Submission on discussion document: *Unlocking value from our customer data*

Your name and organisation

Name	**Dr Zofia Bednarz** University of Sydney and ARC Centre of Excellence on Automated Decision-Making and Society **Mr Chris Dolman FIAA** Executive Manager, Data and Algorithmic Analytics, IAG **Prof Kimberlee Weatherall** University of Sydney and ARC Centre of Excellence on Automated Decision-Making and Society
Organisation (if applicable)	We note that this submission is made in our personal capacities and not as representatives of any of the organisations with which we are associated.
Contact details	Privacy of natural persons

[Double click on check boxes, then select 'checked' if you wish to select any of the following.]

☐ The Privacy Act 2020 applies to submissions. Please check the box if you do not wish your name or other personal information to be included in any information about submissions that MBIE may publish.

☐ MBIE intends to upload submissions received to MBIE's website at ***www.mbie.govt.nz***. If you do not want your submission to be placed on our website, please check the box and type an explanation below.

I do not want my submission placed on MBIE's website because… [Insert text]

Please check if your submission contains confidential information:

☐ I would like my submission (or identified parts of my submission) to be kept confidential, and **have stated below** my reasons and grounds under the Official Information Act that I believe apply, for consideration by MBIE.

I would like my submission (or identified parts of my submission) to be kept confidential because… [Insert text]

Responses to discussion document questions

In this submission, we would like to bring your attention to a paper focusing on the application of the Australian CDR to the insurance sector. The updated version of the paper entitled 'Consumer Data Right, Insurance Contracts and How Much Choice There Really Is' is forthcoming in the August 2023 issue of the *Competition & Consumer Law Journal*. The paper was first presented at the All Actuaries Summit organised by the Actuaries Institute in May 2022 (under the title 'Insurance Underwriting in an Open Data Era: Opportunities, Challenges and Uncertainties'). Our paper contains findings relevant to questions posed in the discussion document. Please see our brief answers to the discussion questions 6, 17 and 21 below, and the May 2022 full version of our paper is attached to this submission in 'Other comments' section.

How will the draft law interact with protections under the Privacy Act?	
1	*Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?*

Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*

3	*What settings for managing ongoing consent best align with data governance tikanga?*

4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*

5	*How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*

6	*What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?*
	The *Customer and Product Data Bill* indicates that a data request can only be a condition of accessing a product or service if data sharing is '*reasonably necessary*' to facilitate the provision of the product (s 35). This is similar to the data minimisation principle contained in the Australian CDR (which we refer to hereafter simply as the CDR). A significant part of the discussion in our paper relates to that requirement. **In particular, we observe that the CDR contains a requirement under the data minimisation principles that data needs to be 'reasonably needed' for the intended purpose. It is unclear whether and how this might create barriers for insurers who wish to use CDR data to create novel underwriting questions. Certainly it is not the case that CDR**

	data used in such a manner would be necessary to offer insurance: it is not used today, after all. But a test requiring that data be 'reasonably needed' to offer some good or service is substantially weaker than saying it must be necessary. Is broad and substantial insurer access to consumer data held by banks, telecommunications companies and energy companies 'reasonably needed', merely because an insurer wishes to use it to assess risk? Are there some circumstances which are acceptable and some not? When and why? This is unclear to us today, and so far as we have seen in the various policy documents recently published in relation to the CDR, little thought has been given to whether certain kinds of access or use are unacceptable. **This uncertainty regarding what is permitted - and what *ought* to be permitted - is not limited to insurance, and we suggest ought to be clarified by further discussion and guidance. We could start by contemplating hypothetical cross-industry data uses within existing designated sectors. For example: is it 'reasonably needed', or not, for a loan application to seek access to electricity consumption data, to decide whether to provide an offer or product feature such as a lower interest rate? Is it 'reasonably needed' for that same electricity provider to request banking transaction data, perhaps to target discounts at the most reliable customers, or those who commonly make use of payment authorisations? We ought to have clear answers to such questions. And we ought to be thinking through the industry and societal *implications* of saying that data is 'reasonably needed'. Are there, for example, customers who are going to miss out on discounts, or be excluded from service or products, as judgments begin to be made about their credit card histories? Consideration of such questions naturally leads onto broader considerations of fairness – a topic we discuss in more detail via a stylised insurance market example in the full paper attached.**
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*

8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*

9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[1] are suitable for use in other sectors, and which could require significant modification?*

10	*What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?*
	---

[1] New Zealand API standards to initiate payments and access bank account information. They are based on the UK's Open Banking Implementation Entity standards but tailored for the New Zealand market. Market demand has driven development and led to the creation of bespoke functionality for New Zealand.

Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*

12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*

13	*What accreditation criteria are most important to support the participation of Māori in the regime?*

14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*

Unlocking value for all	
15	*Please provide feedback on:* • *the potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty* • *the types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori* • *any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.*

16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*

17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
	Please refer to our full paper attached below in relation the accessibility and inclusion. Our stylised market example demonstrates, in the context of the CDR which operates on very similar principles to those proposed by the *Customer and Product Data Bill,* that the two features of CDR: optionality of data transfer, and non-universal ability to share that data, will create some significant social challenges in insurance underwriting, likely exacerbating issues of affordability, particularly for vulnerable customers. We note that these are core design principles of the CDR. While our example focused on insurance, it is general in nature: it is inherent in the idea of detailed consumer data being used for pricing - and so the issues of fairness, and the undermining of optionality are likely to generalise to other forms of personalisation, particularly economic personalisation.

	One promising avenue for reform to prevent such outcomes – which would be most keenly felt by already vulnerable and disadvantaged consumers – is within the CDR regime itself, through reform of the data minimisation principle. Perhaps, for example, it could be split into two. On one hand, this could be designed to readily accept use cases which require CDR data as a genuinely essential feature for the product or service to exist at all (a much higher bar than 'reasonably needed'): this would cover, for example, collection and use of product data for the purposes of comparing deals available in the market. Then for personalisation use cases (such as insurance pricing), where data may be 'reasonably needed' to facilitate the intended personalisation but the personalisation itself is not essential to the general product offering and might cause some detriment to some community members, more emphasis could be given to considerations of fairness across and between customers before such use cases are permitted. This would mean that CDR would have to reorient itself away from individual rights and an emphasis on individual outcomes, towards broader consideration of the effects of data availability on markets and whether those effects are fair to consumers in general, with particular emphasis on vulnerable or disadvantaged consumers. We think this would be a positive move for the community.
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*

Ethical use of data and action initiation	
19	*What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?*

20	*Are there other ways that ethical use of data and action initiation could be guided or required?*

Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	The two of the purposes of the proposed Act are to (a) realise the value of certain data for the benefit of individuals and society; and (b) promote competition and innovation for the long-term benefit of customers. **Please refer to our paper attached where we outline how, unfortunately, vulnerable consumers may be further disadvantaged and marginalised as the consequence of an economy-wide data sharing scheme, which we discuss using the example of the insurance sector in Australia. This would however mean that the benefit of the scheme for the society as a whole, and for certain consumers, is questionable, unless specific safeguards are put in place.**
22	*Do you agree with the territorial application? If not, what would you change and why?*

Regulated data services	
23	*Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?*

24	*How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?*

Protections	
25	*Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?*

26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*

Regulatory and enforcement matters	
27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*

Administrative matters	
28	*Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?*

29	*What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?*

30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*

31	*Which additional information in the closed register should be machine-readable?*

32	*Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?*

33	*Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?*

34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*

Complaints and disputes	
35	*In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?*

Other comments

Insurance Underwriting in an Open Data Era: Opportunities, Challenges and Uncertainties

Paper presented at the Actuaries Institute *All Actuaries Summit*, May 2022
Zofia Bednarz, Chris Dolman and Kimberlee Weatherall

Abstract

Exchange of information is a critical part of insurance pricing and underwriting. Traditionally, this is in the form of mandatory question sets, which the prospective insured person must answer to a suitable level of reliability before obtaining a quote for cover. In Australia, the Insurance Contracts Act sets out some rules around this, and other analogous systems exist in various other countries around the globe.

The traditional manner of data collection had inherent practical limits. Questions had to be easily understood by laypeople, readily answerable by them, and not so extensive as to be off-putting. With the advent of open data regimes around the globe, many of these traditional limitations may be reduced or removed. By a mere press of a button, consumers may be able to share extensive and unprecedented data with an insurer, in order to automatically and accurately answer detailed questions that they might not necessarily understand or be able to answer if asked directly.

In this paper, we analyse whether open data regimes can be used in this manner to replace existing underwriting questions or to create new ones. We then examine the impact that this change may have on various cohorts of customers, particularly considering the potential impact on those without access to data, who may be more likely than average to be otherwise vulnerable or disadvantaged. We suggest thematic areas to consider for further guidance or reform, based on our analysis.

Keywords: Data, CDR, Open Data, Insurance, Underwriting, Pricing, Fairness

Background

Australia is in the midst of implementing an extensive 'open data' reform called the Consumer Data Right ('CDR'). The broad intent is to give consumers the ability to access data about themselves and their activities held by companies in designated industries, and direct the companies who hold that data to make it available to companies of the consumer's choice. As framed on its introduction, the CDR is about empowering consumers: it is "designed to give customers more control over their information leading, for example, to more choice in where they take their business, or more convenience in managing their money and services."[2]

Insurers are understandably interested in the prospects of more data becoming available: insurance has always been a data driven business. Data about people and the assets they care about has been used to assess risk and determine prices and policy conditions for centuries. Insurance legislation has long recognised this importance of data, resulting in a somewhat unique legal framework requiring more transfer of data than many other sectors of the economy. The *Insurance Contracts Act 1984* (Cth) ('ICA') contains significant provisions related to disclosure, giving insurers the ability to ask certain questions of a customer and giving the customer an obligation to answer those questions to a suitable level of reliability, in order that risk might be properly assessed.

In exploring the CDR regime and its potential relationship to pricing and underwriting practices, and disclosure duties, we can see some inherent structural questions and potential challenges. We structure the discussion in this paper by asking two related families of questions:

1. Can you replace existing underwriting questions with CDR data requests?

   Under the CDR rules, is it permitted to allow consumers to utilise CDR data to answer existing underwriting questions? Will this meet the requirements of existing disclosure rules? What effect may this have on outcomes for consumers? Are there any challenges, inconsistencies, or uncertainties?

2. Can you use CDR to create new underwriting questions?

   Can we use the existence of CDR to create new forms of underwriting questions – particularly, questions which could not reasonably be asked in a traditional manner due to their nature or extent? If we do so, what challenges, uncertainties or issues may exist – both for consumers and in terms of legislation?

Within both families of question, we focus on a critical principle of the CDR regime: that it is *the consumer's choice whether to share data* (which we refer to as 'optionality'). We consider how this

[2] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth), 3.

interacts with existing ICA rules and industry practice, identifying potentially severe consequences for this optionality principle when applied to insurance underwriting.

Can you replace existing underwriting questions with CDR Data Requests?

Many traditional underwriting processes can be represented by a series of questions on a webform. An obvious initial use case for CDR is to seek to replace or supplement some or all of this webform with a CDR data request. To do this we must ask: is this permitted under the CDR regime, and does the existing disclosure regime of ICA operate appropriately when this occurs?

Does the CDR Regime Permit This?

In short, whilst there are various conditions attached to the use of CDR for this purpose, there do not appear to be any significant *legal* barriers within the CDR regime which would stop this from occurring. The more substantial barriers are likely to be practical, arising from differences between the Australian Privacy Principles[3] that insurers are used to, and the more stringent privacy rules that apply to the CDR:[4] in particular, data minimisation, and rules requiring explicit, and active (not implied) consent to all secondary uses.

To access a consumer's data via the CDR, an insurer must first meet the requirements to become an accredited data recipient set out in Part 5 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (version 4) ('CDR Rules'). There are a range of conditions: the insurer (including its officers and CDR decision-makers[5]) must meet a 'fit and proper person' requirement, the firm must be able to take the necessary steps to adequately protect CDR data from misuse, interference, loss and unauthorised access, modification or disclosure; have appropriate insurance and an internal dispute resolution system as well as be a member of a recognised external dispute resolution system. None of these requirements would seem to be difficult for the average insurance company to overcome. Some would already be in place as part of general operations (notably in relation to dispute resolution), most others would seem simple to arrange.

Then, we must consider what data is being requested. Consumer data requests can only be made in relation to certain classes of product and consumer CDR data, specifically enumerated for each declared industry, in separate Schedules to the CDR Rules. In the case of banking,[6] an insurer might request:

- data about the customer (name, address, but also any information a person has supplied in applying for a product; if the person operates a business, then data about the business such as ABN, the nature of the business, date of registration etc);
- data about the account (opening and closing balances; direct debit authorisations);

[3] *Privacy Act 1988* (Cth) sch 1.

[4] *Competition and Consumer Act 2010* (Cth) pt IVD div 5.

[5] The set of people who must be 'fit and proper' extends to all 'associated persons' within the meaning of the *Corporations Act 2001* (Cth), as well as persons who would be involved in decision-making of the firm to be accredited, and people who can significantly impact the applicant's management of CDR data: CDR Rules (v4) Rule 1.7.

[6] CDR Rules (v4), sch 3.

- transaction data (transactions, descriptions, amounts, dates).[7]

We should also mention that CDR rules do not affect credit reporting provisions set out in the Part IIIA *Privacy Act 1988* (Cth). This means that the strict rules against disclosure and limiting use of reports provided by credit reporting bodies still apply, and these cannot be accessed for other purposes using the CDR.[8]

So let us assume that data relevant to an existing underwriting question that we wish to replace with CDR data is included within the scope of these Schedules. For example, transactions recording income might be used for setting coverage limits or prices of income protection policies. Such data would appear to be available - in principle - for this use. While the opportunity appears quite limited today, as CDR designation expands to other industries and datasets, this will also expand the potential underwriting questions which might be replaced in such a manner.

The potential challenges arise at the stage of specifying what CDR data would be sought, and how it would be obtained from the customer. The CDR rules here are prescriptive: far more so than rules that otherwise apply under general privacy law. First, the data minimisation principle (CDR Rules, Rule 1.8) limits an insurer's ability to request (and use) CDR data. An entity requesting CDR data:

- must not collect more data than is reasonably needed, or for a longer time period than is reasonably needed, in order to provide the requested goods or services; and
- may use the collected data only as reasonably needed in order to provide the requested goods or services or as otherwise consented to by the consumer.[9]

The first condition is probably easy to meet, at least where the data being sought would answer an existing underwriting question. However, the limitation on additional uses and requirement for specific consent is designed to be more stringent than existing privacy laws. Insurers would need to carefully consider whether their existing secondary uses of underwriting data would still be allowed for data collected via CDR: or whether customers would consent, if asked.

Div 4.3 deals with consents, again applying heightened rules compared to the *Privacy Act,* to ensure that consents are voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn (rule 4.9). In other words, the control over data use is meant to be in the consumer's hands (we return below to the question of how realistic this is). These rules dictate the form for consents in ways that will require changes in insurers' systems. Consents must (4.10):

- accord with consumer experience data standards (systems specifications, set out elsewhere);

---

[7] How informative this data truly is at the moment is an interesting question, which we will leave to one side for now. As anyone who has ever looked at their account or credit card statements knows, the data about transactions is not always especially informative: so much so that many companies will proactively tell their customers to expect a transaction on their card under a particular name. And this is even before we get to issues such as, "Yes it looks like I spend a lot of money at the hospital, but that's because I'm paying my mother's/child's/friend's hospital bills".

[8] This is true even though sch 3 of the CDR Rules (version 4) says that among the information that can be sought under the CDR includes "(iii) any information that: (A) the person provided at the time of acquiring a particular product; and (B) relates to their eligibility to acquire that product". Part IIIA of the Privacy Act 1988 (Cth) makes it unlawful for a credit provider (bank) to disclose credit eligibility information (which is defined in s 6 of the Privacy Act 1988 (Cth) as information received from a credit reporting body). Most of Part IIIA is however not relevant to insurers. The restrictions in Part IIIA are largely directed at the activities of credit reporting bodies (part IIIA div 2), and credit providers (part IIIA div 3).

[9] Compare the *Privacy Act 1988* (Cth), which allows secondary uses without consent if related (or in the case of sensitive data, directly related) to the primary purpose of collection, provided the individual would reasonably have expected that use to occur (Australian Privacy Principle 6.2).

- be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids;
- must not refer to the accredited person's CDR policy or other documents so as to reduce comprehensibility, or bundle consents with other directions, permission, consents or agreements.

The system must also (under rule 4.11):

- allow the CDR consumer to choose the types of CDR data to which the consent will apply by enabling the CDR consumer to actively select or otherwise clearly indicate their selections.
- obtain consent for the particular types of CDR data to be collected or disclosed, and the specific uses to be made of the CDR data.[10]

An example of a collection consent process might be for an insurer to present the CDR consumer with a set of un-checked boxes on a quote form corresponding to different types of data, inviting them to select the boxes that correspond to the data they consent to the insurer collecting via a CDR request. This might then be followed by a further 'use consent' for anything the insurer may wish to do with that data outside of the quote process. The rules (4.11 and 4.12) also require an insurer to provide, at the same time, information to a customer about how the collection or use (as applicable) complies with the data minimisation principle. In the case of a collection consent, this includes that collection is reasonably needed, and relates to no longer a time period than is reasonably needed; and in the case of use consent, that use would not go beyond what is reasonably needed in order to provide the requested goods or services to the CDR consumer or make the other uses consented to.

While these conditions - data minimisation and detailed explicit consent rules - do not expressly prevent data being used to replace underwriting questions, it may make such replacement unattractive to an insurer.

Does the Disclosure Regime of ICA Permit This?

Often, challenges with innovation stem not just from the new regime created, but with its compatibility (or lack thereof) with existing, overlapping, regimes. In our case, ICA is a significant piece of existing legislation covering the disclosure of information when people are applying for insurance, so it must be considered. Of particular relevance are the disclosure requirements, split between s 20B (consumer insurance contracts) and s 21 (other contracts).

The overarching aim of the insured's disclosure duty is to allow risk assessment by the insurer whilst also attempting to avoid issues of adverse selection and moral hazard, thus potential market failure.[11] The ICA implicitly assumes that an insured knows more about their own risk than an insurer is able to know, and therefore imposes a duty either to disclose all the relevant matters (s 21), or a duty to take reasonable care not to make a misrepresentation (s 20B).

The ICA also assumes the disclosure duty is carried out through a proposal form with a questionnaire a prospective insured fills in. Perhaps unsurprisingly, novel data transfer mechanisms such as CDR do not appear to have been contemplated. For example, the Act expressly refers to situations in which a prospective insured fails to answer (or gives an obviously incomplete or irrelevant answer to) a

[10] Compare the *Privacy Act 1988* (Cth), under which consent may be implied (s 6).

[11] Brendan McGurk, *Data Profiling and Insurance Law* (Hart Publishing, 2019) 141–43; Michael Rothschild and Joseph Stiglitz, 'Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information' (1976) 90(4) *The Quarterly Journal of Economics* 629; George A. Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84(3) *The Quarterly Journal of Economics* 488.

question included in a proposal form about a matter (ss 20B(5) and 21(3)). In such a case, in relation to consumer contracts, failure to answer one of the questions is not sufficient to amount to misrepresentation on the part of the insured. In the case of other contracts, the insurer is deemed to have waived compliance with the duty of disclosure in relation to the matter covered by the question, if they accept such an answer. These rules place the burden on an insurer to check if a prospective insured answered all the precontractual questions to a satisfactory standard. However, if we assume that sharing one's data through the CDR mechanism could be construed as replacing the proposal form and questionnaire, or at least sections of it, a refusal to share the data would likely be viewed similarly to a refusal to answer any or some (significant part) of the questions in a proposal form. This would not pass unnoticed by an insurer, thus making rules of ss 20B(5) and 21(3) somewhat redundant.

It seems likely that an insurer would offer manual data entry as a non-CDR option for completing an existing question in a quote, similarly to today's processes: until CDR matures, many potential insureds would not necessarily have access to, or be comfortable in using, a new data sharing mechanism like CDR. But if we look at the law, it's possible that there would be some pressure on consumers to use the new system. The question under s 20B(2) is '[w]hether or not an insured has taken reasonable care not to make a misrepresentation is to be determined with regard to all the relevant circumstances.' If an insured elects not to use CDR to answer a question, then answers that question manually yet incorrectly, does the decision to decline the option of CDR represent a sufficient lack of care to fall foul of s 20B? If it does, then this would challenge the opt-in nature of the CDR itself - insureds may feel obligated to consent to a CDR request to avoid a potential issue of misrepresentation, rather than take the risk of manual data entry. They may also feel unable to correct, or uncomfortable correcting CDR data retrieved which they suspect might be incorrect, in case they are wrong in that assessment. This becomes even more challenging when an insurer elects to refuse cover altogether if questions are not answered - which is common industry practice in many cases. All this could essentially make CDR data transfer mandatory for getting an insurance quote, which is against the conception of the CDR regime as being under the control of, and at the option of, the consumer only.

Summary

ICA was drafted with traditional proposal forms in mind, not data sharing regimes like the CDR. Whilst there does not appear to be anything specific in ICA or the CDR rules which might prevent CDR requests from replacing traditional underwriting questions, there are open questions surrounding such a regime, particularly surrounding the disclosure obligations of ICA. This may require some additional guidance or redrafting of ICA in order to more clearly contemplate data sharing as an alternative to traditional proposal forms.

Importantly, common market practice today is to make access to a product dependent on completing all relevant underwriting questions. While CDR is - in theory - opt-in, disclosure obligations within ICA combined with common market practice could result in a situation where CDR data transfer becomes effectively mandatory. This conflict between the intended consumer control and choice over CDR, and the likely practice on implementation in insurance should be considered in any future CDR reforms. Whilst it is not in the scope of this paper, we also observe that optionality of CDR may be similarly challenged in other industries - for example loan application forms are typically also required to be completed in full in order to access the product.

Can you use CDR to create new underwriting questions?

For those with a focus on innovation in insurance markets, perhaps a more interesting question to ask is whether CDR opens opportunities for *new* underwriting questions. No doubt, there are many situations where insurers would like to have access to certain types of information, or would like to ask particular questions of insureds, in order to assess risk. However, the process of asking and answering questions takes time and effort, especially from consumers, so questions must be easily

understood by laypeople, readily answerable by them, and not so extensive as to be off-putting. This puts natural limits on both the number, and kind of questions that can realistically be asked and answered. However (and as we discussed above), any consumer or business for whom CDR data is available can easily transfer it – so at least where data is available via CDR, these traditional barriers may be reduced or removed.

So, extending the discussion above, are there any additional considerations for us in using CDR data in this way, not as a replacement to traditional questions, but to create new questions that cannot traditionally be asked?

Data minimisation principle under CDR

As we noted above, the CDR contains a requirement under the data minimisation principles that data needs to be 'reasonably needed' for the intended purpose. It is unclear whether and how this might create barriers for insurers who wish to use CDR data to create novel underwriting questions. Certainly it is not the case that CDR data used in such a manner would be necessary to offer insurance: it is not used today, after all. But a test requiring that data be *'reasonably* needed' to offer some good or service is substantially weaker than saying it must be *necessary*.[12] Is broad and substantial insurer access to consumer data held by banks, telecommunications companies and energy companies 'reasonably needed', merely because an insurer *wishes* to use it to assess risk? Are there some circumstances which are acceptable and some not? When and why? This is unclear to us today, and so far as we have seen in the various policy documents recently published, little thought has been given to whether certain kinds of access or use are unacceptable.

This uncertainty of what is permitted - and what *ought* to be permitted - is not limited to insurance, and we suggest ought to be clarified by further discussion and guidance. We could start by contemplating hypothetical cross-industry data uses within existing designated sectors. For example: is it 'reasonably needed', or not, for a loan application to seek access to electricity consumption data, to decide whether to provide an offer or product feature such as a lower interest rate? Is it 'reasonably needed' for that same electricity provider to request banking transaction data, perhaps to target discounts at the most reliable customers, or those who commonly make use of payment authorisations? We ought to have clear answers to such questions. And we ought to be thinking through the industry and societal *implications* of saying that data is 'reasonably needed'. Are there, for example, customers who are going to miss out on discounts, or be excluded from service or products, as judgments begin to be made about their credit card histories? Consideration of such questions naturally leads onto broader considerations of fairness – a topic we return to below via a stylised example.

Disclosure Requirements under ICA

In this new situation, we are assuming that it would not be practical to offer a traditional form of underwriting question asking for similar information (for example, if the data requested is extremely extensive). Hence the consumer is left to choose between opting into the CDR request, or not sharing data at all. On our reading, the ICA could allow such a request to be extremely broad. This is as a result of recent reforms made to ICA. This would mean that any limits come from the CDR rules: which include what may be only a relatively weak data minimisation principle, for reasons we've described above.

In the ICA, the classic insured's disclosure duty is set out in s 21 ICA, which requires a prospective insured to disclose every matter that they know is relevant for the insurer's decision whether to accept

[12] In this respect, note the contrast between the data minimisation principle articulated in the General Data Protection Regulation (GDPR) in Europe, article 5.1(c), which states that personal data shall be 'adequate, relevant and *limited to what is necessary* in relation to the purposes for which they are processed ('data minimisation')'.

risk. This was recently replaced for consumer insurance contracts by the current duty to take reasonable care not to make a misrepresentation within s 20B.[13] This reform was recommended by the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry,[14] as being more appropriate for consumer contracts and considerably less complex. The Explanatory Memorandum to the Financial Sector Reform Bill pointed out that 'Commissioner Hayne noted it placed the burden on an insurer to elicit the information that it needs and does not require the consumer to surmise or guess what information might be important to an insurer.'[15] Interestingly, CDR data sharing offers precisely that: a prospective insured will not need to 'guess' what information might be relevant, they merely consent to it being provided. Then the insurer will need to extract relevant information from the data received.

At the same time, the 2020 Reform Act[16] repealed rules that applied to 'eligible insurance contracts', on the basis that they were no longer needed.[17] These rules covered certain contracts, such as motor vehicle or travel insurance, and required an insurer to ask *specific and relevant* questions, limiting the insured's duty of disclosure to responding to those questions asked by the insurer.[18] Those older rules prevented insurers from asking 'catch all' questions.

Current law does not prevent insurers from asking broad and extensive questions, which may extend to CDR data requests. The assumption in the 2020 reforms is instead that where questions are open-ended, or long, or broad, then the corresponding duty of the insured to take reasonable care not to make a misrepresentation is lowered - because such questions are harder to answer.[19] The government considered this provided a strong disincentive for asking 'catch all' questions, despite the absence of any express consequences for asking them.[20] However, we argue that in the context of CDR data sharing these rules become inadequate, as data request no longer risks being a question which is difficult to understand or interpret, or long and open-ended. It may be very extensive, but it *does not create any additional difficulty in answering for the insured* - a CDR request is intended to be easy for insureds, by design. The burden therefore is once again shifted away from an insurer: in contrast to 'eligible contracts' rules there is no duty to ask specific and relevant questions. Data requests could therefore be extremely wide-reaching and may not even need to be intuitively relevant (e.g. all transaction data for the last x years).

Note also that there is nothing in the law to prevent an insurer refusing cover if they receive no data, especially if data sharing is an inherent feature of an insurance product offered. Insurers can also price policies and offer terms and conditions dependent on data being shared (or not shared). While we expect that in practice it is likely that - at least initially - products will still be offered if no CDR data is provided (though certainly on different terms, else the practice of asking for the additional data is of no value), we observe again that this challenges the much-vaunted opt-in nature of the CDR regime.

Furthermore, CDR data sharing of this form introduces a new level of opacity to the underwriting process. A traditional questionnaire is significantly more transparent: a prospective insured can certainly see the questions they are being asked and will be likely to understand why they are being

---

[13] *Financial Sector Reform (Hayne Royal Commission Response) Act 2020* (Cth) sch 2 pt 2 ('2020 Reform Act').

[14] Recommendation 4.5.

[15] Draft Explanatory Memorandum, Financial Sector Reform, Hayne Royal Commission Response – Protecting Consumers (2020 Measures) Bill 2020 (Cth), rec 4.5 (Duty of Disclosure to Insurer) ('Explanatory Memorandum') [1.10].

[16] *Financial Sector Reform (Hayne Royal Commission Response) Act 2020* (Cth)

[17] Ibid [1.67].

[18] Repealed ss 21A, 21B.

[19] See also *Insurance Contracts Act 1984* (Cth) s 20B(3)(c), and Explanatory Memorandum [1.37]–[1.38] noting the lower duty because it would be more difficult for an insured to answer 'compound questions that are open-ended, general or long; or questions that are difficult to understand or interpret'.

[20] Ibid [1.39].

asked such questions. But when an individual shares CDR data such as their banking transaction history, do they really know what an insurer (or anyone else) is looking for and how it is being used? As noted previously, the CDR regime suggests some explanation of use should be given to consumers, but it is unclear how extensive this would need to be - it might be permissible merely to state in high level terms that "the data is used for pricing and underwriting along with other data collected during the quote". We suggest that insurers should also concern themselves with whether data generally ought to be used for such purposes, even if it is predictive of claims costs.[21]

Even if we assume that consumers have a degree of control over which data they are sharing with insurers under the CDR regime and which not (which supposes that an insurer would still offer cover to consumers who share incomplete data), the possibility of wilfully hiding certain data (e.g. transaction data from certain merchants) may be limited due to practical factors. We expect that most consumers simply won't spend the time to make specific, granular choices around the data they share. The transparency for insurers when data is shared at all is therefore significantly higher than in traditional questionnaire settings - but for insureds the process becomes more opaque.

In summary, when we use CDR to create new underwriting questions, the *optional nature* of the CDR regime, and its core premise of consumer choice and control is threatened. Additionally, in this scenario, there is an increase in opacity of underwriting to the insured, compared to the use of traditional question sets. In combination, this may incentivise a passive acceptance of mass data sharing on the part of the insured: what is the point of being engaged, when you don't really have a choice about your data use? Again, we suggest this is not in the spirit of the CDR regime, which assumes a more active role of the consumer in deciding which data to transfer, and for what specific purpose.

Consumer Impact - Analysis via a Stylised Insurance Market

We will now examine the impact this sort of innovation may have on consumers in a simple, stylised market, which will then allow us to pose some additional questions about other conduct obligations of insurers, and general questions of fairness.

We begin prior to the CDR, with a simplistic insurance company operating in a simplistic market where everyone pays the same price for cover: $100. Assume that $100 represents the expected costs of claims only, with no allowance for expenses, profits, investment income or other matters such as tax. In a real market there will usually be existing rating factors leading to price variation, and loadings for expenses, profit, etc. Our assumptions do not alter the general conclusions drawn, but serve to simplify the exposition.

Now let us make the following further, simplifying assumptions:

- There are two categories of risk, high and low, which are not directly observed. The expected cost of claims is $120 for high risks, and $80 for low risks. The population is split 50/50 between each risk type;

- CDR data is revealed which can reliably categorise a customer as either high or low risk. We assume no categorisation error, and assume it is objectively fair and reasonable to treat this data as relating to risk that ought to be priced for (which may not always be the case in reality[22]);

[21] For some of our previous considerations on this question, see Dolman et al (2020) "Should I Use That Rating Factor" presented to the All Actuaries Virtual Summit 2020, available at https://actuaries.logicaldoc.cloud/download-ticket?ticketId=dec35c10-44b0-4345-844c-4772da856dba

[22] See eg ibid.

- CDR data is not available at all for 5% of the population (for example new migrants, people fleeing domestic violence, recently released convicts, etc). Again, assume a 50/50 split between low and high risk;

- A further 10% of the population have access to CDR data but cannot make use of it due to lack of digital skills, access or ability. Again, assume a 50/50 split between low and high risk;

- There is 100% market participation, and that coverage is standardised across the population;

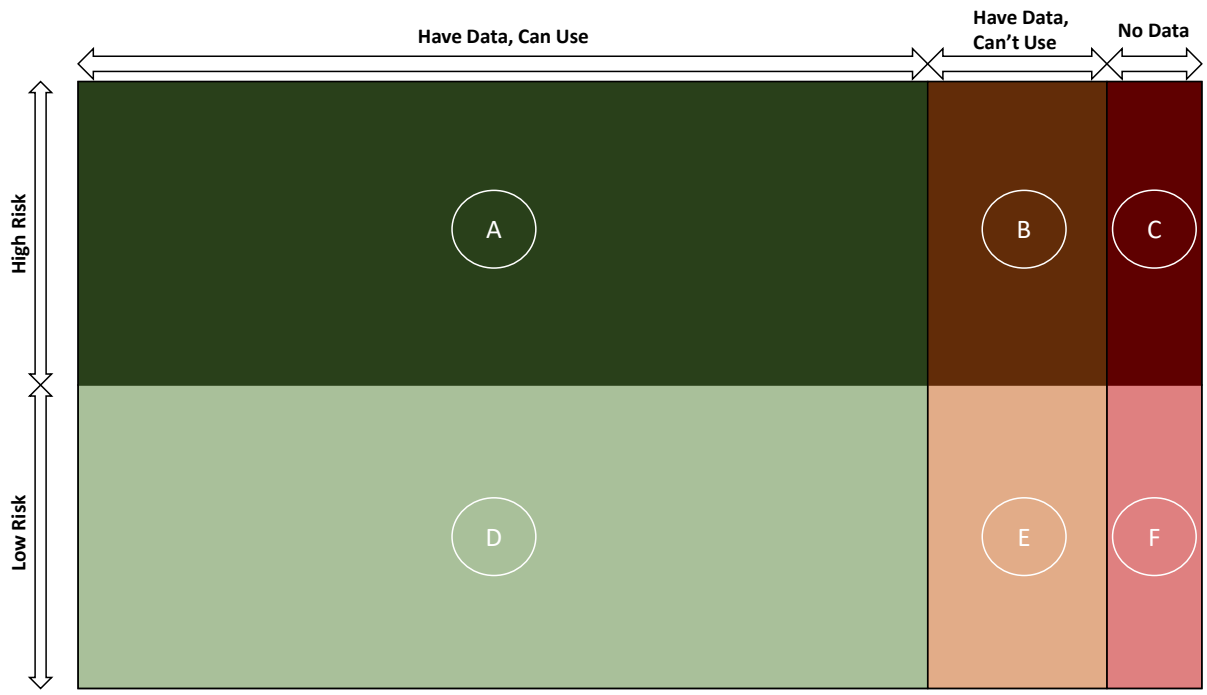
- Insurers act rationally and so wish to use the CDR data to price more accurately. Recognising that not all customers may be able or willing to use CDR, and in line with the CDR rules, insurers give consumers the option to share CDR data with them in order to be priced more accurately. They then adjust prices in line with emerging claims experience for each segment, using 3 rating categories: 'CDR data – high', 'CDR data – low' and 'no data'.

How will insurance prices evolve over the medium term in this environment?

Analysis of Prices

Figure 1 below identifies six sub-populations for analysis.

Figure 1 – Six Subpopulations for Analysis



To consider prices over the medium term in such a market – under the simplifying assumptions made - it is sufficient for us to calculate the size and composition of each of the three rating categories identified: 'CDR data – high', 'CDR data – low' and 'no data'. In the table below, we consider each sub-population illustrated above and identify where it is likely to be situated, before computing the resultant prices for each segment.

Population	Price Category	Rationale
A	No data, potentially a limited number in CDR data – high	Population A is unlikely to share data. If As know they are high risk, they will not wish for this to be used to increase their price, and so will generally not share data unless forced to. If As do not know they are high risk, they will be disappointed with the outcome of sharing their data, and will then simply seek to requote without sharing data (either with the same insurer or an alternate). The result is that their final purchase is likely to be without sharing data.
B	No data	By definition, B falls into the 'no data' segment.
C	No data	By definition, C falls into the 'no data' segment.
D	CDR data – low, potentially some in no data	If population D know they are low risk, they will be highly likely to share data in order to get a better price. There may be a subset of D who choose not to share data, potentially due to privacy or other concerns.
E	No data	By definition, E falls into the 'no data' segment.
F	No data	By definition, F falls into the 'no data' segment.

Let us now use this to compute the average claims costs – and hence prices – of each of our three segments:

Segment	Price	Rationale
CDR Data - Low Risk	$80	This contains only population D. By definition the cost is $80
CDR Data - High Risk	$120	This may contain nobody or may contain a small number of population A which by definition costs $120.
No Data	$114.78	This contains the remainder of the population. Under the assumptions made, low risk consumers in E and F represent 7.5% of the total population, high risk consumers in A, B and C represent 50% of the total (noting this may be slightly changed by any members of A who declare as high risk, or members of D who choose not to share data – we assume both of these situations do not occur, for simplicity). The average cost of claims is then ($120 * 50 + $80 * 7.5) / 57.5 = $114.78.

'Fairness' Questions Arising

This analysis highlights important questions of fairness, particularly for insureds in segments E and F. E and F are *low risk but cannot prove it*, but after this change are forced to pay more for their cover ($114.78) than even the prior state ($100), and certainly more than the 'fair' price for their risk ($80). Their price moves away from the risk price due to greater societal availability of data, not closer to it as many might intuitively believe. We note that these segments are more likely than the average to be considered vulnerable customers, since vulnerability is often correlated with lack of access to digital services and historic data.

Are things 'fairer' if optionality is removed?

Optionality is core to CDR, but as we noted above it might be challenged in practice. So let us examine its removal to see if this may resolve some of the challenges above. Without optionality, segment A must declare as high risk, or else get no cover. The price for the 'no data' segment becomes the average price for those without data – if no response is allowed at all. In our example, this is $100, but in some other situations this may skew towards either the high or low price, which may raise fairness questions.

With no optionality, significant challenges may now exist for segments B and E who may struggle to share the data which exists. Potentially, challenges exist for all of B, C, E and F if a non-response is met with refusal of cover – if adopted as standard industry practice, this would carry a substantial social cost.

However, if any form of 'legitimate' non-response is allowed to partially remedy this issue (e.g. via a declaration of no data being available, for segments C and F), members of Segments A and B might then attempt to fraudulently declare that no data exists, to access a cheaper price. This undermines the goal of removing optionality and will result in a reversion - at least in part - to the first state above.

What happens if everyone can actually answer the question (equivalently, if data is universally available)?

Here, effectively we are assuming only segments A and D exist, but that sharing data is still optional. In this situation we again end up with segment A having no desire to share data, but then rated as high risk in any case due to claims experience of the 'no data' segment, which is mainly, potentially only, As. Segment D are rated as low risk but must answer the question else face a significantly higher price – again this undermines optionality of CDR.

If we revert to mandatory data sharing with universally available data, this is essentially in line with traditional insurance underwriting questions. As and Ds must share their data, are correctly classified and (assuming it is objectively fair to use the data to rate the business), no serious fairness questions can be alleged.

We can see from this discussion that these two features of CDR: optionality of data transfer, and non-universal ability to share that data, will create some significant social challenges in insurance underwriting, likely exacerbating issues of affordability, particularly for vulnerable customers. We note that these are core design principles of the CDR. While our example focussed on insurance, it is general in nature: it is *inherent in the idea of detailed consumer data being used for pricing* - and so the issues of fairness, and the undermining of optionality are likely to generalise to other forms of personalisation, particularly economic personalisation.

How does this relate to broader conduct obligations of insurers?

Above, we have identified a series of fairness problems arising from the use of CDR to create new underwriting questions. In trying to resolve these challenges through making data sharing compulsory, or assuming it is always available, challenges of various forms still remain unless we abandon all of these core features of CDR.

Since this raises questions of fairness, individual insurers will need to carefully consider broader conduct obligations they are subject to. In particular, how might such conduct be interpreted under requirements such as the duty of utmost good faith (UGF) or the duty to provide services efficiently, honestly and fairly (EHF)?

Commentators suggest that UGF can be seen as simply a form of commercial morality.[23] According to Australian law, as set out in *ASIC v Youi Pty Ltd* [2020] FCA 1701, the duty of UGF may require an insurer to act consistently with 'commercial standards of decency and fairness', with due regard to the interests of the insured. Lack of honesty is not considered a prerequisite to breaching the duty, as capricious or unreasonable conduct will also constitute a breach. The duty, being of utmost good faith, requires more than mere good faith and will usually require affirmative or positive action. Although *Youi* was concerned with claims handling by an insurer, and not pre-contractual good faith, the same general principles may apply in the context discussed here. Hence an insurer will need to ask if setting higher prices or refusing cover for prospective insureds who will not (or cannot) share their data in what purports to be an optional data-sharing regime, could amount to a breach of the insurer's UGF duty.

The EHF requirement is quite similar to the duty of UGF. An important distinction is that UGF focuses on a conduct towards one concrete insured, while EHF considers the business as a whole, 'looking at the licensee's behaviour more generally rather than with regard to any one person'.[24] There has been some discussion whether the obligation to act EHF is a compendious one. It seems that it is still regarded as such by the courts:[25] i.e. a person should 'go about their duties efficiently having regard to the dictates of honesty and fairness; honestly, having regard to the dictates of efficiency and fairness, and fairly, having regard to the dictates of efficiency and honesty'.[26] To summarise the effect of the cases, *efficiently* means adequate in performance, and imposes a competency or reasonable standard of performance requirement. *Honestly* refers to a conduct which is morally right, ethically sound. An important feature of *fairness* is that it is to be judged having regard to the interests of both parties, not only the insured: so the insurer can act in their own interest as well.[27] Importantly, the principal focus is on process, not outcomes, so it is primarily on actions taken by the licensee to provide financial services efficiently, honestly and fairly, to 'do all things necessary'.[28]

In our hypothetical example, arguably, prices are being set on a sound actuarial basis, using a clear, explainable and justifiable methodology. Unless consumers are misled in some way then there are no obvious grounds for claiming commercial dishonesty. The fairness requirement allows insurers to act in their own interest, providing they consider the interest of insureds as well. Therefore, if the government adopts 'open finance' and invites insurers to offer new or refined products designed to take advantage of the CDR for the benefit of (some) consumers, an insurer cannot be considered as acting unfairly for doing just that.

It is worth highlighting, however, that this is in part a result of our assumptions. We assumed, for example, that CDR data is revealed *which can reliably categorise a customer as either high or low risk.* To the extent that CDR data is poor quality, or lower quality for particular groups of consumers, fairness issues could still arise. We also assumed that it is *objectively fair and reasonable to treat this data as relating to risk that ought to be priced for*, and we want to emphasise this may not always be true. The more detailed the data available; the more advanced the analytics applied; the less intuitively the data relates to risk or reflects factors within the control of the prospective insured, the more carefully, we would argue, insurers will need to consider whether its use does comply with these broadly based duties of insurers.[29]

---

[23] Frederick Hawke, 'Utmost Good Faith — what does it really mean?' (1994) 6 *Insurance Law Journal* 91, 142.

[24] *ASIC v AGM Markets Pty Ltd (in liq)* [No 3] (2020) 275 FCR 57

[25] Ibid.

[26] *Story v National Companies and Securities Commission* (1988) 13 NSWLR 661

[27] M Scott Donald, 'Regulating for Fairness in the Australian Funds Management Industry' (2017) 35(7) *Company and Securities Law Journal* 406, 411.

[28] Leif Gamertsfelder, 'Efficiently, honestly and fairly: A norm that applies in an infinite variety of circumstances' (2021) 50 *Australian Bar Review* 345, 350.

[29] See eg ibid.

We suggest that discussion between industry, regulators, and consumer representatives, as well as regulatory guidance on the interpretation of these general provisions in the context of CDR would be valuable, so as to give clarity to the industry as to the conduct expected of it, and to develop a broader societal understanding of what is and isn't appropriate and acceptable.

What of market effects?

The sorts of outcomes illustrated by our stylised case study are not only driven by the actions of individual firms. If new products emerge, for example through new providers, low risk insureds who are able and willing to use data may migrate to them. Indeed, *this is a core objective of the CDR regime.* However, this then leaves higher risk insureds or those less able or willing to use data with traditional, legacy products. These products would then need to be repriced accordingly. While no individual firm can be held to be breaching their EHF or UGF requirements, the market as a whole shifts in a manner similar to that which we identified above, to the disadvantage of those most vulnerable and less able to participate in the digital economy. Conduct regulation which applies only to individual firms will not be sufficient to prevent such outcomes.

Conclusion

The CDR regime is centred on individuals, who are given rights over certain types of data in order to act to improve outcomes for themselves, if they so choose. However, providing rights to individuals does not only affect those individuals - it can have an impact on the broader community.[30] In this paper, we illustrate this by highlighting fundamental flaws and conflicts in this model when applied to the insurance sector. Though it is beyond our scope, we suggest these issues are not specific to insurance and similar problems will exist across many other sectors.

First, we considered whether CDR-based underwriting might be permitted as a replacement or augmentation of traditional underwriting question sets. We found no substantive legal barriers to this within either CDR or the existing ICA regime. There are still many unanswered questions, and some practical challenges to work through which may result in some restrictions on insurers' conduct, but in general no substantial legal barriers appear to exist which would prevent CDR data being used for underwriting.

Second, we identified inherent conflicts between the core principle of optionality of the CDR regime and both the disclosure regime of the ICA, and common practices of insurers which CDR is unlikely to change. Without reform, it seems likely that the long-term result will be that data sharing via CDR becomes de facto compulsory for an insurance quotation – or at least a competitively priced one. Not only does this lead to poor outcomes for those without access to data or the ability to leverage their new CDR rights via digital tools, it is inconsistent with the spirit of the CDR regime which has optionality at its core. This suggests that review and potential reform of the optionality principle is required, in light of likely market practices.

Finally, and perhaps most troublingly, we identified a clear potential for detriment to consumers who are unable or unwilling to share data via CDR for insurance pricing and underwriting. While conduct obligations do exist in the industry, these operate at the level of an individual firm. Even if such obligations might restrict individual firms acting in such a manner (which seems doubtful), they cannot act to prevent such outcomes which inevitably arise purely through market forces, competition and the age-old effect of adverse selection. We argue, on this basis, that a serious and urgent discussion

[30] See generally Salomé Viljoen, 'Democratic Data: A Relational Theory For Data Governance' (2020) 131 *Yale Law Journal* 573. For a shorter and more accessible summary of the ideas around the collective impacts of data choices, see Tennison, Jeni, 'Individual, Collective and Community Interests in Data', *Jeni's Musings* (27 December 2020) ***http://www.jenitennison.com/2020/12/27/individual-collective-community.html***

needs to be had, about the extent to which we are prepared to tolerate the effects of market forces in this way.

Here is not the place for a developed set of proposals. But we have begun to think about these questions.[31] One promising avenue for reform to prevent such outcomes – which would be most keenly felt by already vulnerable and disadvantaged consumers – is within the CDR regime itself, through reform of the data minimisation principle. Perhaps, for example, it could be split into two. On one hand, this could be designed to readily accept use cases which require CDR data as a genuinely essential feature for the product or service to exist at all (a much higher bar than 'reasonably needed'): this would cover, for example, collection and use of product data for the purposes of comparing deals available in the market. Then for personalisation use cases (such as insurance pricing), where data may be 'reasonably needed' to facilitate the intended personalisation but the personalisation itself is not essential to the general product offering and might cause some detriment to some community members, more emphasis could be given to considerations of fairness across and between customers before such use cases are permitted. This would mean that CDR would have to reorient itself away from individual rights and an emphasis on individual outcomes, towards broader consideration of the effects of data availability on markets and whether those effects are fair to consumers in general, with particular emphasis on vulnerable or disadvantaged consumers. We think this would be a positive move for the community.

[31] We suggest that interested readers 'watch this space' - this paper is one part of an ongoing collaboration around issues relating to data, insurance, and artificial intelligence.