer testing to ensure that appropriate levels are reached**
25. **The consumer testing results should be made public.**
26. **Further guidance on the meaning of undue weight should be provided.**
27. **Education about the CDR should focus on raising awareness about the risks of the sharing of data and provide warnings to consumers of the potential negative consequences of breaches.**

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 Financial Rights on [redacted]

Kind Regards,

[redacted]

Karen Cox
Coordinator
Financial Rights Legal Centre
[redacted]