

DATA
STANDARDS
CHAIR



Consumer
Policy Research
Centre

Vulnerability, capability, opportunity

Understanding consumer
vulnerability as a key to
unlocking benefit from the
Consumer Data Right



Objective

The Consumer Policy Research Centre (CPRC) has been engaged by the Data Standards Body (DSB) to prepare a series of consumer research reports on how the Consumer Data Right will change the experience of Australian consumers transacting in the data economy.

Our reports cover subjects identified as being priority topics by the DSB and CPRC, addressing issues that are of significance for government, industry and the wider community. Our research findings are derived from direct engagement with community sector stakeholders, evidence held in CPRC's broader consumer research bank, and analysis of a range of material relating to CDR and to data markets and consumer data reforms in other jurisdictions.

This report, the third in the series, explores opportunities to realise benefits of CDR for consumers experiencing vulnerability; community services supporting those individuals and households; and policymakers seeking to understand how use of consumer data impacts on peoples lives, wellbeing, and access to essential services.

Our project is helping to realise the policy intent of CDR as a consumer-centric reform geared toward creating a fair and inclusive data economy in which competition and innovation provide consumers with opportunities and mechanisms to achieve the market outcomes they deserve.

Our work taps into the subject expertise of community sector organisations to bring practice-informed knowledge of consumer experiences, needs, and expectations for data sharing into the evidence base informing ongoing development of data standards for Australia's Consumer Data Right (CDR). Our vision is for the community sector to be supported in contributing to CDR development in ways that will facilitate all Australian consumers having access to positive outcomes from the regime.

Methodology

This report is based on qualitative research (case study methods) and literature review. It also draws on previous CPRC research in the area of consumer vulnerability, in particular our recent report for the Australian Energy Regulator: [Exploring regulatory approaches to consumer vulnerability: a report for the Australian Energy Regulator](#), Melbourne: AER/CPRC.

Qualitative research for the project was conducted in two phases:

Phase 1 consisted of in-depth interviews, conducted via telephone or video conference. A CPRC staff member spoke to 20 individuals from 13 peak and frontline organisations providing advice, advocacy or services to consumers across financial, energy and telco markets. Interviewees held professional expertise in a range of areas, including consumer policy; consumer vulnerability; financial capability, hardship and debt; domestic and family violence and economic abuse; services for Aboriginal consumers; legal services; consumer rights; and inclusive service design. Most interviews were recorded (where permission to do so was granted by interviewees). Consumer issues in relation to joint accounts was the primary topic of discussion: we spoke about where CDR might exacerbate or ameliorate existing consumer issues; and where new opportunities and risks might emerge specific to consumers' use of CDR products and services. These were largely unstructured conversations, guided by the interviewer to accommodate differing consumer expertise and level of CDR understanding held by interviewees; and intended to surface real and fictional joint accounts scenarios that were grounded in lived experience. Phase 1 interviews comprise the primary evidence base informing CPRCs second report in this series (which looked at CDR and joint accounts), and have also been utilised in compiling this, our third report.

Phase 2 consisted of two video conference roundtable discussions, with eight participants drawn from the pool of prior interviewees. These were semi-structured discussions facilitated by the same CPRC staff member who conducted the Phase 1 interviews. The nominated topics for discussion were consumer vulnerability and capability; consumer consent; and measuring consumer outcomes. Permission was obtained from participants to record both roundtables, however recording failed in one case – for this discussion we have notes only. The phase 2 interviews again sought to surface real and fictional CDR scenarios, this time in relation to consumer experiences of vulnerability and implications for CDR.

We note that a public consultation period on proposed CDR Rules changes had closed immediately prior to our Phase 2 research roundtables (the Australian Competition and Consumer Commission, *CDR rules expansion amendments - Consultation Paper*). As a result, these Phase 2 interviews incorporated discussion of many of the proposed changes set out in that consultation, including elements which were not ultimately adopted in December 2020 Rules changes; but which remain open as future possibilities for CDR. Accordingly, the hypothetical scenarios developed out of Phase 2 discussions that are included in this report do not always entirely correspond to CDR Rules current at the time of writing. We acknowledge this variance, but consider they remain relevant as reflecting policy settings – and associated potential consumer vulnerability impacts – that have been communicated as remaining very much 'on the table' for future iterations of CDR. To mitigate against any potential confusion, we have noted in-text the variances against current policy settings. We further consider that any potential for confusion is outweighed by value gained in representing important stakeholder views on consumer vulnerability and CDR opportunity and risk from a consumer interest perspective.

Qualitative research was conducted with a relatively small sample group of interviewees, and we recognise that discussions with a different universe of participants would have surfaced a different set of experiences, opinions, and scenarios. This report does not purport to capture the full range of views held by consumer representatives regarding consumer vulnerability or CDR data sharing. Rather, we have sought to highlight the diversity and complexity of consumer circumstances; and provide a channel for the CDR regime to continue to engage with consumer representatives to support better outcomes for all consumers whose data it is enacting rights to.

Contents

Executive Summary	1
Part 1: Landscape	3
<i>Understanding consumer vulnerability</i>	
Part 2: Use cases	9
<i>Consumer vulnerability in the context of CDR</i>	
Part 3: Toolbox	19
<i>A conceptual toolbox for tackling consumer vulnerability</i>	
Part 4: Approaches	25
<i>Applying principles to practice for CDR standards and implementation</i>	
Part 5: Opportunities	30
Conclusion	35
Endnotes	37
Appendix 1	41
<i>Table: definitions of consumer vulnerability</i>	

Executive Summary

Vulnerability affects us all. Principles that support policymakers, consumers, businesses, and regulators to act safely and well in their decisions and actions will help realise the potential social and economic value of the CDR reform.

CPRC's most recent data and digital consumer survey tells us that 97% of Australians believe companies have a responsibility to protect consumers against their information being used in a way that makes them worse off, and 94% believe this responsibility is shared by government¹.

A Consumer Data Right that supports the autonomy and wellbeing of consumers, works against exploitation of vulnerability, and which provides for both businesses and consumers to gain fair value from consumer data will yield a stronger and more sustainable reform than one which leads consumers to feel they have been misled or manipulated into outcomes they did not expect. The challenge of achieving this is significant, but the cost of not attempting it will be higher.

In speaking with consumer advocates and community sector organisations about CDR, the overarching concern we heard is that CDR reforms might inadvertently widen consumer disparity, exacerbate vulnerability, or contribute to market exclusion. These fears are well-founded: informed by longstanding engagement with the financial, legal, and social impacts of fallible information systems; familiarity with predatory, discriminatory, or careless market practices; and exposure to the debilitating effects of consumer disempowerment.

Our interviews and roundtables with community sector also surfaced perspectives on how to unlock CDR's potential and fulfil its aim of providing consumers with safer and more transparent modes of data sharing than are currently available to them. Drawing on the knowledge shared in these conversations, and other research findings, we suggest four key principles to guide CDR's approach to consumer vulnerability² (outlined on the right).

Vulnerability principles for CDR



CDR reforms should respond to consumer vulnerability as a positive opportunity to strengthen systems, build resilience, and grow trust.

CDR services should provide people with agency to achieve ambitions, and respond to crises, as well as to manage their everyday consumer experience.



CDR use should not increase consumer vulnerability. No one should be put in a position where choosing to use CDR products leads to significant harm or compromises their access to essential services.

CDR design should support consumers' market participation. No one should be unfairly denied opportunity to use CDR products and services, obtain benefits from CDR data sharing, or challenge the legitimacy of negative outcomes.



Presenting real-world case studies and imagined scenarios to illustrate different aspects of consumer vulnerability and how these might intersect with potential CDR use cases, this report provides context for why operationalising vulnerability principles is key to unlocking benefit from the Consumer Data Right for all consumers.

We propose there are opportunities for a range of systemic and operational approaches to be implemented that could help embed a duty of care for vulnerable consumers into the CDR regime. Specifically, we suggest:

- **Integration of vulnerability principles into the work program of the Consumer Data Right.**
- **Development of clear aims, indicators, and measures for consumer outcomes of CDR, including measures that are specific to known or predicted areas of consumer vulnerability.**
- **Mechanisms to harmonise consumer experience of data standards across industry and legislative contexts.**

And, as part of the DSB work program:

- **Iteration of data standards and/or CX guidelines specific to CDR consumer dashboards and consent management.**

These are deliberately aspirational calls to action, some of which we recognise are beyond the scope of DSB to implement. This reflects our view that both consumer vulnerability and consumer data reforms require cohesive whole of government approaches if they are to succeed. Our proposals, and the role DSB might play in actioning them, are more fully elaborated in Section 5.

Defining consumer vulnerability

A clear definition of consumer vulnerability will assist CDR policymakers and regulators in the design of internal processes to collect, analyse and communicate data that evidences the effects of the reform in terms of accessibility, usability, safety, and fair outcomes for consumers.

Agreed terminology is important to be able to meaningfully compare effects in and across different sectors: to predict and detect problems, to outline desired outcomes, to perceive successes, and to clarify requirements or expectations incumbent on industry participants who want to make use of consumer data under the scheme.

A common understanding of consumer vulnerability between CDR participants, policymakers and regulators reduces the likelihood of misunderstandings about what is required where CDR standards, rules, or metrics require attention to vulnerability. It plays an important part in building shared understandings between different disciplines within and across organisations: allowing economists, technical specialists, and subject experts in consumer vulnerability to communicate effectively and embed a culture of consumer safety into organisational cultures.

Equally, it is important to realise that any definition can only be partial. In providing a working definition of consumer vulnerability, we emphasise that there is no uniformly accepted or consistently held definition of consumer vulnerability among regulators, business, or consumer advocates³. As well, we recognise that 'vulnerability' is rarely the preferred language of consumers themselves, and initiatives using this language may further isolate people they are seeking to help.

At its broadest, consumer vulnerability refers to circumstances that cause difficulty in using markets or in receiving adequate products and services; or which heighten the risk of harm, detriment, or disadvantage to consumers.⁴



Part 1: Landscape

“We need to acknowledge that there are people who, no matter what perspective or lens you apply, they are vulnerable. In every aspect of their lives.

But vulnerability can also be episodic and unexpected – you can be absolutely fine one minute and completely vulnerable the next.”

- Participant at CPRC Roundtable, November 2020

Markets contribute to consumer vulnerability

Consumer vulnerability is often contingent with personal circumstances⁵, but this does not mean that everyone who shares those attributes will be vulnerable. However, because indicators for vulnerability are so frequently described in relation to personal circumstances or attributes, it can be easy to overlook the fact that market design is also a cause of consumer vulnerability.

Vulnerabilities experienced by both 'marginalised' and 'mainstream' consumers can be directly instigated by market features and behaviours. Businesses that steer consumers towards taking certain actions which are not in their best interests (whether that be purchasing junk insurance, taking out unaffordable loans or credit, upgrading to a product that exceeds their actual needs, or simply agreeing to unfavourable terms of service) sometimes do so by deliberately generating or manipulating vulnerability. This might include triggering consumer anxieties, leveraging information asymmetries, or exploiting behavioural biases⁶.

Consumer products or markets that initiate or amplify vulnerability through design features do so either inadvertently or deliberately⁷. Awareness of the prevalence of market impacts on consumer vulnerability⁸ and the additional sensitivities consumer data acquires as it is combined and processed⁹ challenges governments to devote attention to what CDR participants and regulators might need to do to ensure consumer data sharing under the scheme is inclusive and responsive to people's circumstances.

We suggest CDR can drive innovation that leads Australia's data economy to evolve in ways that are safe for consumers and which deliver benefit on both supply and demand side. Our community sector consultation emphasised this is particularly crucial within markets providing services essential to participate in society (energy, water, housing, telecommunications, banking); and in circumstances where consumers face heightened vulnerability.

SNAPSHOT 1:

Understanding consumer vulnerability

Addressing consumer vulnerability is the bedrock for consumer trust

Vulnerability is present whenever there is an information or power differential; it is an intrinsic part of market transactions.

The challenge is to ensure market environments do not abuse consumer trust or exploit CDR data - ie: no surprises.

Consumer vulnerability is dynamic and relational

Vulnerability is not a fixed state: market behaviours, regulatory actions, and consumer choices all play a part in influencing outcomes.

The challenge is to design systems that are responsive to changing needs and capabilities.

Consumer vulnerability is an indicator for systemic market issues

Vulnerability is not a symptom of individual weakness; it is an indicator of how systems and relationships are functioning.

The challenge is to avoid market environments that make vulnerable consumers canaries in the coalmine.

Consumer vulnerability affects everybody

We can all find ourselves vulnerable as a result of personal circumstances, external events, or market design.

The challenge is to design systems that ameliorate negative effects rather than enabling exploitation.

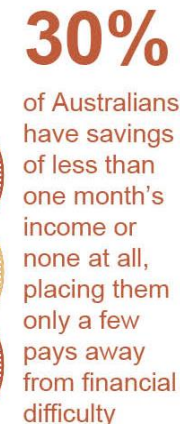
SNAPSHOT 2: Australian consumers' circumstances¹⁰

“We’ve been working really hard – with the banks in particular, but everyone in consumer industries – to try and improve accessibility at all levels.

For people without internet, for people who are not literate, people who speak English as a second language, all of these things. At the best of times, they’re finding it difficult to communicate and understand their rights.

When it’s something as complex as CDR ... the accessibility principle needs to be front and centre.”

Participant, CPRC consultation, August 2020



Consumer vulnerability has many shapes and many causes

Consumer vulnerability is not a clearly defined problem with a neat solution. It happens to all of us: in different ways, at different times, and with different outcomes. Policymakers and regulators around the world are increasingly shifting focus to acknowledge that vulnerability is not a niche condition and that anyone can become vulnerable as a consumer¹¹.

As consumers, we are faced with countless choices. Some relate to essential products and services, things necessary to sustain our health and wellbeing. Some relate to purchases that are discretionary but still important to our life satisfaction and participation in local economies. Some are potentially harmful. As individuals, we all make good choices and bad choices – and sometimes we are overwhelmed by life or by the moment, or by what is being asked of us, and don't feel capable of making choices at all.

At other times, we may not know about the range of choices available to us; may not be able to successfully communicate the choices we want to make; or may find ourselves unable to access important products and services because of unaffordability, unavailability, discrimination, or other barriers¹².

These are all aspects of consumer vulnerability.

The COVID-19 pandemic offers a global illustration of the extent to which consumer vulnerability can unfold in unexpected, widespread, and pervasive ways. While Australia has so far escaped the high infection rates and death toll that the virus has caused elsewhere, the unexpected loss of income experienced in many households and businesses, and the difficulties many people have faced in accessing medical, emotional, and wellbeing supports during and after 'lockdown' episodes demonstrates how easily consumers – who may never have previously considered themselves as vulnerable – can find themselves exposed to compounding financial and mental health stressors.

Flow-on effects of the pandemic response also give insights into some of the ways already-vulnerable consumers can face heightened disadvantage in accelerated shifts to digital platforms and services¹³.

“I don't think consumer vulnerability has really been fully addressed in CDR because the discussion so far has been so focused on privacy – even though that's also really important – that some of these issues have been slightly pushed aside.”

Participant, CPRC consultation, August 2020

“The realities of COVID inevitably amplify and increase vulnerability across most Australian households.

This can reduce people’s capacity to engage with financial decisions and handle ‘life admin’ tasks... It can also reduce people’s capacity to assess information and can lower their defences, making them more vulnerable to scams and misinformation.

...Products and services should not contain surprise fees or hidden features. This sort of ‘sludge’ harms consumers and ultimately costs business and shareholders.”

Karen Chester, Acting Chair, ASIC at the 2020 AFR Banking & Wealth Summit ¹⁴

Protections to mitigate consumer vulnerability build trust and wellbeing, enable market participation, and can even save lives.

Despite economies reopening and rebuilding after lockdowns, October data from CPRC’s six-month research initiative, *Consumers and COVID-19: from crisis to recovery*, register new spikes in payment assistance, missed payments, and refinancing activity continuing through October 2020. Missed household bill payments have been on the rise across almost all sectors, with 12% missing a telco payment, 12% missing a rental payment and 11% missing a credit/loan repayment¹⁵.

Consumer vulnerability can be triggered by personal circumstances, external upheavals, the design of consumer products and markets, or a combination of these elements. Consumers facing these conditions are more likely to experience exploitation and financial distress. Easing regulatory obligations as a mechanism to boost business throughput is not an effective remedy to economic downturn if it means that consumers who are already doing it tough are left vulnerable to greater harm¹⁶.

While many people will recover from the economic stress of recession, and some may thrive in the face of new opportunity, others will not be so lucky. Recent research suggests that people who experience severe financial strain may have up to a 20-fold higher risk of attempting suicide than those who have not been subject to financial hardship, with the risk increasing when financial stressors accumulate from multiple sources (debt, housing instability, unemployment, and low income)¹⁷.

This statistic is particularly troubling in the face of what we know about impacts of the COVID-19 recession, combined with the findings of the 2020 ACOSS Poverty Report which, on pre-COVID data, indicates 3.24 million people (or, 13.6% of the population) as living below the poverty line in Australia – including more than one in six children (17.7%) and one in seven young people (13.9%)¹⁸. These are devastating numbers.

There is scope for CDR to contribute to alleviating financial distress for some consumers by giving them access to tools and services capable of providing combined analysis of personal and product data to identify choices that are affordable, beneficial, and appropriate to their needs. For other consumers, CDR may help them in directing advocates and support services towards relevant, accurate and timely information in relation to their consumer data and how it has been shared.

With its focus on data innovation and data analysis, there is also opportunity for the scheme to play a role in early identification of vulnerability and consumer harms, which might assist businesses and support services in minimising the accumulation of financial strain on vulnerable consumers. This is relevant not only to CDR’s initial roll out in banking, but also for comprehending and combating consumer vulnerability in relation to essential services such as utilities, telecommunications, and housing; as well as vulnerability impacts in other financial markets such as insurance and superannuation (and managed funds more broadly).

Learning from consumer vulnerability

CDR improves the data sharing landscape but is not a panacea against poor data sharing practices. Alongside legislative reform, government must continue to effectively promote cultural changes within business and data communities that recognise a healthy digital economy as one that provides sound duty of care for consumers alongside increased consumer agency.

A social model of vulnerability is one way to understand what consumer vulnerability can convey about how to create fair and inclusive markets. This is analogous to a social model of disability¹⁹, which contends that it is society's responses to disability (rather than disability itself) which comprise the underlying 'problem' that confronts people with disabilities. Similarly, conceptualising a social model of consumer vulnerability can help to clarify for CDR participants and consumers that vulnerability itself is inherently neither good nor bad; and it is how market environments shape and respond to the consumer experience of vulnerability that has most influence over positive and negative outcomes.

Importantly, flipping the 'vulnerability problem' from the individual to the social situates it more clearly in the policy domain. Understanding how triggers for consumer vulnerability are set by market actors (at both transactional and structural levels) allows clearer scope to design effective policy and regulatory solutions. As well, a social model recognises that consumer vulnerability does not only have negative consequences as a precursor to exploitation, but that appropriate policy and practice responses to vulnerability can also seed positive impacts for consumer trust and empowerment.

CDR legislation provides for important consumer protections that can help set the scene for this kind of model. It requires that consumers voluntarily give their express, informed, and specific consent for Accredited Data Recipients to collect, use or disclose data²⁰. It articulates the right of consumers to elect that CDR data they choose to share for a specific purpose is deleted when consent expires, is withdrawn or is otherwise revoked²¹. It offers a safer alternative to the risky but widespread practice of screen scraping²². And, through the mechanisms of CDR receipts and dashboards it requires channels for consumers to maintain visibility over the status of their CDR data sharing consents, and to extend, amend, or withdraw those consents in line with their circumstances and intentions.

Embracing the spectrum of social and technical needs and capabilities of consumers who experience vulnerability will strengthen CDR systems by making them more usable and accessible for everyone. Extending CDR's existing CX principles and data standards to provide guidance for inclusive consumer dashboards and consent management platforms will help embed these considerations to products that are both responsive and responsible.

“Opportunity focused reforms are often contingent on a lot of assumptions about people interacting in a certain way, or understanding certain things based on the information they are given.

Vulnerabilities change those interactions and can mean people are not able to exercise their choices in the way the system assumes they will.”

Participant, CPRC Roundtable, November 2020

Part 2: Use cases

“What is the benefit of CDR to business versus the benefit to consumers – and particularly more vulnerable consumers – compared to the risks it might bring?”

Are you designing a system that’s safe to use, or are you designing a system that puts all the onus back on people experiencing vulnerability and the services that support them to manage any risk created by the platform?”

- Participant at CPRC consultation session, August 2020

How do we anticipate consumers who experience vulnerability will be using CDR products and services?

The following pages present a selection of potential CDR use cases highlighting areas where consumer experiences of vulnerability may be expected to interact with CDR products and services. We emphasise that there are many other influencing factors in relation to consumer vulnerability that are not covered by these use cases, including experiences relating to age, disability, CALD contexts, mental health, trauma, social isolation, and digital fluency. All of these (and more) should continue to be explored as part of understanding consumer inclusion and opportunity through CDR.

CPRC has developed hypothetical consumer “scenarios” to assist in thinking about consumer vulnerability in the context of CDR and its possible future directions – these are fictional examples, drawing on our discussions with community sector organisations and consumer advocates. We note that a public consultation period on proposed CDR Rules changes had closed immediately prior to our Phase 2 interviews, and our discussions spanned some of the proposed changes set out in that consultation, including elements which were not ultimately adopted in December 2020 Rules changes; but which remain open as future possibilities for CDR.

Accordingly, the hypothetical scenarios presented here have some variance from CDR Rules current at the time of writing. They remain relevant as reflecting policy settings – and associated potential consumer vulnerability impacts – that have been communicated as remaining ‘on the table’ for future iterations of CDR. To mitigate against potential confusion, we have footnoted variances against current policy settings. We consider that any potential for confusion is outweighed by value gained in representing important stakeholder perspectives on consumer vulnerability and future CDR opportunity and risk.

Use cases capturing how consumer vulnerabilities might affect or inform CDR offerings and outcomes will, by their nature, expose both opportunities and risks. Stakeholders with professional expertise dealing with consumer vulnerability in the community sector readily acknowledge that businesses face significant challenges when dealing with customers who are experiencing vulnerability. There are often discrepancies between what a business must do under the law, what they are directed to do according to industry or best practice guidance, and what they may want to do to meet a customer’s specific personal needs.

Stakeholders we spoke to also recognised that CDR is a high-level reform that will apply to an extremely diverse set of businesses across all sectors of the economy, and that CDR rules and standards will not always be the appropriate mechanism through which to implement vulnerability measures, many of which will by necessity be matters of organisational policy or will fall within the domain of other regulatory standards or instruments applying to a particular sector.



Consumer vulnerability & impacts for CDR use cases

Community sector organisations have told us:

- Not all people who are experiencing vulnerability want to disclose it.
- Not all people who are experiencing vulnerability are able to disclose it.
- Terminology that emphasises ‘vulnerability’ can be stigmatising and disempowering; use of strengths-based language is preferable.²³
- People who are at risk of vulnerability may not always meet formal criteria or preconceptions of a vulnerable consumer.
- People experiencing vulnerability are likely to be anxious about the reliability of information others hold about them: “That data is so powerful – a provider says to them: *That’s your word, but I’m looking at data that say x, y, z.*”²⁴
- CDR expects a certain level of engagement and capability from consumers which is not realistic for many and may be particularly unrealistic when combined with stressors associated with consumer vulnerability: “There’s an assumption that people are aware of all the detail – systems that work on that assumption increase risk.”²⁵
- Access to information is important, however reliance on information disclosure is not the answer to market induced consumer vulnerability.²⁶
- Automated channels for customer interactions may limit the opportunity for businesses to identify signs of vulnerability²⁷ and to initiate investigations or exceptions that can help individuals in the system: “Transfers of data become a substitute for an actual relationship with a person.”²⁸
- Being heard if things go wrong helps mitigate vulnerable consumers becoming disengaged or disenfranchised from the scheme: “Awareness that there is something you can do that works, that you access for free.”²⁹

Scenario: Cal

Cal is in his thirties and has recently separated from his defacto partner of ten years. He works long hours in a high-pressure job. Cal uses betting as 'stress-relief' and has been racking up increasingly large gambling losses recently. He doesn't believe himself to have a gambling problem, but recognises it's starting to affect his ability to meet financial commitments on time.

Looking for a way to get on top of his finances, Cal runs some internet searches for budgeting tools. Later that evening when he logs into one of his betting apps Cal sees an ad for free budgeting app 'Pebble'. He recognises the name and decides to sign up.

Cal's impatient to get started. Even though he only read the first page of Pebble's Terms of Service (and none of the Privacy Policy) when he created his Pebble account, Cal ticks all the boxes requesting CDR consent. In doing so, Cal has provided Pebble with CDR consents to collect and use his data for twelve months, including for research and direct marketing, as well as giving them an insight disclosure consent.

Pebble combines Cal's CDR data with the data they collect about his use of the budgeting app. They know that he usually logs on late at night, after he has made online or onsite gambling transactions, and is most interested in reviewing the status of his debts. CDR data from his credit card shows frequent spending on online gambling sites and cash advances at the casino. CDR data from his transaction account tells them his income.

Pebble sells deidentified insights to a gambling platform. These insights contain summaries of spending patterns and amounts outlaid on betting platforms for service users with Cal's demographic and usage profile. Based on this insight, the gambling service begins to target existing customers who match this profile - including Cal - with new offers designed to increase their share of those customers overall spend on gambling platforms. This is allowable as there is no prohibition on companies outside the CDR ecosystem undertaking direct marketing based on insights they have purchased.

Meanwhile, Pebble begins making direct marketing offers to Cal for personal loan products where they have relationships with the vendor (and take a fee for referral conversions). They justify this direct marketing on the basis that a personal loan will be better for Cal, budget wise, than cash advances with a high interest rate.

Cal takes out a personal loan but also increases his spend on online gambling as he takes up offers that the gambling platform which purchased insights from Pebble sends him. The loan is soon exhausted, and Cal finds himself with more debt than he started out with.

Factors influencing Cal's vulnerability:

Personal and circumstantial

- Addictive behaviour – although Cal doesn't consider his gambling to be a problem, it is habitual, increasing in frequency/severity, and impacting on his financial wellbeing.
- Emotional fragility – recently split from long term partner.
- Loss of support network – since breaking up with his partner Cal is no longer in contact with many of their shared friends. Working long hours, he has also found it difficult to schedule time with other friends, many of whom have young families.
- Cognitive load, stress, & lack of sleep – adjusting to the absence of a loved one, working long hours under stress, late night gambling, functioning on sub-optimal sleep hours.

Market

- Information asymmetry – Cal is not aware of the two-way commercial agreements in place between Pebble and the betting app. Nor does he know that Pebble receives financial incentives from loan vendors whose services they are recommending to Pebble users.
- Sludge – Pebble's Terms of Service and Privacy Policy are long and confusing to read, with important information about how insight data may be used and on sold by Pebble obscured by jargon and appearing towards the end of the lengthy documents. Even if he had read these documents, Cal may not have been clear about how his CDR data and other data relating to his use of the Pebble app could be used alone and in combination.
- Targeting vulnerability – Pebble uses tracking data from cookies on their website to place individually targeted advertising on gambling platforms. They do this because they believe customers of these platforms will be more likely to be in financial difficulty and receptive to using a 'free' budgeting tool, and the loan products they generate income from referring.
- Conflict of interest – Pebble is nominally providing services to Cal to improve his financial health, but they are also selling insights from his data to companies that are exacerbating his financial problems.



Where can CDR have positive impact for Cal's vulnerability?

Personal/circumstantial factors

- Pebble could offer a service to highlight to Cal if his gambling spend is increasing and foreshadowing where he is likely to miss his budget targets. Cal could opt in and elect the frequency of alerts regarding missed targets. Multiple alerts might trigger an internal signal for Pebble to initiate an in-person conversation.
- A write-access CDR might further allow Cal to set spending limits or deferrals for certain transaction types or payees.

Market factors

- CDR Data Standards supporting effective design of consumer dashboards and consent management will help consumers like Cal understand how their CDR data is being used, even if the terms of service may not make this clear up front. CDR requires consent to be express and informed (and able to be easily withdrawn), however determinations on the extent of information provided are affected by questions of cognitive load, as noted below. Opportunities for data standards to support dashboards and consent management are outlined in feature boxes on pages 23 and 27 of this report.
- CDR Rules could require ADRs provide greater transparency for consumers regarding arrangements or monetary benefits to that ADR flowing from disclosure of CDR data or insights. We note that this issue is raised in Update 2 to the CDR Privacy Impact Assessment, in relation to direct marketing and noted in the ACCC Response, without being endorsed; on the grounds that "cognitive overload could result if a consumer must be presented with such information prior to giving a Use Consent or a Disclosure Consent". We emphasise that stakeholders have told us this information is relevant and important to meaningful consumer consent, and we encourage further CX research into how standards and guidelines might assist with associated cognitive load being mitigated through design.

Scenario: Ngarie

Ngarie is in her twenties, early in her working life but with a stable income.

She has been living in a share house for the past two years, with the housemates all individually named on the lease and each paying their share of the rent via separate direct deposit payments into the trust account nominated by the real estate agent. There have been no disputes with the landlord or problems among the flatmates during the tenancy. However, over time everyone's circumstances have changed, and they've now agreed it's time to move on.

Ngarie prides herself on being independent and responsible with her money. She has decided she'd like to live on her own and is seeking a suitable residential rental.

Ngarie has found an apartment within her price range that she likes and is ready to lodge her rental tenancy application. The property manager informs Ngarie that to complete the process the agency has a policy of confirming rental payment history using 'Verity', a trust scoring service. Ngarie is told that if she wants to apply for this property, she will have to abide by this requirement.

Ngarie isn't 100% comfortable with this, but she really likes the property, so she provides a CDR consent to Verity for a one-off collection, use, and insight disclosure of CDR data from the transaction account from which her rent was paid by direct debit.

The next day, Ngarie's tenancy application is rejected. She doesn't know if this is because of the insight provided by Verity to the real estate agent, or for another reason.

She remembers that her rent was late one month when her pay was unexpectedly delayed due to IT issues with her employer's payroll – Ngarie asks the property manager if this is the issue, and explains it was a one off. However, the property manager won't provide any further details about Ngarie's application being rejected, and simply says another tenant has been accepted.

Next, Ngarie contacts Verity, but they say they are not obliged to tell her exactly what the insight contained. They emphasise that their customer is the agent, not Ngarie.

Ngarie is left feeling anxious about her ability to secure housing and unclear about what will happen if she applies for another rental property listed by the same agency, or with another real estate agent who uses Verity.

Factors influencing Ngarie's vulnerability:

Personal and circumstantial

- Aboriginality – Ngarie has experienced racial discrimination when seeking housing in the past. Lived experience of discrimination feeds her anxiety over why her rental application was rejected, and her uncertainty about what will happen if she applies for another property with this agency.
- Age – despite having good references from her past and current tenancies, Ngarie's youth means she has a limited rental history, and none as a sole tenant.
- Housing stress – Ngarie and her housemates have provided notice to vacate; she knows she has options at this point, but is anxious about the prospect of homelessness if she is unable to secure a lease on another property.

Market

- Information asymmetry – proposed CDR Rules changes require Ngarie to be informed when a CDR insight disclosure is made, but not what it contains.
- Power asymmetry – Ngarie *needs* housing and *wants* this property – she is in a poor negotiating position in relation to challenging the real estate agent as to whether this CDR demand is a reasonable requirement, or if alternative options might exist. Arguably this compromises her CDR consent to Verity.
- Accountability – as there is no suggestion that Verity has mishandled Ngarie's data, or acted outside the CDR Rules, CDR complaint mechanisms are not open to Ngarie. She has no right to know what insight was disclosed based on her data and no grounds to challenge the process or outcome through CDR mechanisms.
- Housing stress – low levels of affordable rental stock.



Where can CDR have positive impact for Ngarie's vulnerability?

Personal/circumstantial factors

- If insight disclosure is introduced into the scheme, we suggest vulnerable consumers will benefit from CDR Rules that require ADRs to provide consumers with a copy of any insights that are disclosed to other ADRs or to unaccredited third parties. In Ngarie's scenario, knowing what information or derived opinion about her consumer data has been disclosed might alleviate her anxiety, increase her willingness to share data with Verity again (or with other CDR participants), and would allow her to challenge data or insights which are inaccurate.

Market factors

- Opportunity for CDR to help reduce information asymmetry (as noted above). This could be further enhanced if, in addition to insights themselves, consumers were able to obtain a human understandable explanation of how such insights have been derived.
- Opportunity for CDR to improve accountability so that participants supplying CDR insights to others are required to provide regulators with an Algorithmic Impact Assessment, including a human understandable explanation of how their insights are derived (distinct from the technical algorithm or other commercial IP).
- Opportunity for CDR data standards for consumer dashboards to facilitate positive consumer experience and, in this scenario giving Ngarie the ability to monitor what information her 'insight disclosure consent' has allowed to be released, and to whom that data/insight has flowed. As part of creating this chain of consent, technical standards that require consent authority be embedded as part of metadata to CDR datasets may provide an avenue for more effective management and oversight of consent for consumers, participants, and regulators.

Scenario: Sami

Sami is a member of the LGBTQI+ community, who has recently been made redundant from their job. Due to this change in employment circumstances, Sami is reviewing his financial commitments and is potentially looking to switch providers for a range of products and services, including health insurance.

Sami is pretty sure there are better deals out there than his current health plan. However, so far, Sami has been hesitant to switch – partly because of concerns that changing provider may affect his ability to access specialist services or limit choice of health care providers. Although assigned female at birth, Sami has identified as male since his early twenties. He has transitioned socially, and medically through hormone therapy, with no current plans for surgical transition.

Sami currently has a supportive health network in place but has experienced being misgendered when dealing with health services in the past, which left him feeling stressed, humiliated, and angry. Sami is experiencing anxiety about the potential need to establish a relationship with a new gynecologist should he have to relocate for a new job. He is dreading having to explain all this personal context multiple times to different insurance companies when seeking quotes and product information.

A friend recommends that Sami open an account with Linx – an online provider that specialises in ‘lifestyle concierge’ services for the LGBTQI+ community, facilitated by use of CDR data. The company has gender diverse founders and markets itself as having an authentic understanding of the experiences and needs of LGBTQI+ consumers.

Sami reviews Linx’s website and privacy policies and is satisfied by their assurances that his health information, financial data and other personal information won’t be shared without his knowledge and express permission.

Linx collects information from Sami through an online questionnaire and through his consent to share CDR data. Importantly for Sami’s peace of mind, Linx supplies a call centre number on their website, and he can speak to a real person who is able to answer specific questions about how Sami’s data and personal information will be disclosed.

Within days of signing up with Linx, Sami switches to a new health insurance plan that offers additional benefits relevant to his specific needs. Happy with the result, he extends use of Linx to a broader range of products.

Factors influencing Sami's vulnerability:

Personal and circumstantial

- Financial stress due to unexpected redundancy and uncertain employment future.
- Being transgender – anxiety and marginalisation arising from ongoing exposure to experiences of discrimination, abuse, and disrespect from people who are deliberately or unwittingly transphobic.
- Ongoing specialist health needs.

Market

- Product offerings – mainstream health and insurance services lacking understanding in relation to specific issues faced by transgender consumers.
- Training and procedures - frontline staff acting in discriminatory or offensive ways.
- Information systems – forms and databases that do not accommodate non-binary gender data by design, and handle it inconsistently (eg, notes field) – information may be overlooked; or, conversely, present higher chance of privacy breach.



Where can CDR have positive impact for Sami's vulnerability?

Personal and circumstantial factors

- Being able to negotiate multiple services through a company that specifically represents Sami's community and has similar lived experience means he can speak safely, provide sensitive information once only, and is not being made more vulnerable by having to deflect cisheteronormative assumptions.

Market factors

- We suggest CDR require ADRs to provide contact details (not just contact forms) on their website. Being able to speak to a person if something is unclear, or if something goes wrong, builds consumer trust and reassurance. It also contributes to a culture of consumer safety and CDR compliance by requiring ADRs to have sufficient understanding of CDR obligations to be able to answer customer questions.
- Existing CDR Rules for data sharing provide a strong baseline for privacy and data security. This could be further enhanced by embedding consent data as metadata to CDR datasets.
- CDR drives personalised services and can lead to better choices being available for consumers – in this case health insurance services that are designed with an awareness of Sami's circumstances, rather than treating them as exceptional.

The flipside of this last point (ie, where CDR might exacerbate vulnerability) is if there are vulnerable consumer cohorts for whom niche services do not arise naturally from market competition. These people may be further disadvantaged by widening gaps in the market. Measuring consumer outcomes of CDR should include monitoring pricing spread resulting from CDR-enabled product switching, to determine the extent to which CDR results in firms competing for the most 'attractive' consumers, with higher cost products left to 'higher risk' consumers.

Case study: Carol

Carol and Rod were both born overseas, where they met and lived together for some years before marrying and immigrating to Australia. They have two adult children. Carol completed high school and obtained an industry qualification. She now works part-time. Rod is university educated, has a professional qualification, and works in highly remunerated employment. Carol and Rod separated more than a decade ago; however, they remain legally married. Rod has never accepted the marriage is over.

Carol describes their long relationship as turbulent and dysfunctional. Rod's controlling behaviours began in the early years and escalated after they arrived in Australia with their infant first child. Existing financially controlling and socially isolating behaviours continued, and Rod became physically violent towards Carol over many years.

Carol tried to leave on four occasions before their final separation. She returned each time because she struggled to care for the children alone, did not have adequate independent financial resources, and Rod would regularly find where she was staying. Eventually, Rod's behaviour became so terrifying that she believed he would harm the children and was likely to kill her. Following police advice, she initiated proceedings for a protection order against Rod.

Rod had on many occasions promised to financially cripple Carol. On the day that the first protection order was granted – which from Carol's perspective marks their final separation – Rod withdrew hundreds of thousands of dollars from various joint accounts, including a line of credit never previously used, and sent the money to overseas bank accounts that Carol had no knowledge of. Carol does not recall signing any documentation for the joint line of credit and was distraught that the bank would allow it to be drawn down without her authorisation.

Over the years Rod has continued to stalk and harass Carol. He has been charged and convicted on five occasions for breaches of protection orders. He has received a fine each time, which Carol believes has no deterrent effect due to Rod's significant income. Carol feels that Rod is becoming more dangerous and lives with the fear he will one day kill her.

Carol's financial resources are limited. She earns a modest income and has no assets of significant value other than the house she resides in and owns jointly with Rod. Carol has for decades serviced the original debt on the property; she feels she can manage this with her earnings. Rod further mortgaged the property some years ago and he continues to service that liability. Carol's preference is to divorce Rod, but this would require a property settlement. Carol knows equity in the home will largely be exhausted in paying the more recent debt that was accrued by Rod but is held in their joint names.

Factors influencing Carol's vulnerability:

Personal and circumstantial

- Domestic violence – longstanding physical, emotional, and financial abuse.
- Trauma – psychological impacts of DV experience.
- Financial constraints – no independent assets; part-time employment.
- First generation immigrant – distance from extended family support networks.
- Lack of trust in official systems – police, legal and financial systems have all failed to protect Carol in various ways, eroding her trust over time.

Market

- Procedures and training - at the time of Carol and Rod's separation, the bank does not seem to have been aware of the domestic violence situation, making it easy for Rod to inflict financial abuse.
- Questionable approach to responsible lending - more recently, Rod's ability to obtain a second mortgage on the property has further compromised Carol's financial security at a point in time when an extensive legal record of breached protection orders exists to substantiate the threatening and coercive nature of the relationship.



What effects does CDR have for Carol's vulnerability?

Carol's case study (as published by the University of Queensland)* has a legal service focus and does not indicate whether Carol accessed financial counselling advice at any point via domestic violence support services or other channels.

In a similar scenario, CDR might assist community workers to better support consumers like Carol with fuller knowledge of financial products held jointly in their name, more timely access to their data, and clarity over potential pathways to financial independence.

CDR's proposed 'Trusted Advisor disclosure consent' is the most likely channel through which this will be facilitated through CDR frameworks. As our discussion of the strengths and weaknesses of Data for Good initiatives (pages 21-22) makes clear, to do so effectively requires more than making data disclosure possible – the capacity of services to use this data in ways that can help realise effective service provision is critical for success.

Dedicated investment and incentives for non-profit and community sector to steer or lead collaborative projects with technology companies will be necessary to develop platforms and services that enable CDR data to be accessed by 'Trusted Advisors' in the community sector through platforms that are secure, interoperable with familiar tools and software, and which are addressing demonstrable needs of vulnerable consumers. If CDR innovation funds are geared only towards commercial sector, it is unlikely that such investment will result in new digital products and services that are designed primarily to improve consumer welfare and wellbeing, without commercial motive.

* Online at: <https://law.uq.edu.au/research/dv/using-law-leaving-domestic-violence/case-studies>



Part 3: Toolbox

“We are seeing businesses that rely on both measures – using human observations or ‘small’ data to recognise trends, then drawing on the power of AI and big data analysis to detect or address the scale of problems.”

- Participant at CPRC Roundtable, November 2020

Rights by design

A rights by design approach is one which commits to designing tools, technologies, and services to respect rights by default; to apprehend and counter potential design vulnerabilities that would permit abuse or exploitation of a person's rights³⁰.

Rights by design extends on more well-established principles-led design approaches, such as privacy by design³¹, requirements for which are increasingly becoming the norm as part of data reforms in jurisdictions around the world³². It is not difficult to imagine rights by design approaches to market services becoming similarly necessary for obtaining social license as the digital economy expands to constitute an ever-increasing slice of consumer interactions.

Recognising vulnerability by design

Design vulnerabilities are a familiar concept for software engineers and info security experts: legitimate functions or features of a system or network with unintended consequences that can be deliberately exploited by an attacker to manipulate the system to their own ends.

Design vulnerabilities which are based in technical features can also transcend the technical domain. Legitimate functions of a technical system can be similarly exploited in ways that exacerbate vulnerabilities of people interacting with those systems (such as one-time-passwords being manipulated where a perpetrator in an abusive or controlling relationship is mediating access to the account holder's mobile phone).

As well, poorly designed technical systems and information technology can generate vulnerability by default for certain user groups – as with many documented examples where AI and machine learning have produced algorithms that entrench existing bias, marginalisation, and vulnerability³³. More specifically, *vulnerability by design* arises where the cultivation of consumer vulnerability becomes a deliberate design choice, rather than an unintended consequence.

For CDR, this has impacts at both system and product level. Regulators need to be alert to CDR products and services which may seek to exploit the vulnerabilities of markets and consumers; and policymakers need to be cognisant of whether CDR Rules and Standards discourage such design practices or create environments in which they flourish.



Opportunity: Algorithmic Impact Assessments³⁴

Algorithmic Impact Assessments (AIAs) are one tool that can help mitigate against vulnerability by design, and which may be a useful addition to CDR's regulatory toolbox.

AIAs evaluate the potential detrimental effects of an algorithm in the same manner as environmental, privacy, data, or human rights impact statements, to ensure that AI vendors and their customers have assessed and understood the social implications of their technologies before they are rolled out to be used by the public.

These assessments may be open to regulatory review or be required to be published so that the public can read or comment on them.

Data for good

Broadly speaking, the 'data for good' (D4G) movement is established on the notion of bringing data science to bear on social problems. It covers a wide range of projects from citizen science initiatives, hackathons, and service delivery or evaluation tools, through to technical capacity building to seed sustainable data programs in under resourced organisations or communities.

While the aims of D4G are altruistic, in practice such projects are not always collaborative with the communities they are intended to serve, or sufficiently respectful of the lived experience of those whose 'problems' are the focus of the initiatives (including the problems of community organisations). For example, D4G initiatives that provide hardware, licenses, and computational resources at a heavily subsidized rate, or for free, have been criticized for being "well intentioned [but] tone deaf," to the reality that the more common pain point faced by non-profits is often not software but technical training³⁵.

As well, human centred research and data for good initiatives seeking to collaborate may encounter difficulty recruiting community participants or suffer a loss of goodwill over time where marginalised populations are repeatedly approached to rehearse their experience or 'perform' as subjects of extractive research³⁶. This will figure as a real issue, both ethical and logistical, when seeking to actively involve vulnerable communities in articulating data for good problems and solutions using CDR. Engaging community sector organisations who have relationships and protocol in place for working with vulnerable cohorts in shaping any D4G agenda for CDR is a key strategy to mitigate this.

In their various roles of service providers, advocates, and practitioner-researchers, individuals situated in community sector organisations often hold nuanced contextual knowledge about how data sharing currently affects people experiencing vulnerability. As well, these professionals operate with the trust of vulnerable consumers (who may not want to directly engage with government consultation; or may not be able to conform with the processes of such engagement) and can facilitate consumer experiences being safely and impactfully shared. However, this type of activity comes at a cost to community organisations, potentially drawing resources away from provision of services. In asking for their sustained engagement there must be not just hypothetical 'benefit' but benefit that clearly aligns with the agenda, impact, and resources of these organisations.

Involving community services in early-stage knowledge transfer and ongoing skills training can ensure D4G designers are supported to work with an informed understanding of who they are designing for and the realities of those consumer experiences – to see the user journey in the full context of people's lives, and from the perspective of worldviews other than their own. This is necessary groundwork to minimise potential for harm or misunderstanding in projects that are not necessarily community-led, but which are committed to accord with the ethos emphasised by many minority and marginalised communities: *nothing about us without us*.

“As someone who works at a large non-profit in data analytics...

We've had multiple conversations with 'data for good' orgs where we felt like it was either going to be more work on our side for something that wasn't actually what we needed, or else it was too 'boring' for it to be an interesting problem for them.

I have found technology change management and certainly capacity within the organization to leverage technology well have been the biggest challenges.”

Online comment on challenges of 'data for good' projects³⁷

Common criteria used to classify a project as Data for Good³⁸

Non-profit or government agency is recipient of data product.



Volunteers produce the data product for a subsidized rate (often free).



Tools for data work are donated or heavily subsidized.



Educational programs to build technical capacity in underserved communities.



Opportunity: Data for good and disclosure to “trusted advisors”

If proposed CDR rules allowing for disclosure of CDR consumer data to trusted advisors were to be introduced in the future* (“TA disclosure consents”); analytics tools might be developed that facilitate financial counsellors and other non-profits to interpret consumer data more consistently, to determine whether pathways or services are having the desired effects, individually and at scale.

For example:

- did a consumer apply for a product or service to which they were referred?
- did they get that service?
- did the realised benefits match what was promised?
- how long did they continue that service?
- what consumer choices follow on exiting a remedial or transitional service?

As well as benefits of such tools, potential risks were also raised by groups who might use them:

- Disclosure of CDR data to trusted advisors places those datasets outside CDR protections and (potentially) within systems that are more susceptible to privacy breaches and data leakage.
- Victim-survivors of family violence or financial abuse may be exposed to additional harm if they do not have visibility over who has access to their CDR data (as would be the case once it leaves the CDR eco-system through disclosure to a trusted advisor.
- Placing CDR data outside the ecosystem also means consumers would be giving up the right to deletion of CDR data.
- Gaps in internal capability to develop analytics solutions, training capacity to use new products effectively, or financial resources to acquire them.
- Proposed rules changes require TA disclosure to be mediated through an ADR (ie, CDR will not enable a consumer to direct a DH to share directly with TA) and would allow ADRs to charge for the service. Such costs may put this functionality beyond the reach of non-profits unless exemptions created for vulnerable consumers.

() We note that proposed amendments relating to rules for TA disclosure consents and the sharing of data with trusted advisors (as outlined in the ACCC’s September 2020 CDR Rules expansion amendments consultation) were not accepted and have been deferred at this time.*



Opportunity: Data standards for CDR consumer dashboards

The economy-wide scope of CDR assumes consumers will gain sufficient familiarity with CDR consent concepts and processes to act with confidence and self-efficacy when engaging with disparate CDR data holders and accredited data recipients across services and sectors. High expectations are being placed on consumers to learn and effectively interpret CDR conventions. For these to be realistic, there is a dependency on the quality of consumer dashboards as the primary channel for consumers to exercise ongoing consent management.

- Data Holders and Accredited Data Recipients are required to provide consumer dashboards, but there are currently no common standards for how these should be implemented that might warrant.
- To navigate the scheme safely, and build up capability in how to take appropriate actions to reflect their intentions, consumers need to be able to trust that CDR dashboards, while not identical, will represent and facilitate consent management in a comparable manner.
- Consistency in the terminology and protocol surrounding available dashboard actions, and in-app notifications of what such actions (and associated consent status) entail in practice, is likely to improve consumer engagement and aptitude with CDR processes. This can be supported through relevant data standards and CX guidelines.
- Rather than deeply prescriptive instructions for how dashboards must function, we suggest a combination of mandatory and voluntary guidance with regard to clarity of information, accessibility in design, and consistency of approach across sectors and providers.
- A dictionary of CDR consent terms (as recommended by the Farrell CDR Future Directions Report)³⁹ will help align business and regulatory understandings of rights and responsibilities, especially where commonly understood terminology in relation to datasets or consent might otherwise differ between sectors. Based on the examples provided in the Farrell report, we suggest that further work will be needed to align such definitions to be consumer friendly. Development of this resource should be substantially informed by consumer representatives with specific knowledge of inclusion, diversity and vulnerability, as well as by industry.

Applying existing vulnerability frameworks

A key issue raised by many community sector stakeholders in our consultations is that streamlining out points of human contact in the process of consumer decision making and consent for data sharing, risks inhibiting groundwork where vulnerability frameworks and strategies are beginning to be incorporated in practice⁴⁰. This issue has also been recognised by the Data Standards Body, who, by way of mitigation, have recommended providing in-flow instruction to consumers to better facilitate safe and informed authorisations and create pathways for account holders wishing to self-disclose vulnerability or financial abuse⁴¹.

Stakeholders pointed to further possibilities for integrating humans in the loop, using consumer data to recognise the sorts of behaviours or vulnerabilities that might otherwise be picked up in interpersonal settings. Specifically, several spoke positively regarding the work of major banks to identify and act on situations where perpetrators of abuse are manipulating small value online transactions to send abusive or threatening messages⁴².

A key challenge in aligning CDR with best practice for vulnerable consumers is enabling data innovation to flourish in ways that allow digital interactions to work in accord with, or directly support, human interactions or interventions, such as the frameworks described on the following page, which are widely used in client-facing service provision⁴³.

Interpersonal communication frameworks designed for engaging with vulnerable consumers may not, at first glance, translate readily to technical standards or protocol for online data sharing, however we believe these approaches have application for CDR, as outlined further on the next page.

These are important opportunities to address risks where CDR offerings may not otherwise establish safety and inclusion for vulnerable consumers. Guidance will be particularly important for smaller businesses who may be less advanced on the journey to operationalising vulnerability frameworks, or who in outsourcing support functions such as CDR consumer dashboards may make choices that do not support best practice for accessibility or vulnerability.

IDEA

Talking to a client about their vulnerability.



- **Impact:** what are they finding hard? "What has the impact been on your personal and financial situation?"
- **Duration:** how long has the client been living with the vulnerability? "So when did this first start to happen?"
- **Experiences:** how is the client experiencing this vulnerability? Is it something that fluctuates? "Have you experienced this before?"
- **Assistance:** "Is there anything else we should know about any support, treatment or care you're receiving? It could help us to support you better."

www.wiseradviser.org/vulnerability

TEXAS

When your client tells you about themselves.



- **Thank them:** "Thanks for telling me, it will help us advise you better."
- **Explain:** "We'll use information you share to tailor the advice. We'd like to make notes in our database so we can look at them next time we advise you. We won't share your information with anyone outside our organisation."
- **eXplicit consent:** "Are you happy to give me permission to note down and save the information you've shared with me today?"
- **Ask:** "Does your situation make it harder for you to manage your money or communicate with us? Do you have any help, for example from a relative?"
- **Signpost:** refer to the most appropriate internal or external help.

www.wiseradviser.org/vulnerability

SPIDER

Advise bad news and actions clearly with minimal distress.



- **Set the scene:** "Thanks for getting in touch. It's important we talk about..."
- **Perspective:** "I want to understand your perspective. How are you feeling and what options are you considering?"
- **Invitation:** invite questions. "Are you able to talk this through today?" Do they need the info in a different format or to talk another time?"
- **Deliver:** use simple, bite-sized, jargon-free language. Allow it to 'sink in'. "I'm sorry, this news might be disappointing. I'll explain and we'll talk options..."
- **Empathise:** listen carefully with empathy, giving space for them to express feelings.
- **Recap:** summarise and recap to check understanding. Are they ready to make a new decision or take action? If not, rearrange and offer lots of reassurance.

www.wiseradviser.org/vulnerability

BRUCE

For clients experiencing a mental capacity limitation.



- **Behaviour:** look for clues of a limitation in the client's behaviour and speech.
- **Remembering:** if they are struggling to remember the repeat advice. Ask what might help, write it down or see if someone can help them.
- **Understanding:** ask them to summarise their understanding. Fill any gaps by repeating advice or using different explanations by simplifying or rephrasing.
- **Communication:** how would they prefer to communicate? Try to accommodate this. Allow enough time and pause regularly.
- **Evaluation:** (or weighing-up) – discuss each option simply, writing down any pros and cons. Does anyone usually support them?

www.wiseradviser.org/vulnerability



Opportunity: Integrating vulnerability frameworks

Interpersonal communication frameworks designed for engaging with vulnerable consumers may not, at first glance, translate readily to technical standards or protocol for online data sharing, however we believe they can have application for CDR. We encourage DSB and others to seek innovation in integrating these frameworks to online interactions and data driven contexts. For example:

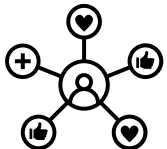
- To inform the development of RegTech (regulatory technology) offerings that can help detect potential breaches of mandatory disclosure requirements in CDR financial service offerings and, across all sectors, identification of more subjective examples of poor disclosure, such as potentially misleading or deceptive conduct ⁴⁴.
- Where businesses such as banks or energy retailers employ call centre staff to promote in-house or white labelled CDR products and services, such frameworks may assist in early identification of vulnerability and/or prevent pressure marketing being applied to consumers who do not feel confident to engage with CDR.
- Where chatbots are the first point of contact or consumer 'help' medium for a CDR app or service, guidelines that encourage design conformance of language processing AI with these frameworks could help ADRs identify and triage vulnerable consumers to ensure they receive appropriate levels of support.
- Where elements of these approaches can be integrated into CDR's data standards – for example 'Communication' (BRUCE) might support requirements for CDR services to provide alternative communication channels; and 'Signpost' (TEXAS) might inform guidelines whereby, if vulnerability is indicated during a consumer enquiry or consent flow then consumers have options to exit from CDR process with relevant support (for relevant DSB noting paper, see note 41).
- And, in the development of guidelines or standards relating to the design and consumer experience of CDR consumer dashboards.



Part 4: Approaches

“If CDR enables [data recipients providing a consumer service] to have a more data rich picture of someone then they can much more easily detect where someone is vulnerable and may need other assistance, like hardship assistance, or referrals to other supports ... and there’s opportunity to detect things like financial abuse or elder abuse at a much earlier stage and prevent harm down the track.”

- Participant at CPRC consultation session, August 2020



CDR reforms should respond to consumer vulnerability as a positive opportunity to strengthen systems, build resilience, and grow trust.

What are we aiming for?

An efficient CDR – one that encourages competition and data innovation in areas that matter to consumers and which lead to improvements in their wellbeing.

Consumer trust in markets will facilitate economic recovery in the aftermath of COVID19. Appropriate responses to vulnerability will have positive impacts on economic growth and recovery as well as the long-term sustainability of CDR.

What does this require?

- CDR participants seeking to make use of consumer data are compelled to compete on issues beyond cost and convenience.
- CDR reforms encourage innovation in data sharing processes and data enabled services that lead to measurably fairer and more inclusive markets: giving consumers choices that allow them to easily implement their intentions regarding consent, privacy, accessibility, and responsiveness to change (including situations of hardship).

“No one needs to trade away the rights of their users to deliver a great product.

[...]

If a business is built on misleading users, on data exploitation, on choices that are no choices at all, then it does not deserve our praise. It deserves reform.”

- Tim Cook, Apple CEO⁴⁵

What will help us get there?

- Integrating CDR into wider regulatory vulnerability strategies as they are developed across sectors (for example, referencing CDR in relevant industry codes such as the Banking Code of Practice and BNPL Code of Conduct).
- Active and involved regulators and clear complaints mechanisms that consumers can easily identify and access, including a digital or data Ombudsman for identification and action on systemic issues.
- Demonstrated understanding of consumer vulnerability by CDR participants – for example requiring vulnerability policies or algorithmic impact assessments as part of CDR accreditation.
- Vulnerability Impact Assessments for significant changes to CDR Rules.
- Articulating quality indicators for privacy and consent that measure consumer needs and expectations as well as technical compliance, to support collection of CX metrics and evaluation of consumer outcomes of CDR (including understanding and limiting scope for data leakage).



CDR services should provide people with agency to achieve ambitions, and respond to crises, as well as to manage their everyday consumer experience.

What are we aiming for?

An effective CDR – capable of supporting positive outcomes for all consumers, including during times of acute vulnerability, and for those who live with pervasive vulnerabilities.

What does this require?

- CDR products and services are comprehensible and responsive to people's circumstances, with use cases that address a wide range of consumer needs and capabilities.
- CDR apps and platforms are easy to understand and navigate when making, reviewing, amending, or withdrawing CDR consents.
- Consumers can obtain meaningful help when they need it, including through businesses proactively identifying and offering support to at-risk consumers.
- No surprises for consumers – outcomes of using a service align with promises and expectations.



Opportunity: Consent management

One Roundtable group of community sector stakeholders drew an analogy with parcel tracking: proposing an opportunity for consumer dashboards to represent the data journeys effected by active consents, so that consumers can clearly see and understand where their data is and who has access to it through real time.

We recognise that under current system requirements data holders and ADRs would have differing capacity to show this, indicating a potential need for further data standards requiring ADRs to communicate back to data holders on consent status and associated data usage.

Alternatively, realising this concept might support daisy-chaining consents in a way that is traceable and detailed (and could build on the current record keeping requirements that consumers can access). The chain of consent would then become a resource in its own right - equivalent to a dataset - that could be transferred to a centralised dashboard (of the consumer's choice) with read and action-initiation capabilities. This could provide an avenue for more effective management and oversight of consent (benefiting consumers, participants, and regulators), including better prospects for a 'bulk-withdrawal' mechanism.

What will help us get there?

- A consumer data charter as an industry-agnostic goodwill document setting out public expectations and key consumer rights in data sharing⁴⁶.
- Consumer dashboards reflect consistency and clarity of information and available actions, supported through relevant data standards and CX guidelines.
- Requiring all CDR participants to provide simple ('one-touch') mechanisms for consumers to effect bulk withdrawal of consent as a failsafe mechanism.
- Decision support tools, designed with community and consumer experts to ensure a range of tailored information, meaningful for culturally, linguistically, and cognitively diverse consumers.
- Explicit investment in non-profit data for good initiatives to be led by community organisations, support innovation of CDR-enabled services in the consumer interest.



CDR should not increase consumer vulnerability. No one should be put in a position where use of CDR products causes them significant harm or compromises their access to essential services.

What are we aiming for?

A safe CDR – does not replicate market conditions where harmful or exploitative behaviours are demonstrated to flourish.

Using CDR services should not put consumers in a position where they bear additional or disproportionate risks because of vulnerability.

What does this require?

- Accredited Data Recipients take on a proportionate share of risk/responsibility for how their service impacts on vulnerable consumers' lives and wellbeing.
- Line of sight beyond the 'advertised' parameters of a transaction.

“There are a range of data points that can prejudice the products and prices people are offered.

Demographic data, hardship provisions, late or missed payments, default payment plans – how that information is shared could be problematic.”

Participant, CPRC Roundtable, November 2020

What will help us get there?

- Responsible market stewardship and monitoring of outcomes; trialling algorithmic impact assessments (for CDR participants) and vulnerability impact assessments (for CDR rule makers)
- Embedded markers in datasets to maintain consent information as metadata and facilitate the source of breach being more readily/rapidly identified in the event of data leakage or mishandling. In the case of disclosure of CDR data to third parties, if a 'Trusted Advisor' or accredited party is responsible for repeated breaches; their status should be revoked⁴⁷.
- In the case of disclosure of CDR data or insights by accredited persons in receipt of CDR consumer data, any financial benefit being obtained by the ADR should be made clear to consumers at the time of request. To give effect to this, CDR data standards could require disclosure consent include a statement explaining that where a consumer provides a disclosure consent in order to receive x service or y benefit, the ADR will be paid by that external party (making explicit where a third party will be the ADR's customer for a consumer's data or derived insights).
- Product and price monitoring in CDR-designated markets to ensure policymakers understand distributional impacts of the scheme regarding pricing and access to products or services across the customer base and have sound evidence demonstrating whether vulnerable cohorts are benefiting from CDR.



CDR should not shut people out from market participation. No one should be unfairly denied the opportunity to obtain benefits from CDR data sharing, or the means to challenge the legitimacy of negative outcomes.

What are we aiming for?

A fair and inclusive CDR – ensuring the same rights can be exercised by consumers with diverse capabilities and circumstances.

What does this require?


- Recognition that consumers do not come to CDR from a level playing field.
- Recognition that a system which treats everyone as being equipped with the same set of capabilities and life advantages will disadvantage people who are experiencing vulnerability.
- Policy levers and practice guidance to recognise and mitigate exclusion and discrimination.

“For many people, life is complex enough already without adding more things that require them to engage in a certain way to get results.”

Participant, CPRC Roundtable, November 2020

What will help us get there?

- Rights by design and inclusive design approaches across different aspects of CDR (policy, information systems, and platforms/interfaces).
- Accountability in use of AI decision making and effective enforcement of human rights legislation to protect against discrimination⁴⁸.
- Where a product is not suitable for a consumer due to vulnerability, CDR providers can confidently and comprehensibly explain why this is the case, supporting a consumer right to know why they have received a particular outcome – such as being rejected for a loan, insurance product or energy deal.
- Requirement for consumer-facing CDR service providers to provide contact details (not just contact forms), and published service standards for responding to consumer requests for information.
- In the case of insight disclosure, a right for consumers to obtain insights disclosed and a human understandable explanation of how such insights have been derived.
- In the case of insight disclosure, a requirement for CDR participants supplying such insights to provide regulators with a human understandable explanation of how their insights are derived (distinct from the technical algorithm or other commercial IP).



Part 5: Opportunities

Opportunities to mitigate adverse impacts of CDR on consumer vulnerability

DSB action opportunity:

- **Iteration of data standards and/or CX guidelines specific to CDR consumer dashboards and consent management.**

Wider reform opportunities:

- **Integration of vulnerability principles into the work program of the Consumer Data Right.**
- **Development of clear aims, indicators, and measures for consumer outcomes of CDR, including measures that are specific to known or predicted areas of consumer vulnerability.**
- **Mechanisms to harmonise consumer experience of data standards across industry and legislative contexts**

DSB action opportunity:

Iteration of data standards and/or CX guidelines specific to CDR consumer dashboards and consent management.

Aim

Consumers can easily understand and navigate processes to provide and withdraw consent for data sharing; clearly comprehend what each consent means in terms of who has access to their data and the purposes for which it will be used; and are not surprised by outcomes of giving consent for CDR data sharing.

Purpose

CDR participants provide functional support tools (dashboards) that are suitable to facilitate consumers with diverse skills and abilities to clearly understand, manage, and withdraw the consents they provide to share their CDR data, and which support consumers to be able to effect actions that reflect their intentions regarding the validity of data sharing consent provided.

Consumers can expect consistency in the way the spectrum of CDR consent is described, interpreted, and managed across CDR services they might access from different providers and platforms and have recourse to agreed standards in the event of dispute over consent.

Rationale

Dashboards are the main instrument through which consumers will have access to ongoing visibility of their CDR consents. They must be secure, accessible, comprehensible, and easy to use by a wide range of people to be fit for purpose for consumers to exercise meaningful control over CDR consents.

This is of direct relevance to the large number of consumers whose experience of vulnerability includes barriers to use of technology (or who may be subject to financial abuse through manipulation of technology) because of factors such as English language proficiency, literacy levels, digital fluency, personal digital access, age, or difference in cognitive or physical ability.

Wider reform opportunity (A):

Integration of vulnerability principles into the work program of the Consumer Data Right

Aim

Recognise and embed the diverse experiences, needs and expectations of vulnerable consumers into design and implementation of CDR.

Purpose

At a systemic level, to strengthen consumer safeguards for consumers who experience vulnerability, so that CDR reforms promote consumer wellbeing and parity in access and outcomes of the scheme for vulnerable consumers.

Rationale

These four high-level principles are based on local knowledge of consumer data sharing practices and outcomes described to us by community sector organisations and consumer advocates.

As well, they reflect broader findings stemming from open banking and implementations and other consumer data reforms in international jurisdictions; including research and evaluation publications produced by the UK's Open Banking Implementation Entity⁴⁹ and by Europe's leading consumer organisation, BEUC⁵⁰.

Vulnerability principles for CDR:



CDR reforms should respond to consumer vulnerability as a positive opportunity to strengthen systems, build resilience, and grow trust.

CDR services should provide people with agency to achieve ambitions, and respond to crises, as well as to manage their everyday consumer experience.



CDR use should not increase consumer vulnerability. No one should be put in a position where choosing to use CDR products leads to significant harm or compromises their access to essential services.

CDR design should support consumers' market participation. No one should be unfairly denied opportunity to use CDR products and services, obtain benefits from CDR data sharing, or challenge the legitimacy of negative outcomes.



Wider reform opportunity (B):

Development of clear aims, indicators, and measures for consumer outcomes of CDR, including measures that are specific to known or predicted areas of consumer vulnerability.

Aim

Identifying qualitative criteria and quantitative metrics to measure levels of consumer success that can be captured through CDR reporting and other data sources.

Purpose

To better understand different aspects of consumer vulnerability as they relate to CDR, and provide an evidence base for evaluating effects of CDR on consumer vulnerability, and consumer outcomes more generally.

To demonstrate if and where CDR alleviates or exacerbates market-induced consumer vulnerability, and how the reform is contributing to reduction or increase in levels or impacts of consumer vulnerability.

Rationale

Consistent collection and analysis of data against consumer outcomes criteria that are considered appropriate by government and consumer stakeholders (determined and verified through consultation with community and consumer organisations) will clarify if and where additional standards are required to improve consumer outcomes of CDR, or to measure them in an effective and transparent manner.



Opportunity: Outcomes measurement

For example:

Measuring how consumer vulnerability is reduced

- Quantify numbers of consumers assisted by community workers through mediated use of open banking (service reporting by community organisations), or disclosures of CDR data to non-profit 'trusted advisers' such as financial counsellors or community legal centres (CDR reporting metrics).
- Track volume and results of specific use cases, such as micro-savings or budgeting apps targeted to low-income cohorts. Potential use of DH/ADR service data to gauge improved financial wellbeing over time.

Measuring how consumer vulnerability is increased

- Use of demographic data to test whether digitally excluded consumer cohorts share in benefits of CDR (or, don't get as much access to best discounts, pushing them further behind).
- Monitor price spread through evaluation of CDR-enabled switching data in essential service markets. (Do 'desirable' consumers get heavy discounts, while low income/high risk receive higher cost offers and products?)
- Analysis of CDR complaints data to monitor and quantify harms to consumers against different categories/causes (such as data leakage or abuse of CDR processes). Be alert to patterns of harm where a DH has vulnerability flags in place on an account (hardship; domestic and family violence; elder abuse).

Wider reform opportunity (C):

Mechanisms to harmonise consumer experience of data standards across industry and legislative contexts

Example 1 -

Establishment of a Data Ombudsman

Aim

Promote good governance, accountability and transparency over data sharing platforms and processes affecting Australian consumers of goods and services – including, but not limited to, CDR-enabled data sharing – through oversight of relevant government policy administration and service delivery.

Purpose

To cement public expectations for safe, fair, and inclusive data sharing; support regulators in establishing market stewardship for offerings under the CDR regime and other digital platforms; and provide perspective on consumer impacts of data sharing across government reforms.

For consumers experiencing vulnerability, to ensure fair processes and access to redress are available for people who may mistrust or struggle to navigate internal CDR complaints mechanisms as the scheme rolls out,⁵¹ or whose complaint applies more clearly to data sharing issues at systemic rather than process level.

Rationale

A Data Ombudsman could enhance how CDR consumer complaints contribute to improving broader data governance and policy matters; so that responses to complaints are (where applicable) looking beyond individual process failures to identify where systemic issues are leading to poor outcomes for consumers or widespread breaches of consumer rights. The functions of existing regulators to respond to these issues in the first instance would not be replaced. It may help to augment the functions of CDR regulators in relation to their capacity to perform broader data governance, so that fewer CDR issues need progress to a Data Ombudsman (this could also offer a performance indicator for the CDR).

“Ombudsmen contribute to improving accountability and good governance in three main ways ...

Firstly, we do resolve individual disputes. We investigate complaints, we safeguard citizens from government actions which could adversely affect them, and we give citizens a voice to complain [on matters] that affect everyday lives. **Because ombudsmen services are free, they are practically valuable to the most vulnerable.**

We investigate systemic problems... we might have one complaint made to us which we can see might well apply to many other thousands of people. So, we look at how we can fix problems through an Ombudsman investigation, not only in relation to the complaint that has been made to us, but also to help others who might have been adversely affected.

We contribute to improving public sector performance, and that works in two ways: directly, where the information from complaints about areas of poor service delivery is fed back to agencies; and indirectly, where the potential oversight of each decision by the Ombudsman is an incentive to public servants to improve the quality of their actions and decisions.

... Agencies should rightfully be the first to receive and deal with complaints. If the citizen is not satisfied, they can come to us. For this reason, we are very interested in agencies' complaint-handling systems. The better they work, the fewer disputes that come through to ombudsmen.”⁵²

Wider reform opportunity (C):

Mechanisms to harmonise consumer experience of data standards across industry and legislative contexts

Example 2 -

Development of a 'consumer data charter' as an industry-agnostic goodwill document setting out public expectations and key consumer rights in data sharing

Aim

A clear and concise document setting out a shared understanding of public expectations and consumer rights in data, and which formalises a goodwill relationship between stakeholder communities.

Purpose

As a mechanism to establish a basis for trust for consumers, in recognition of power and information asymmetries inherent in the way data is transacted between individuals and businesses or government.⁵³

Such a charter could be developed as part of regulatory guidance for CDR participants (for example, informed by existing CX principles; and/or with accredited persons becoming signatories to the charter), or it could be established under the wider remit of a data ombudsman and positioned to also address consumer expectations and rights in relation to government service data.

Rationale

Jurisdictions further along the open banking path, such as the UK, have already recognised the value of this type of goodwill document in pushing for "innovation in the way the market thinks about consumers ... [driving firms to] shape products around people, rather than expecting consumers to shape themselves around products".⁵⁴ A document of this kind, even if not legally binding, represents an important part of creating sustainable movement towards a data driven society that respects and protects the welfare of citizens by instituting public commitments to fair, safe, and ethical usage of consumer data.

Conclusion

The Consumer Data Right is in a unique position to establish Australia's consumer data economy as one which is characterised by fairness, safety, and inclusion. This means making honest assessments about what the scheme will and won't do to address the effects of digital exclusion, barriers to digital and data literacy, and other social or market-driven factors that contribute to vulnerability and impact on the ability of all consumers to benefit from CDR products and services.

Acknowledging the complexities of consumer vulnerability and recognising that direct impact on some vulnerability measures will remain beyond the remit of the reform should not prevent policymakers and regulators from asking challenging questions: if the desired market state is 'fair and inclusive' - what *is* in CDR's power to affect/effect and how will these outcomes be measured?⁵⁵ Although CDR cannot be expected to "fix" circumstantial or structural sources of consumer vulnerability; it does have a preventative role to play in limiting to the extent to which consumers using CDR will be exposed to vulnerability by design.

Articulating a sound consumer outcomes framework for CDR will help demonstrate government intent and accountability for the scheme, quantify the consumer impact of data innovation stemming from CDR reforms, and ultimately help grow consumer trust and capability. Used well, data analysis can be a tool to ensure that expectations are clear; that initiatives and services are relevant (whether targeted to vulnerable consumers specifically or addressing consumer vulnerability in mainstream products); that outcomes can be measured and communicated; and that vulnerability work is manageable and impactful.

Intangible assets such as reputation, intellectual property, and customer base now account for over 80% of total corporate value as compared to under 20% 40 years ago.⁵⁶ There is real impetus for industry to recognize consumer needs and public demands for fair and ethical business behaviour, and to cultivate positive customer experiences as part of sound business practice. This will be best supported by a Consumer Data Right that engages with the value of consumer data to businesses without limiting the rights of consumers to retain agency over how that value is extracted and refined, and the benefits they might gain from it. Challenging the ways in which we think about consumer vulnerability is a necessary part of establishing fair, safe and inclusive markets – and a fair, safe and inclusive Consumer Data Right.

Positioning CDR to improve the quality of competition and choice in Australian consumer markets requires both innovation and imagination; and demands that engineers of elegant solutions not lose sight of the messy human lives that unfurl behind tidy data points. We encourage policymakers to persist with consultation and policy design approaches that recognise consumers as the experts in their own lives, maintain the rights of consumers as a central tenet of the reform, and allow consumer experience to inform data standards and guidelines in providing markers to good practice.

Standards that drive data holders and data recipients to exercise a duty of care for consumers as a requirement of participation Consumer Data Right should be recognised and championed as helping to lift the innovation bar high enough to stimulate CDR products and data services that allow vulnerable consumers to exercise resilience and agency.⁵⁷ This is the pathway to the kinds of equitable, sustainable, and competitive outcomes that all Australians deserve from CDR.

“Data can be used for good to help identify areas of pressing need, prioritise regulators’ vulnerability work, and identify customers at risk of, or experiencing, vulnerability.

It can also be used by industry participants and others to develop innovative interventions and engagement with consumers experiencing vulnerability, and in better product and service design.

This should be coupled with qualitative inquiry into the nuances and real-life experiences of markets.”⁵⁸

Endnotes

- 1 CPRC (2020) *Data and Technology Consumer Survey: Consumer research conducted in partnership with Roy Morgan Research over March and April 2020*, p30 .
- 2 In complement to the Consumer Data Right's existing principles-based approach to consumer experience (demonstrated through articulation of defined CX principles as part of the CDR data standards), we have developed four key principles to guide CDR's approach to consumer vulnerability. These principles represent a high-level synthesis intended to encapsulate the diverse experiences, needs and expectations of vulnerable consumers. They are based on local knowledge of consumer data sharing practices and outcomes described to us by community sector organisations and consumer advocates; and on broader findings of the international community, including research and evaluation publications produced by the UK's Open Banking Implementation Entity and by Europe's leading consumer organisation, BEUC.
- 3 Acknowledging this, the UK's Financial Conduct Authority cautions against overworking definitional issues: "Vulnerability in consumer policy has been widely discussed and is recognised in legislation; however, definitions tend to vary widely [...] The characteristics of the individual, their circumstances, static and transitory states, and the practices of providers, all appear in these definitions in various ways. What is clear is that, however finely nuanced the definition of vulnerability is, the real challenge lies in how to operationalise it: how to embed it both in the culture of the regulator, and the practices of firms." (Financial Conduct Authority (February 2015) *Consumer Vulnerability – Occasional Paper No. 8*, p19).
- 4 Drawing on earlier CPRC work for on consumer vulnerability for the Australian Energy Regulator (AER), and our discussions with community sector and consumer advocates for this project, we suggest this definition as a useful starting point for creating a shared understanding of what is meant when talking about consumer vulnerability in relation to CDR. Appendix one of this report reproduces a table of definitions of consumer vulnerability used by regulators in Australia, the UK and by the OECD, as published in our report for the AER. As this review table shows, some definitions focus on identifying specific cohorts of people considered to be at greater risk of vulnerability in their interactions with markets, such as older people, people with disability and people experiencing mental illness. Other definitions rely less on a list-based approach and focus more on broad circumstances of vulnerability. Most definitions remain quite general, leaving room for understandings of vulnerability to evolve in response to regulatory, business, technological and social changes, and new understandings of consumer needs.
- 5 As a society, we understand that vulnerabilities frequently manifest in chronic and ongoing ways correlated with complex experiences of marginalisation and exclusion. Indicators for this can include cognitive, cultural, or sexual difference; isolation; disability; mental health; family violence; intergenerational poverty or trauma; and associated forms of discrimination. We also recognise that specific events such as illness or injury, job loss, the death of someone we love, financial shock, incarceration, divorce, and natural disaster will create vulnerability in consumers' lives. And we know that common experiences across all life stages can heighten our vulnerability: transitioning to living independently, becoming a parent or caregiver, ageing. Because indicators for vulnerability are so frequently described in this way, in relation to personal circumstances or attributes, it can be easy to overlook the fact that market design is also a cause of consumer vulnerability.
- 6 Elisabeth Costa, Katy King, Ravi Dutta and Felicity Algate (2016) [Applying behavioural insights to regulated markets](#), London: Citizen's Advice.
- 7 The deliberate manipulation of consumer behaviour using 'sludge' and 'dark patterns' is described in the first CPRC report in this series, [Stepping Towards Trust](#). See also the work of the Norwegian Consumer Council in this area: <https://www.forbrukerradet.no/dark-patterns/>.
- 8 Information asymmetry between consumers and business with access to data about their consumer habits and behaviours can enable new forms of price discrimination. A study of in-app advertising across ten service platforms, conducted by the Norwegian Consumer Council, found evidence that: "Extensive knowledge about purchase histories, browsing habits and economic situations can be leveraged to determine the maximum price a consumer is willing to pay for a product or service, and adjust the pricing accordingly. If the price of a product or service differs on an individual level, it also becomes impossible for consumers to compare offers. Similarly, (dis)information campaigns using targeted messaging are difficult to uncover and survey, because two people will never see the same message." Forbrukerrådet [Norwegian Consumer Council] (2020), [Out of Control - How consumers are exploited by the online advertising industry](#), pp47-48. Data analytics allows consumer profiling across datasets not only to generate sales leads but also to identify when those individuals may be most vulnerable to being approached or influenced to make certain choices. For example, the Privacy International report [Your mental health for sale](#) presents the results of a 2019 research study of 136 mental health websites, finding that 76% of the sites surveyed contained embedded third-party trackers that harvest data for advertising or marketing purposes, including instances of depression websites passing answers and results of online mental health check tests to third parties.
- 9 Large scale manipulation of consumer data has increased opportunities for market features that generate or exploit consumer vulnerability to proliferate. The profitability of such features has become the underlying business model for many data brokers, service aggregators, and online advertisers, to the detriment of consumers. Consumer protections have struggled to keep pace with the detail, volume, and extent of data collection, the speed and specificity of targeting that can be obtained through algorithmic analysis, and the opacity of decision-making that can result. This can have significant consequences for consumers seeking to challenge poor outcomes or demonstrate unfair treatment. (See, for example: Ramirez et. al. (2014) [Data Brokers: A Call for Transparency and Accountability](#) US Federal Trade Commission; Australian Human Rights Commission (2020), [Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias](#), p53; and Australian Competition and Consumer Commission (2019) [Digital Platforms Inquiry Final Report](#), Canberra: ACCC; p498 and Recommendation 21).

- 10 Graphic reproduced from O'Neill, Emma (2020), [Exploring regulatory approaches to consumer vulnerability: a report for the Australian Energy Regulator](#), Melbourne: AER/CPRC, p5.
- 11 Ibid.
- 12 For a more detailed treatment of consumer choice and engagement, see Ben Martin-Hobbs and Emma O'Neill (2020), [The experiences of older consumers: towards markets that work for people](#), Melbourne: CPRC, pp48-54.
- 13 One such example is the proliferation of new online scams and phishing attempts targeting people with limited digital literacy and other vulnerabilities (<https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams>). As well, rapid uplift in online shopping and, in face-to-face environments, the shift toward 'tap and go' and other online payments (including implementation of app-based ordering and payment platforms in food and beverage businesses) have created new barriers for some customers where digital payment platforms are not readily understood or navigated because of differing language, cognitive, technical, or physical ability; or are not sufficiently accessible due to assumptions about people's ownership and mastery of electronic devices.
- 14 Keynote address by Karen Chester, Acting Chair, ASIC at the 2020 AFR Banking & Wealth Summit, Wednesday 18 November 2020, <https://asic.gov.au/about-asic/news-centre/speeches/getting-on-with-it/>
- 15 In the case of the Consumer Data Right (CDR), concerns exist amongst the community sector that cross-policy lobbying by industry will loosen the scheme's initial consumer protections in areas including direct marketing, on-selling of consumer data, and disclosure of CDR data to unaccredited third parties. The impacts these changes could create in terms of heightened consumer vulnerability have been highlighted by consumer groups and by an independent Privacy Impact Assessment. See, for example the joint submission provided by Financial Rights Legal Centre and Consumer Action Legal Centre in response to the ACCC's September 2020 CDR rules expansion amendments Consultation Paper; and the Maddocks (2020) Australian Competition and Consumer Commission – Consumer Data Right Regime, Update 2 to Privacy Impact Assessment: Analysis as at 29 September 2020. On the successful representation of industry viewpoints, we note findings from our first report in this series that written submissions representing consumer interests average less than 20% by number of public submissions to CDR consultations (CPRC, [Stepping Towards Trust](#), p1) and draw attention to views and findings represented in the Senate Select Committee on Financial Technology and Regulatory Technology's 2019 interim report.
- 16 Consumer Policy Research Centre, *Consumers and COVID-19: from crisis to recovery: 6 month trend data (October monthly briefing)*, Melbourne: CPRC.
- 17 Elbogen, E., Lanier, M., Montgomery, A., Strickland, S., Wagner, H. and Tsai, J. (2020), '[Financial Strain and Suicide Attempts in a Nationally Representative Sample of US Adults](#)', *American Journal of Epidemiology*, Volume 189, Issue 11, November 2020, pp 1266–1274.
- 18 Davidon, P., Saunders, P., Bradbury, B. and Wong, M. (2020), *Poverty in Australia 2020: Part 1, Overview*. ACOSS/UNSW Poverty and Inequality Partnership Report No. 3, Sydney: ACOSS, p9.
- 19 See, for example; <https://pwd.org.au/resources/disability-info/social-model-of-disability/>
- 20 Section 56BAA of the Competition and Consumer Act prescribes that "The consumer data rules must specify a requirement on an accredited data recipient to delete all or part of CDR data in response to a valid request by a CDR consumer.
- 21 Rule 4.9 of the CDR Rules.
- 22 Screen scraping was specifically identified by multiple legal and counselling services we spoke to as being a factor observed to exacerbate vulnerability and financial hardship for clients of their services. We were given examples where companies have used knowledge of consumers financial position obtained through screen scraping to target them at a later date with unaffordable (and unsolicited) offers for payday lending. More generally, screen scraping may void existing consumer protections by putting consumers in breach of their user agreements with banks and other data holders. Unlike CDR, data sharing through screen scraping gives consumers little or no oversight or recourse with regard to demonstrating harmful or unauthorised use of consumer data by those third parties.
- 23 CPRC's roundtables with consumer advocates and community sector organisations suggest that 'vulnerability' can often be conflated in people's minds with "weakness", "being a problem", or "being a victim". Policymakers and regulators should be alert to how this perception impacts on the comfort and willingness consumers may have in engaging with programs and policy interventions that are overtly targeted towards vulnerability. One policy analyst working in domestic violence services explained it: "[In the domestic violence field] we often use 'marginalised' rather than vulnerability – this turns the focus back on the products and services rather than the people who use them." (Participant, CPRC Roundtable, November 2020).
- 24 Participant, CPRC Roundtable, November 2020.
- 25 Ibid.

- 26 The evidence base for this proposition is well established. See, for example, Martin-Hobbs, B. and O'Neill, E. (2020) [The experiences of older consumers: towards markets that work for people](#), Melbourne CPRC, and ASIC REP632 (2019) [Disclosure: Why it shouldn't be the default – A joint report from the Australian Securities and Investments Commission \(ASIC\) and the Dutch Authority for the Financial Markets \(AFM\)](#).
- 27 Examples given include: in the banking sector, direct observation of interactions between joint account holders (for example in meetings to discuss home loan products) which may signal flags of family violence or financial abuse; in the utilities sector community sector representatives posed the example of regional water services developing trusted relationships with longstanding customers experiencing ongoing vulnerability, leading to earlier disclosure of difficulty by customers, greater understanding and empathy from the water retailer, and more successful negotiation of hardship
- 28 Participant, CPRC Roundtable, November 2020.
- 29 Ibid.
- 30 Rights by design approaches to consumer platforms, administrative systems, and regulatory technology – in particular, data rights by design – are currently the focus of research into administration of human displacement (see: Anne Gilliland and Kathy Carbone (2019) 'An analysis of warrant for rights in records for refugees' *The International Journal of Human Rights*, 24: 483-508) and child protection systems (Greg Rolan, Han Phan, & Joanne Evans (2020). 'Recordkeeping and Relationships: Designing for Lifelong Information Rights'. In *DIS '20: Proceedings of the 2020 ACM Designing Interactive Systems Conference*, Eindhoven Netherlands July 2020.
- 31 The privacy by design framework was developed in the 1990s by Ann Cavoukian, Information and Privacy Commissioner of Ontario as an approach to systems engineering, following her joint work with the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research. In 2010 the framework achieved international acceptance when the International Assembly of Privacy Commissioners and Data Protection Authorities unanimously passed a resolution on privacy by design recognising it as an international standard and resolving (among other commitments) to promote privacy by design as widely as possible and foster the incorporation of the principle into policy and legislation.
- 32 For example, the California Consumer Privacy Act (CCPA) in the US, the General Data Protection Regulation (GDPR) in Europe, and indeed Australia's Consumer Data Right (CDR). Regarding social license and rights to privacy in digital markets, publications by digital rights action groups such as Access Now are instructive.
- 33 Relevant examples are described in Nicol Turner Lee, Paul Resnick, and Genie Barton (2019) [Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms](#), Washington DC: Brookings Institution. For a technical treatment of algorithmic bias: Australian Human Rights Commission (2020) [Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias](#), Sydney: AHRC.
- 34 On Algorithmic Impact Assessments see, for example: Lee et.al ([ibid](#)); Dillon Reisman, Jason Schultz, Kate Crawford, Meredith Whittaker (2018) [Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability](#), New York: AI Now Institute; and Mathieu Lemay (2019) [Understanding Canada's Algorithmic Impact Assessment Tool: A must for doing business with the Federal Government](#).
- 35 Anonymous (public comment); appended to Hooker, Sara (2018) 'Why "data for good" lacks precision' <https://towardsdatascience.com/why-data-for-good-lacks-precision-87fb48e341f1>
- 36 Goodson, Lisa & Phillimore, Jenny [eds.] (2012) *Community Research for participation: from theory to method*. Bristol: The Policy Press.
- 37 Hooker, Sara (2018) 'Why "data for good" lacks precision' <https://towardsdatascience.com/why-data-for-good-lacks-precision-87fb48e341f1>
- 38 Ibid.
- 39 Recommendation 6.19 in Farrell, S. (2020) [Future Directions for the Consumer Data Right](#), The Treasury, Commonwealth of Australia, p135. On data standards for consent, see also pp 143-144 of the same report.
- 40 See, for example Financial Conduct Authority (2020) [Guidance Consultation and feedback statement: Guidance for firms on the fair treatment of vulnerable customers](#); The Australian Banking Association [Industry guideline: Financial abuse and family and domestic violence policies](#).
- 41 Data Standards Body (2021), CX Working Group Noting Paper 157: [CX Data Standards Following v2 Rules](#).
- 42 Regarding this example: Crozier, R. '[CBA, other banks weigh IT countermeasures against digital payment abuse](#)' (IT News, June 11, 2020) and Collier, A. '[NAB highlights technical hurdles filtering for abuse in transaction descriptions](#)' (IT News, September 16, 2020).

- 43 Wiseradviser operates as part of the UK Money Advice Trust. They offer free tools and services to charities and provide training to 85% of the free debt advice sector in the UK. These frameworks have been reproduced from their website.
- 44 This could potentially build on recent RegTech projects conducted by the Australian Securities & Investments Commission (ASIC) that have explored similar territory, such as testing the utility of voice analytics and voice-to-text (VA&VT) technologies for processing a large volume of life insurance sales calls “to identify, analyse and report on poor conduct, including pressure sales tactics, sales to vulnerable consumers, inappropriate or omitted information about products, and possible indicators that consumers were not comfortable engaging with the service” (<https://asic.gov.au/for-business/innovation-hub/asic-and-regtech/asic-regtech-initiative-series-2018-19/regtech-life-insurance-sales-calls-voice-analytics-and-voice-to-text-trial-and-symposium/>). See also: <https://asic.gov.au/for-business/innovation-hub/asic-and-regtech/asic-regtech-initiative-series-2018-19/regtech-monitoring-financial-promotions-demonstration-and-symposium/>
- 45 Cook, Tim. From an introductory session address at *CPDP 2021: Enforcing Rights in a Changing World*, Computers, Privacy and Data Protection Annual Conference, Brussels, January 2021.
- 46 This extends on ideas discussed in the first CPRC report in this series; and is elaborated further in Section 5, as part of Recommendation 4b of this report.
- 47 Potential utility of embedded consent markers to support vulnerability principles, strengthen oversight and trust, and improve mechanisms for desirable CDR functionalities is discussed on page 27 of this report.
- 48 On this, see Australian Human right Commission (2020) [Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias](#), pp 52-56.
- 49 See resources available at: <https://www.openbanking.org.uk/insights/vulnerable-customers/>
- 50 BEUC (2020), [The Manipulated Consumer, The Vulnerable Citizen](#).
- 51 We recognise that the complaints framework for CDR is underpinned by a ‘no wrong door’ approach aimed at ensuring an accessible mechanism for consumers, however we also note that such approaches in and of themselves will not guarantee accessibility for people experiencing vulnerability. For example, a 2019 study of Victoria’s out-of-home-care system conducted by the Commission for Children and Young People (CCYP) found that “an extremely low number of children and young people raise complaints using the department’s complaints mechanism” (CCYP, 2019, [In Our Own Words: Systemic inquiry into the lived experience of children and young people in the Victorian out-of-home care system](#); Finding 13), with three key reasons identified: these processes are not child friendly or informed by issues affecting children in care; they are not known; and they are not trusted (ibid, pp124-125). These shortfalls were occurring despite the apparent existence of no wrong door style approaches to young people raising complaints (described ibid, p126).
- 52 Neave, Colin (2015) ‘Exploring the Role of the Commonwealth Ombudsman in Relation to Parliament’ in *Papers on Parliament no. 63*, Canberra: Commonwealth of Australia.
- 53 This opportunity and its basis of trust is prefigured in the first CPRC report in this series, [Stepping Towards Trust](#), refer p41.
- 54 Reynolds et. al. (2019) [Consumer Priorities for Open Banking](#), p2.
- 55 A wide range of data about use of CDR will be generated through the scheme and can be used to build a picture of the impact it is having for consumers (including types of service offerings coming onto market; uptake of various CDR products and providers within and across sectors; and metrics relating to volumes of customers, accounts, consents; volumes of requests being handled through CDR APIs; system performance levels and numbers of invalid requests; volume and substance of complaints). As well, opportunities will exist for hybrid analysis - such as gathering evidence of qualitative measures through language-based analysis of complaints data. To achieve greatest benefit for CDR consumers when considering how the success of use cases and procedures will be tested, it is important to think not just about the objective validity of metrics (eg. repeatability, integrity of source) but also who they are being validated for. Different measures will be necessary to satisfy different stakeholders. For example, metrics intended to demonstrate how well a government policy objective has been met might be measured simply by capturing the number of participants or products in a system, or the number of ‘switches’ facilitated by CDR. Aligning outcomes with the needs and expectations of community members themselves is likely to require greater reliance on qualitative evidence, and more detailed analysis of user experiences – for example, comparison of number of participants against volumes and types of complaints; or following the flow on effects of CDR initiated switches in energy providers to observe longer term impacts on consumers’ levels of energy security or distress.
- 56 UK Financial Reporting Council (2016) [Corporate Culture and the role of Boards: report of observations](#), p8.
- 57 At first glance the notion that there is a collective responsibility for creating (and addressing) consumer vulnerability may seem at odds with an emphasis on greater individual responsibility, but arguably both positions are working towards a similar purpose. Bringing a social model of consumer vulnerability to CDR is an acknowledgement of the need to establish conducive market environments before self-efficacy, resilience, and personal responsibility can take root and thrive. If CDR’s consumer protection settings are misjudged, or if moral and legal responsibility for ‘doing the right thing’ is avoided, CDR consumer data sharing may put consumers at greater risk of being targeted for products and services that deepen financial distress, increase exposure to fraud or scams, or otherwise heighten vulnerability. Conversely, if these protections and responsibilities are embedded into the culture of CDR participation, consumer vulnerability becomes a positive opportunity to strengthen systems, build resilience, and grow trust.
- 58 O’Neill, Emma (2020), [Exploring regulatory approaches to consumer vulnerability: a report for the Australian Energy Regulator](#), Melbourne: AER/CPRC, p8.

APPENDIX 1

Consumer vulnerability: table of definitions¹

Sector / organisation	Definition
Cross-sector	
Organisation for Economic Co-operation and Development	Vulnerable consumers are consumers who are susceptible to detriment at a particular point in time, owing to the characteristics of the market for a particular product, the product's qualities, the nature of a transaction or the consumer's attributes or circumstances. ²
Australian Competition and Consumer Commission	<p>Conduct affecting vulnerable and disadvantaged consumers is an ongoing compliance and enforcement priority for the ACCC.³</p> <p>The ACCC does not adopt a single definition of consumer vulnerability. In its compliance guide for business on disadvantaged and vulnerable consumers, it states some consumers may be disadvantaged or vulnerable in marketplace situations if they:</p> <ul style="list-style-type: none"> • have a low income • are from a non-English speaking background • have a disability • have a serious or chronic illness • have poor reading, writing and numerical skills • are homeless • are very young • are old • come from a remote area • have an Indigenous background.⁴ <p>In its 2018 Retail Electricity Pricing Inquiry, the ACCC considered two overlapping forms of vulnerability:</p> <ul style="list-style-type: none"> • where a consumer who, due to personal circumstances, is unable to meet or is at risk of being unable to meet the cost of electricity supply and, as a result, is at risk of experiencing detriment to their wellbeing and standard of living

¹ O'Neill, Emma (2019) *Exploring regulatory approaches to consumer vulnerability: A report for the Australian Energy Regulator* Melbourne: CPRC. Reproduced with permission of the AER.

² Organisation for Economic Co-operation and Development (March 2014) *OECD Recommendation on Consumer Policy Decision Making*, p4.

³ Australian Competition and Consumer Commission (2019) 'Compliance & Enforcement Policy & Priorities'.

⁴ Australian Competition and Consumer Commission (2011) 'Don't Take Advantage of Disadvantage: A Compliance Guide for Businesses Dealing with Disadvantaged or Vulnerable Customers'.

Sector / organisation	Definition
	<ul style="list-style-type: none"> • where a consumer faces additional barriers to engaging with the retail electricity market.⁵
Competition and Markets Authority (UK)	<p>Consumer vulnerability is defined as 'any situation in which an individual may be unable to engage effectively in a market and, as a result, is at a particularly high risk of getting a poor deal'. The CMA distinguishes between:</p> <ul style="list-style-type: none"> • market-specific vulnerability, which derives from the specific context of particular markets and can affect a broad range of customers in those markets • vulnerability associated with physical characteristics, such as physical disability, poor mental health, or low incomes, which may result in individuals with those characteristics facing particularly severe, persistent problems across markets.⁶
Commission for Customers in Vulnerable Circumstances (UK)	<p>The CCVC adopts the Ofgem definition of vulnerability— that is, where a consumer's personal circumstances and characteristics combine with aspects of the market to create situations where they are:</p> <ul style="list-style-type: none"> • significantly less able than a typical consumer to protect or represent their interests; and/or • significantly more likely than a typical consumer to suffer detriment or that detriment is likely to be more substantial.⁷
European Commission	<p>A vulnerable consumer is one who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation or market environment:</p> <ul style="list-style-type: none"> • is at higher risk of experiencing negative outcomes in the market • has limited ability to maximise their wellbeing • has difficulty in obtaining or assimilating information • is less able to buy, choose or access suitable products • is more susceptible to certain marketing practices.⁸
Energy sector	
Ofgem (GB)	<p>Vulnerability occurs where a consumer's personal circumstances and characteristics combine with aspects of the market to create situations where they are:</p> <ul style="list-style-type: none"> • significantly less able than a typical consumer to protect or represent their interests; and/or

⁵ Australian Competition and Consumer Commission (June 2018) *Restoring Electricity Affordability and Australia's Competitive Advantage: Retail Electricity Pricing Inquiry – Final Report*, p291.

⁶ Competition and Markets Authority (February 2019) *Consumer Vulnerability: Challenges and Potential Solutions*, p4.

⁷ Ibid p19.

⁸ European Commission (January 2016) *Consumer Vulnerability Across Key Markets in the European Union – Final Report*.

Sector / organisation	Definition
	<ul style="list-style-type: none"> significantly more likely than a typical consumer to suffer detriment or that detriment is likely to be more substantial.⁹
Financial services sector	
Australian Securities and Investments Commission	<p>Any consumer can experience vulnerability as a result of a number of factors, including:</p> <ul style="list-style-type: none"> the actions of the market or individual providers, e.g. being targeted by products that are inappropriate for a particular consumer, or being given inadequate or overly complex documentation experiencing specific life events or temporary difficulties, e.g. an accident or sudden illness, relationship breakdown, family violence, job loss, having a baby or the death of a family member personal or social characteristics that can affect a person's ability to manage financial interactions, e.g. speaking a language other than English, having different cultural assumptions or attitudes about money, or experiencing cognitive or behavioural impairments due to intellectual disability, mental illness, chronic health problems or age.¹⁰
Banking Code of Practice	<p>Vulnerable customers include those who are experiencing:</p> <ul style="list-style-type: none"> age-related impairment cognitive impairment elder abuse family or domestic violence financial abuse mental illness serious illness any other personal or financial circumstance causing significant detriment.¹¹
Life Insurance Code of Practice	<p>The Code refers to 'consumers requiring additional support' rather than vulnerable customers. It states: 'we recognise that some groups may have unique needs, such as older persons, consumers with a disability, people from non-English speaking backgrounds and Indigenous people, when accessing insurance, making an inquiry, claiming on their insurance, making a compliant and communicating with us'.¹²</p>
Insurance in Superannuation	<p>The Code has a section on vulnerable consumers but does not define this term as such. It states: 'we recognise that some people may have unique needs, such as older persons, people with</p>

⁹ Ofgem (13 June 2019) Draft Consumer Vulnerability Strategy 2025, pp47-48.

¹⁰ Australian Securities and Investments Commission (2019) ASIC Corporate Plan 2019-2023 – Focus 2019-20, p12.

¹¹ Australian Banking Association (1 July 2019) Banking Code of Practice, p22.

¹² Financial Services Council (2019) Life Insurance Code of Practice, p14.

Sector / organisation	Definition
Voluntary Code of Practice	<p>mental health conditions, people with a disability, people from non-English speaking backgrounds, people with low levels of literacy, people in financial distress, and Indigenous Australians, when accessing insurance, making an enquiry, claiming on their cover, making a complaint and communicating with us'.¹³</p>
Financial Conduct Authority (UK)	<p>A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care.¹⁴</p>
Telecommunications sector	
Telecommunications Consumer Protections Code	<p>The Code requires telecommunications suppliers to have regard to the ACCC compliance guide 'Don't Take Advantage of Disadvantage' in respect of disadvantaged and vulnerable consumers but does not provide a definition of these consumers.¹⁵</p> <p>Telecommunications regulation provides entitlements to people with particular needs, including older people, those living in rural and remote areas, people who speak English as a second language, and people with disability or a life-threatening illness.¹⁶</p>
Ofcom (UK)	<p>UK telecommunication providers have regulatory obligations in relation to people with disability, and consumers who may be vulnerable due to circumstances such as age, physical or learning disability, physical or mental illness, low literacy, communications difficulties or changes in circumstances such as bereavement.¹⁷</p>
Water sector	
Ofwat (UK)	<p>Ofwat uses the concept of 'a customer whose circumstances make them vulnerable', defined as 'a customer who due to personal characteristics, their overall life situation or due to broader market and economic factors, is not having reasonable opportunity to access and receive an inclusive service which may have a detrimental impact on their health, wellbeing or finances'.¹⁸</p>

¹³ Association of Superannuation Funds of Australia, Australian Institute of Superannuation Trustees and Financial Services Council (2018) Insurance in Superannuation Voluntary Code of Practice, p11.

¹⁴ Financial Conduct Authority (February 2015) Consumer Vulnerability – Occasional Paper No. 8.

¹⁵ Communications Alliance (July 2019) Industry Code C628:2019 – Telecommunications Consumer Protections Code, p20.

¹⁶ See Australian Communications and Media Authority, 'People with Particular Needs'.

¹⁷ Ofcom (1 July 2019) General Conditions of Entitlement – Unofficial Consolidated Version.

¹⁸ Ofwat (February 2016) Vulnerability Focus Report, p20.

Acknowledgement

This report is the product of many minds.

The Consumer Policy Research Centre thanks everyone who participated in the discussions that informed this document. We share our gratitude for your willingness to engage meaningfully on a complex subject at a time when COVID-19 has invoked new demands and challenges in the community sector.

In recognising the generosity of all involved, we further acknowledge this participation as a clear indication of the community sector's interest in contributing to the development of a Consumer Data Right that supports fair markets and positive outcomes for all consumers, through innovation that understands the diverse forms that vulnerability and capability take.