Treasury

Review of the Consumer Data Right PIA – Consulting report

Version 1.0

Stephen Wilson
Lockstep Consulting
January 2019

PUBLIC

Consulting report

Review of the Consumer Data Right PIA

Version 1.0
For the Treasury
[Lockstep Treasury CDR PIA QA Report (1.0.1)]

Stephen Wilson

ABN 17 582 844 015

PUBLIC

Lockstep Consulting (est. 2004) provides independent research, analysis and advice on digital identity, privacy, cyber security policy and strategy, and e-business risk management.

http://lockstep.com.au

Table of Contents

Executive Summary

Lockstep Consulting was engaged by the Treasury to undertake an independent review of the initial Consumer Data Right Privacy Impact Assessment published by Treasury in December 2018 [5]. This review is timed to help inform parliamentary committees due to consider the CDR legislation in early 2019.

Lockstep finds that Treasury's initial PIA is a thorough and carefully considered analysis. Treasury's chosen approach to the PIA borrows from security Threat & Risk Assessment methods, in which adverse events are analysed in terms of likelihood and consequences. This treatment is unusual for a PIA yet certainly worthwhile, provided it is clearly explained to external stakeholders who may be accustomed to a more qualitative assessment against external privacy principles. Lockstep recommends that Treasury follow through on its risk-orientated assessment by setting out for further consideration what the department considers to be acceptable levels of residual privacy risks, and planning for ongoing risk management processes to monitor how known and unknown privacy threats play out in practice as the CDR regime develops.

This report includes a detailed review of the PIA's estimates of privacy threat likelihoods and consequences, and an assessment of the Treasury's proposed CDR privacy risk mitigations. Lockstep makes specific recommendations for the current version of the PIA, future iterations of the document, and for CDR privacy in general. Chief amongst our recommendations are the following:

- The PIA should be updated as soon as the current draft ACCC CDR Rules are ratified, and when the information security standards are stable.
- Information security standards under development for CDR should include mutual authentication, access controls, internal audit tools, and encryption key management.
- The likelihood of identified privacy risks would be better considered at the group level rather than the individual level, in light of the system-wide impacts of such threats as unauthorized disclosure of CDR data, should they occur.

Glossary

Abbreviations

ABA	Australian Bankers Association
ABAC	Attributes-Based Access Control
ACCC	Australian Competition and Consumer Commission
API	Application Programming Interface
APP	Australian Privacy Principle
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
DSB	Data Standards Board
FIDO	*An authentication protocol industry standards body*[1]
IDM	Identity Management
ISTRA	Information Security Threat & Risk Assessment
ISMS	Information Security Management System
KYC	Know Your Customer
LACS	Logical Access Control System
MFA	Multi Factor Authentication
MITM	Man In The Middle [attack]
OAIC	Office of the Australian Information Commissioner
OBR	Open Banking Review
OTP	One Time Password
PACS	Physical Access Control System
PbD	Privacy by Design
PC	Productivity Commission
PI	Personal Information
PIA	Privacy Impact Assessment
PKI	Public Key Infrastructure
RBA	Reserve Bank of Australia
RBAC	Role-Based Access Control
TRA	Threat & Risk Assessment
UI	User Interface
UX	User Experience
2FA	Two Factor Authentication

Other terms

Mutual Authentication	A security measure where the end user of a resource is authenticated by the resource owner or controller, as well as the resource being authenticated by the end user, to prevent fake websites or, in the case of CDR, fraudulent registration of participants or tampering with the Accreditation Register.

[1] The definition of the acronym "FIDO" is of historical interest only; interested readers should refer to see www.fidoalliance.com.

Introduction

Lockstep Consulting was engaged by the Treasury to undertake an independent review of the initial Consumer Data Right Privacy Impact Assessment published by Treasury in December 2018 [5].

Terms of Reference

In its Approach to Market TSY RFQ 013/19, Treasury called for consultancy services to:

> *[Undertake] a critical assessment of PIA version 1, and work with Treasury staff to revise the document to incorporate their comments. The Supplier should consider whether there are outstanding issues that should be addressed in the PIA, and upon direction by Treasury prepare text to address these. In reviewing PIA version 1, the Supplier should place a particular focus on the PIA's assessment of risks associated with the CDR, proposed mitigants for those risks, and on the recommendations made by the PIA.*

Background

The Consumer Data Right (CDR) is a new regime, borne out of the Open Banking Review [1], with the primary aim to:

> *give consumers the ability to access more information about themselves, and about their use of goods and services, in a manner that allows them to make informed decisions about both themselves and their participation in the market. By doing so, the CDR aims to increase competition in any market, enable consumers to fairly harvest the value of their data, and enhance consumer welfare.*

The CDR introduces a comprehensive suite of coordinated measures including:

- legislation drafted by Treasury [2][3][4]
- data safeguards built into the legislation
- detailed rules being developed and to be overseen by the ACCC [6]
- new oversight responsibilities for OAIC
- technical standards for data sharing APIs and information security, being developed through a largely open process by Data61
- an accreditation regime for organisations managing consumer data under the auspices of the legislation.

Treasury on behalf of the whole regime undertook the first Privacy Impact Assessment of the CDR, at a relatively early stage, with the intent of informing parliamentary committees which will consider the legislation in early 2019. In turn, Treasury sought this external expert input to the draft PIA, before it was finalised.

Recent developments in the rules

Important changes to the ACCC's draft CDR rules occurred over the course of this engagement, affecting some of the PIA. For example, after the draft PIA was published, the ACCC proposed in its December release of the rules [6] to preclude CDR data being transferred outside the CDR system, to non-accredited recipients. That is, the CDR will initially be a closed system.

This closure is an important new privacy mitigation, not included in the PIA under review (see p104 [5]). Lockstep generally has tried to factor in late changes as far as they are known to us. We have tried not to make observations on the PIA that are obsoleted by these sorts of more recent developments.

Important disclaimer

The consulting advice in this document does not constitute legal advice and should not be construed or relied upon as legal advice by any party. Lockstep Consulting is not a law firm. No legal professional privilege applies to this report.

The PIA methodology

It is said that the Consumer Data Right PIA was prepared in accordance with the Australian Government's APP Code and the OAIC *Guide to undertaking privacy impact assessments* [11]. These guidelines are not especially prescriptive; they allow discretion in the way a PIA is undertaken and how it is reported. In Lockstep's experience there is a reasonably uniform pattern to most PIAs seen in Australia, and therefore some broad expectation about the content. The CDR PIA deviates from what we view as the norm.

Threat likelihood and severity

Typical PIAs include a thorough examination of how features of the system impinge upon a relevant set of regulatory principles (naturally the APPs in the case of a national project). The CDR PIA does not benchmark the system against any existing principles as such, as the CDR Privacy Safeguards replace other legislated privacy principles.

Further, the PIA is highly novel in the way it enumerates particular *threats*[2] to privacy and gauges the overall risk of each threat according to estimated likelihood and consequence. This sort of treatment is commonplace in security *Threat & Risk Assessments* (TRAs) but in Lockstep's experience rarely if ever features in PIAs. Lockstep does not object to this variation, for we have advocated similar approaches to "privacy engineering" [12]. In our judgement, Treasury's attempt to rate the severity of threats to privacy is worthwhile. By the same token, we suggest that a novel approach like this needs to be carefully couched and introduced to readers so they are not distracted.

Ongoing risk management

Since the CDR PIA adopts the methods of security risk estimation, Treasury should consider going further by giving consideration to the *acceptable residual risk* for each identified threat. It is customary for a security TRA to set out what risk level is deemed acceptable. The process of deciding what risks are acceptable, if undertaken collaboratively across all stakeholders, can itself be instructive, for it will help socialise how a new system is expected to behave, and build better shared understanding.

In reality, a new system will often involve threats which are still predicted to exceed the acceptable limits even after the application of agreed mitigations. In those cases, a system operator should put additional management processes in place, to monitor how threats pan out, keep up

[2] Let it be noted that the term *risk* is actually used in the PIA for adverse events that could harm privacy, whereas the standard terminology in threat & risk assessment is *threat*. Conventionally, risk is a measure of the seriousness of a threat, gauged by combining the likelihood of the threat occurring and the seriousness of the consequences if it does. Lockstep uses the term *threat* in this report for events that Treasury has called risks.

the management visibility of risks, support decisive action in response to real threat events, provide feedback to the TRA process itself, and maintain records to prove the organisation's good planning and preparedness. Typically a large program will have a *Risk Committee* or equivalent that periodically considers all residual risks deemed to exceed acceptable limits and oversees ongoing corrective actions and continuous improvement.

We also have additional detailed comments below on the risk estimates.

Adverse events versus intended operation

According to the OAIC guidance, a PIA aims to show if and how a given project "meets legislative privacy requirements and community privacy expectations" [11]. By focussing on threats (i.e. adverse events), the CDR assessment so far tends to avoid consideration of the privacy impacts of the CDR regime *when it is operating as intended*. We suggest that additional analysis be undertaken to baseline the impact of consumer privacy of the CDR, which could be expected to be largely positive, thanks to the new legislated safeguards (and the consent rules in particular), new data security standards, and the accreditation requirement.

Review of the PIA's Risk Assessment

General remarks

The PIA is said to use a modified form of Treasury's risk rating matrix. At Table 4 (pp 48-49 [5]), likelihood and consequence ratings are described along with guidance provided, including the following descriptions:

> *Likely:* *The risk to the individual/business will probably eventuate within the CDR system*
>
> *Possible:* *The risk to the individual/business may eventuate within the CDR system*
>
> *Unlikely:* *The risk to the individual/business may eventuate within the CDR system at some time but is not likely to occur*

Lockstep finds the qualitative gauges of likelihood lack a little precision. In other TRAs, it is common for likelihood to be calibrated, at least approximately, through guidance such as a "likely" event being expected to happen once a month and that an "unlikely" event is not expected to happen more than once annually.

Scope of likelihood estimation

Estimating likelihood is not an exact science, and assumptions must be made about the scope of events that are considered. The PIA is clear in that regard. See for instance:

> *The likelihood of risks arising was assessed with regard to an individual participating in the CDR over a given year and across multiple interactions with multiple data recipients and data holders. The likelihood assessment **does not** reflect the probability of harm per interaction with the system. Adopting such an approach generally resulted in a 'rare' assessment against each risk and therefore did not provide meaningful information to a reader seeking to assess the level of a given privacy risks.* [5] p59 (emphasis in original).

That is, the assessment examines the likelihoods that threats will occur to an individual over a period of one year across all multiple transactions, rather than the likelihood of threats occurring per transaction; otherwise all estimated likelihoods would be rare and the analysis would not be instructive. Lockstep finds this to be reasonable.

On the other hand, the PIA confines itself to threats occurring to individuals as opposed to groups, or the whole population:

> "Note also that if risks were assessed at the group level, this may increase the likelihood and/or severity attached to those risks."

We understand the point being made that likelihoods estimated at the group level might become too high to be useful, but on the other hand, Lockstep sees merit in considering group level consequences.

Consider a particular type of risk, the "inside job", where corrupt employees at institutions access consumer data inappropriately. Experience shows that this risk is commonplace, and across the whole group, could reasonably be expected to happen at least once a year. That is, the threat would be rated as "Likely" or "Almost Certain". While it is true that the likelihood of any *given* consumer being affected by an inside job would be much lower, the severity of the effect on the whole system should still be considered. Table 4 of the PIA is concerned in part with *reputational damage* suffered by individuals *and businesses too*. An insider attack within a participating institution, even if confined to one individual consumer, would have systemic implications for security. It would certainly shake confidence in that participant, and in the whole CDR system, especially in the early days of the scheme. Therefore such an event could be reasonably rated as having "Major" consequences.

We provide further commentary on group versus individual likelihood in the table below.

There is no single correct or standard way to estimate likelihood in a TRA (or indeed in a PIA), and we acknowledge the good job Treasury has done in clearly setting out its approach. However we recommend that the impact of privacy threats generally be gauged at the *group* level, so that a more cautious risk assessment is achieved, and clearer priorities are assigned as a result to mitigating actions.

Comments on the risk estimations

This section combines most of the content of Tables 5 and 7 of the PIA, and adds Lockstep's critical comments (as grey coloured extra rows) regarding the risk estimations, and the efficacy of the PIA's proposed mitigations.

#	Threat	Likelihood	Severity	Risk	Mitigation	Likelihood post mitigation
1.1	A third party may pose as the accredited data recipient in order to acquire the individual's authentication information.	Possible	Moderate	**Medium**	Primary: Misleading or deceptive conduct offence, holding out offence, Education Other: 19, 15, 6, 8, 4, 14, 9, 20, 21, 24, 7	Unlikely
		The reputational damage from successful faking of an accredited Data Recipient could be worse than Moderate.			*None of the mitigations actively prevent fraudsters impersonating accredited recipients. Lockstep suggests that risks with actual financial impact should be mitigated by a mix of legal and technological controls.* *We understand that mutual authentication of the Accreditation Register is under consideration by the Data Standards Body, with the aim of digitally certifying the status of registered entities. That would (1) enable CDR Participant software to programmatically verify that a Data Recipient is properly registered, and (2) make it difficult to tamper with the register.* *Mitigation 4 (accreditation) does not apply because the threat is that accreditation is bypassed.* *Mitigation 14 (Accreditation Register) doesn't actively mitigate the risk because a fraudster will tamper with the register.*	*Possibly optimistic.*

1.2	The individual may use a false identity to acquire authentication information from the accredited data recipient	Possible	Moderate	**Medium**	Primary: Misleading or deceptive conduct offence, Education Other: 19, 15, 6, 8, 4, 14, 9, 20, 21, 24, 7	Unlikely
	In other words, "identity theft" of the individual.	*We agree with the estimated risk.*			*None of the mitigations actively prevent fraudsters impersonating individuals or taking over their logon credentials. Legal mitigations are important but experience in Internet financial crimes suggests that the CDR regime will attract identity thieves.* *We appreciate that user authentication is a work in progress of the standards body. We recommend that state-of-the-art multifactor authentication such as FIDO Alliance protocols be considered.*	*Optimistic.*
1.3	The individual may engage an accredited data recipient who instead seeks data outside the CDR system.	Possible	Minor	**Low**	Primary: Misleading or deceptive conduct offence, Holding out offence, Education, Accreditation requirements Other: 19, 5, 6, 7, 8, 9,10, 24	Unlikely
			Agreed.			
2.1	The individual may authorise the accredited data recipient to use or collect their data in a way that they did not genuinely intend.	Almost Certain	Minor	**Medium**	Primary: Consent requirements based on user testing, restrictions on direct marketing Other: 4, 17, 11, 5, 9, 7, 18	Unlikely
		Agreed.			*We agree with the measures but recommend more cautious expectation management. Informed consent is predicated on complete transparency of how digital companies put data to use, and experience shows that these types of business are highly reluctant to disclose their Big Data processes. It may take some time for regulations and education to take effect.*	*Optimistic.*
2.2	The individual may inadvertently authorise a level of access or use of their data beyond what is required for the services they are seeking.	Almost Certain	Minor	**Low**	Primary: Consent requirements based on user testing, Rules, Standards Other: 10, 15, 16, 17, 11, 5, 8, 9, 7, 18	Unlikely

		Agreed.			*See 2.1 above.* *We note that the User Experience (UX) of data usage consent is likely to be complex and novel. We expect a lot of experimentation in the design of e.g. consent and user data dashboards. We should not expect sudden improvements in these risks.*	*Optimistic.*
2.3	The information that the individual discloses in the course of seeking services may be used or disclosed by the accredited data recipient without authorisation.	Possible	Minor	**Low**	Primary: Rules, Privacy Act, Other: 11, 4, 5, 9, 7, 8	Unlikely
			Agreed.			
2.4	The accredited data recipient may use the individual's data in an unauthorised manner.	Possible	Moderate	**Medium**	Primary: Privacy Safeguards Other: 4, 3, 17, 6, 8, 3, 11, 5, 9, 7, 18	Unlikely
		We suggest that Major damage to confidence in the CDR regime would result from unauthorised use or disclosure of data by an accredited recipient, because the whole point of the regime is to restrain such data flows.			*Awareness campaigns for Data Recipients are consumers alike will be crucial.* *Because the CDR regime is expressly intended to restrain the unauthorised use and disclosure of consumer data, we recommend that government commit to strong legal action against offenders, and possibly a zero-tolerance approach.*	*Optimistic.*
2.5	The accredited data recipient may limit the individual's free choice by including contract terms that require access to the individual's data in exchange for a service.	Almost Certain	Minor	**Low**	Primary: Privacy Safeguards, genuine consent requirements, Rules, use restrictions Other: 11, 4, 5, 6, 7, 8, 9, 18, 13	Possible
		We only observe that the prospects of participants inflicting adverse contract terms is probably similar to that of creating less-than-ideal consent experience. Therefore the estimates for 2.5 seem inconsistent with other risks above.			*Awareness is crucial.*	*Inconsistent with 2.1, 2.2 etc.*

2.6	A non-accredited data recipient may request that the consumer access and download their own CDR data in exchange for a service.	Likely	Moderate	**Medium**	Primary: Rules, Privacy Act, education	Possible
Agreed.						
3.1	The accredited data recipient may direct the individual to a fake website posing as the data holder's website.	Unlikely	Extreme	**High**	Primary: Misleading or deceptive conduct, Privacy safeguards Other: 4, 19, 15, 17, 5, 6, 7, 8, 9, 3, 20, 21, 22, 24, 18	Unlikely
	We would seek clarification of whether this possibility represents an accredited data recipient perpetrating a deliberate fraud, or whether it is contemplated that the data recipient is hacked to redirect the consumer to a fake site.	*We agree with the estimates.*			*We suggest that if Treasury does not anticipate these mitigations reducing the likelihood (or severity) of threat 3.1, then the list of mitigations (4, 19, 15, 17 etc.) should be dropped from this row. The PIA should not be padded out with generic mitigations that are not expected to have significant positive impact.* *If threat 3.1 has to do with hacking or tampering with an accredited Data Recipient, then Mitigation 2 (information security standards) is more relevant here than any other mitigation. We suggest that the information security standards work be checked to make sure that explicit protections against hacking and tampering are indeed in scope for the DSB, and that standards working groups be alerted to the expectation that their deliverables will mitigate threat 3.1.*	
3.2	A third person [sic] may pose as the accredited data recipient to gain access to the individual's consent information from the individual	Possible	Extreme	**High**	Primary: Commonwealth Criminal Code, State criminal laws, Holding out offence, Misleading or deceptive conduct Other: 19, 18, 4, 5, 6, 7, 8, 9	Unlikely

	We are unsure precisely what constitutes "consent information" and whether the more general and serious threat concerns CDR data. The term is not defined in the PIA and is not used often.	*Suggest revision after clarifying which data is under threat.*				
3.3	A third person [sic] may intercept an individual's authorisation as it is sent to the data holder.	Rare	Extreme	**Medium**	Primary: Commonwealth Criminal Code, State criminal laws, Privacy Safeguards, Standards Other: 19, 4, 5, 6, 7, 8, 9	Rare
	In other words, a "Man in the Middle" attack on the consumer using the CDR system.	*We do not believe there is sufficient information to make a robust estimate of the likelihood, neither before nor after mitigation. However, the estimate seems optimistic; password interception in Internet banking is arguably more frequent than "rare".*			*Mitigation 2 (information security standards) is relevant here, and perhaps more important than any other mitigation.*	
3.4	The individual may unintentionally authorise the disclosure of the wrong data to the accredited data recipient.	Possible	Minor	**Low**	Primary: Regulators' powers, genuine consent requirements Other: 10, 11, 5, 6, 7, 8, 9, 18	Unlikely
		The consequences of this type confused UX could be more serious, given that consent and authorisations are the bedrock of CDR, and can be expected to be difficult issues to get right.			*See 2.1 and 2.2 above.*	*Optimistic.*
3.5	The individual may accidentally authorise a level of access to their data beyond what is necessary or required for the services they are seeking.	Possible	Moderate	**Medium**	Primary: Rules, Other: 11, 18, 17	Unlikely
		We would expect the estimated likelihood and consequences of this threat to be the same as 3.4.				

3.6	The individual may unintentionally authorise the disclosure of the right data to the wrong accredited data recipient	Unlikely	Moderate	**Low**	Primary: Standards, Privacy Safeguards Other: 11, 14, 15, 17, 18	Rare
			See 3.5.			
3.7	The individual's authorisation to disclose data may not be received by the data holder.	Possible	Minor	**Low**	Primary: Standards Other: 5, 9, 17, 18	Unlikely
		We agree with the estimates.			*The main mitigation here should probably be security measures, to ensure a verifiable handshake protocol when authorizing data transfers.*	
3.8	A third person [sic] may pose as the individual and authorise disclosure of data.	Unlikely	Extreme	**High**	Primary: Misleading or deceptive conduct, Privacy Safeguards, Rules, Commonwealth Criminal Code, State criminal laws Other: 19, 4, 5, 6, 7, 8, 9, 17,	Unlikely
	In other words, "identity theft" of the individual.	*We would expect the same estimates as for Risk 1.2, which is another case of end user identity theft.*			*See 1.2 and our recommendations for strong authentication of consumers.*	.

3.9	The data holder may improperly use or disclose the authorisation itself.	Likely	Minor	**Low**	Primary: Rules, Privacy Safeguards Other: 19, 10, 15, 16, 17, 5, 6, 7, 8, 9, 3, 11,	Unlikely
		Are we correct to view the focus of CDR on Data Recipients rather than Data Holders? It appears that Data Security Standards and accreditation are aimed at Recipients not Holders. *If improper use of data is thought to be likely, then the public might not view this as substantially different from and more acceptable than improper use by Data Recipients, and therefore the estimate of Minor severity and Low risk would be overly generous.*			*There could be a case for CDR accreditation to apply equally to Holders and Recipients.*	.
3.10	The data holder may seek alternative or additional information from the individual during the disclosure that is not required for the primary purpose of data transfer.	Likely	Minor	**Low**	Primary: Privacy Safeguards, genuine consent requirements, Rules Other: 19, 10, 15, 16, 17, 5, 6, 7, 8, 9, 13, 24.	Unlikely
Agreed.						

3.11	The data holder may obstruct or dissuade the individual from transferring their data to the accredited data recipient.	Possible	Minor	**Low**	Primary: Privacy Safeguards, Rules, Standards Other: 19, 5, 6, 7, 8, 9, 4, 18	Unlikely
	"Obstruct" might be too strong a word, but our review of the CDR public submissions certainly suggests that some Data Holders will feel entitled to dissuade customers from moving their data, for security reasons at least.	*Lockstep suggests the consequence of the threat should it occur is higher than "Minor". If the very objective of CDR is to facilitate and encourage data transfers. Any instance where a consumer's desire to move data is thwarted by a Participant would be regarded as a violation of the CDR objectives and therefore would damage the CDR's reputation. We suggest the consequence be rated "Major" because we predict "significant reputational damage" to the government (Ref: Table 5 [5]).* *Relatedly, the decision of the PIA authors to gauge severity according to the probability of harm being done in a 12 month period to a given individual (ref: p59) could be reviewed. In order for the PIA to guide mitigations to protect privacy, then the it might be better to consider the likelihood of threats occurring in the system as a whole, and acting according to the systemic reputational (and other) damage that would result.*				

4.1	The data holder may accidentally send the wrong individual's data to the accredited data recipient.	Unlikely	Moderate	**Low**	Primary: Privacy Safeguards, Standards, Tort of Negligence Other: 5, 6, 7, 8, 9, 4, 17, 22	Rare
		The reputational damage to Participants and to the CDR program itself from such a mistake would, in Lockstep's view, be "Major", not "Moderate". CDR data is highly sensitive, and consumers will reasonably expect this sort of mistake to be very rare. Misdirecting sensitive data is one of the worst case scenarios in the mind of the public. If it happens at all, confidence in the CDR regime will be sapped.			*Security standards (Mitigation 2) should be primary amongst the mix of mitigations here. Handshake protocols and integrity checks should be included to ensure data is not misdirected, and that transferred data matches the request.*	
4.2	The data holder may accidentally send the individual's data to the wrong accredited data recipient.	Unlikely	Moderate	**Low**	Primary: Privacy Safeguards, Standards, Tort of Negligence Other: 5, 6, 7, 8, 9, 4, 17, 22	Rare
See 4.1.						
4.3	The data holder may accidentally send the wrong individual's data to the wrong accredited data recipient.	Unlikely	Moderate	**Low**	Primary: Privacy Safeguards, Standards, Tort of Negligence Other: 5, 6, 7, 8, 9, 4, 17, 22	Rare
See 4.1 and 4.2.						
4.4	The data holder may intentionally or unintentionally fail to send any, or complete data to the accredited data recipient.	Possible	Minor	**Low**	Primary: Privacy Safeguards, Rules, Tort of Negligence Other: 5, 6, 7, 8, 9, 4, 17, 22	Unlikely
See 4.1, 4.2 and 4.3.						

4.5	The data holder may intentionally or unintentionally send inaccurate data.	Possible	Moderate	**Medium**	Primary: Privacy Safeguards, Misleading or deceptive conduct Other: 5, 6, 7, 8, 9, 4, 17, 18, 22, 23	Unlikely
	We recommend that intentional and unintentional transmission be separated because the respective causes and mitigations are distinct.	*It is hard to estimate these likelihood of these threats without knowing more about the contemplated causes or threat vectors.* *We suggest that intentional transmission of inaccurate data would be judged by consumers to more severe than "Moderate".*			*Mitigated likelihood needs to be separated for intentional and unintentional. We suggest data holders who would intentionally send inaccurate data are knowingly acting unlawfully and as such may not be curbed by any regulatory measures.*	
4.6	The data holder may intentionally or unintentionally fail to send the data in a timely manner.	Possible	Minor	**Low**	Primary: Privacy Safeguards, Rules, Standards Other: 5, 6, 7, 8, 9, 4, 17, 18, 23	Unlikely
	See 4.5.					
4.7	The data holder may send the data to the accredited data recipient in a format that frustrates its efficient and timely use.	Likely	Minor	**Low**	Primary: Privacy Safeguards, Rules, Standards Other: 5, 6, 7, 8, 9, 4, 17, 18, 23	Rare
		It seems pessimistic to rate as Likely the prospect of a Data Holder acting to frustrate Data Recipients.				
4.8	The data holder may intentionally or unintentionally send accurate but misleading data.	Possible	Moderate	**Medium**	Primary: Privacy Safeguards, Rules, Penalties Other: 5, 6, 7, 8, 9, 4, 17, 18, 23, 13, 24	Unlikely
	See 4.5.					

4.9	A third party may intercept or interfere with the data during transfer between the data holder and the accredited data recipient.	Rare	Extreme	**Medium**	Primary: Privacy Safeguards, Standards, Commonwealth Criminal Code, State criminal laws Other: 19, 4, 5, 6, 7, 8, 9, 17, 18, 20, 21, 22, 23	Rare
		We do not believe there is sufficient information to make a robust estimate of the likelihood, neither before nor after mitigation. However, Internet crime is rife in general, and the likelihood of criminal interference to CDR transfers is arguably higher than "rare".			*Mitigation 2 (information security standards) is probably more important than any other.*	*If the mitigations do not reduce the likelihood (or severity) then what is the point?*
4.10	A third person [sic] may pose as the accredited data recipient to gain access to the individual's raw transaction data from the data holder.	Unlikely	Extreme	**High**	Primary: Privacy Safeguards, Standards, Commonwealth Criminal Code, State criminal laws Other: 19, 4, 5, 6, 7, 8, 9, 11, 14, 17, 18, 20, 21, 22, 23	Rare
	In other words, organisational "identity theft" of the Data Recipient.	*The threat is framed as an external attack where a stranger poses as the true recipient (and necessarily creates a fake sub-system to which data is unwittingly transferred). On the other hand, an inside job could be more feasible. Therefore we dispute the estimates.*			*Inside jobs must be mitigated by a mix of operations management processes, technical restrictions (perhaps Mitigation 2) and internal audit (Mitigation 17).*	.

5.1	The accredited data recipient, their employee or contractor may access or use the individual's data without authorisation.	Unlikely	Moderate	**Low**	Primary: Privacy Safeguards, Standards Other: 4, 5, 6, 7, 8, 9, 11, 17, 18, 20, 21, 22, 23, 24	Unlikely
	In other words, an "inside job"	*In Lockstep's experience, inside jobs are not unlikely. When Personal Information of large numbers of consumers is available inside a large organisation, the temptation to look up friends & family, out of curiosity or to gain advantage, makes unauthorised access by unscrupulous employees almost inevitable. The reputational damage to the Participant involved, and to the CDR as a whole, would be "Major"; Lockstep suggests that the PIA look at risk at the group-level here, not the individual-level.*			*Lockstep advises that community expectations will be high that the CDR regime expressly protects against inside jobs.* *In general, inside jobs must be mitigated by a mix of operations management processes, technical restrictions (perhaps Mitigation 2) and internal audit (Mitigation 17).* *Mitigation 2 should therefore include access restrictions and internal audit.*	.
5.2	The accredited data recipient may misuse the information provided by the individual in a way technically consistent with their authorisation.	Possible	Minor	**Medium**	Primary: Use restrictions, Privacy Safeguards, genuine consent requirements Other: 4, 5, 6, 7, 8, 9, 11, 13, 17, 18, 20, 21, 22, 23, 24	Unlikely
	What does the qualifier "technically" mean in this context? Does it suggest this threat is thought to be more inadvertent than deliberate?	*Data practices inconsistent with accreditation need to be analysed differently according to whether the activity is deliberate or inadvertent.*			*It is not clear yet to Lockstep how existing mitigations will curb inside jobs, so we recommend more cautious estimates and expectation setting.*	*. Optimistic.*

5.3	The accredited data recipient, their employee or contractor may disclose the individual's data without authorisation.	Possible	Moderate	**Medium**	Primary: Privacy Safeguards, Standards, genuine consent requirements Other: 4, 5, 6, 7, 8, 9, 11, 13, 17, 18, 20, 21, 22, 2324	Unlikely
	In other words, an "inside job"	*As per our comments on risk 5.1, inside jobs are not unlikely at the group level, and should be considered at the group level because of the reputational damage to Participants and the CDR regime.* *Reputational damage in the event of an organised criminal disclosure of CDR data would be "Major" at least and arguably "Extreme".*			*See 5.1.*	.
5.4	A third party may access the accredited data recipient's systems and acquire or use an individual's data without authorisation.	Unlikely	Major	**Medium**	Primary: Privacy Safeguards, Standards Other: 19, 4, 5, 6, 7, 8, 9, 11,17, 18, 20, 21, 22, 23, 24	Unlikely
	In other words, the Data Recipient system is breached.	*When Data Recipients come to acquire large amounts of data (and especially given the possibility of less than ideal security at some organisations such as fintech start-ups) they will be highly attractive targets for cyber criminals and inside jobs. We suggest the likelihood is going to be much higher than Unlikely.*			*Security standards (Mitigation 2) must be a major part of the mix. Resistance to criminal attack against Data Recipients is a high ranking concern amongst incumbent Data Holders and justifiably so.*	.
5.5	The individual may experience increased threats to privacy due to improved insights about the individual enabled by analytics and better access to aggregated datasets.	Possible	Moderate	**Medium**	Primary: Privacy Safeguards, education Other: 10, 11, 16, 18, 19	Unlikely
Agreed.						

6.1	The accredited data recipient may intentionally or unintentionally fail to delete data when required.	Possible	Minor	**Low**	Primary: Right to withdraw consent or delete, Privacy Safeguards, Rules, Standards Other: 4, 5, 6, 7, 8, 9, 16, 17, 23	Unlikely
		We agree with the estimates.			*Just to note that timely destruction of old or superfluous data is fundamental to the CDR regime.*	*Agreed.*
6.2	The accredited data recipient may publicly release personal information that has not been properly de-identified, carrying a risk of future re-identification and hence privacy risks.	Possible	Moderate	**Medium**	Primary: Privacy Safeguards Other: 4, 5, 6, 7, 8, 9, 16, 17, 23	Unlikely
	Yes, the risk of re-identification increases all the time.	*We agree broadly with the estimates but would emphasise that the risk of re-identification is highly context dependent and ideally should be calculated and managed by Participants in their local settings. The overall re-ID risk should also be revisited regularly in light of developments in Big Data.*				*This likelihood, if true, will not stand still for long.*
6.3	The holding of data does not cease even though the accredited data recipient is no longer accredited.	Possible	Moderate	**Medium**	Primary: Right to withdraw consent or delete, Privacy Safeguards Other: 4, 5, 6, 7, 8, 9, 16, 17, 23	Unlikely
	The nature of the threat here relates to a Participant which loses its CDR accreditation retaining consumer data.				*We suggest that a Participant which loses its accreditation might no longer be technically subject to the Privacy Safeguards. Therefore a clearer mitigation against threat 6.3 might be to explicitly require a Participant which has lost it CDR accreditation to delete all CDR data holdings, unless required to retain data for some other legislated requirement (in which case it must refrain from using retained CDR data for any purpose counter to the CDR safeguards).*	

Examining the PIA's Proposed Risk Mitigations

After enumerating privacy threats, the PIA sets out 24 privacy risk mitigations, and then tabulates how they reduce the likelihood of each threat. The mitigations appear somewhat generic; they are offered as a set (organised only in two subsets, for new measures introduced by the CDR, and existing regulatory measures).

In this chapter, we examine the proposed mitigations in detail. The table below contains our observations and recommendations. We also offer some general remarks, and suggest that more coverage be given to authentication.

General remarks

As a general observation, Lockstep is concerned that many of the proposed mitigations are still on the drawing board and are still lacking in specifics. There is limited ability to show how an aspirational measure will address specific threats, or how it will really impact likelihood. The PIA will need to be revised when more details are known about these mitigations.

Authentication

Almost nothing is said in the PIA about authentication as a risk mitigation. Footnote 34 mentions a number of "models" under consideration by the DSB, namely "decoupled approach", "redirect approach" and "known channel redirect approach, none of which Lockstep in fact recognises as conventional approaches. We would like to see authentication normalised in the PIA. Authentication is such an important security measure that the lack of detail is especially disadvantageous to the PIA. Gladly we are informed that the Data Standards Board is working on authentication. This work should be reflected in the PIA, and in turn, the DSB should use the PIA to inform its technical development.

Further, we suggest that *mutual* authentication, to help mitigate against third parties posing as accredited data recipients or tampering with the Accreditation Register (risk 1.1) should be included in the analysis and the standards development.

Baseline protections

Mitigations 19 to 24 all refer to existing privacy protections without modification. Lockstep sees merit in this PIA pointing out the ways that privacy is currently protected, as part of a baseline regulatory regime in which the CDR operates. However we suggest it is unnecessary to enumerate existing measures as *mitigations* as if these are creatures of the CDR regime. It may make the CDR PIA seem like a stretch in some peoples' minds.

Detailed comments on proposed mitigations

Mitigations listed in the PIA (underlines added by Lockstep)	**Lockstep remarks**
1. Privacy Safeguards: The Bill will create a minimum set of Privacy Safeguards for the CDR that may be supplemented by additional protections in the Consumer Data Rules. *CDR participants are all required to comply with the Privacy Safeguards which are 'hardwired' in the primary legislation and set out the minimum privacy requirements. While Privacy Safeguards bear similarities to the APPs, they reflect the more onerous privacy protections required by the CDR framework.*	We agree that the CDR privacy safeguards are more onerous than the APPs, and we recognise the further potential for the ACCC rules to go further. The broad definition of CDR data and applicability of the CDR regime provides a foundation for significant strengthening of privacy and security protections for Australian consumers in banking and other industries, provided the accreditation regime is rigorous.

2. *Information security standards: Data security and transfer standards will be developed by the Data Standards Chair, setting out minimum requirements that must be met.* *The Data Standards Chair will set out data security and transfer Standards containing the minimum information security requirements that CDR participants must meet. These Standards are intended to reduce the risk of unauthorised access to CDR data so that the privacy of individuals will be further protected. These Standards may be supported by additional requirements in the Rules.* *The regime will require all communications to be encrypted, greatly minimising communication risks.*	At this stage, the data security standards are a work in progress. We have specific recommendations elsewhere in this report for inclusions in the data security program. Lockstep acknowledges that mandating data security for financial data is potentially a strong step, for Australia has only had light touch security regulations for e-commerce until now. It remains to be seen how prescriptive the CDR Data Standards, accreditation regime and enforcement arrangements will be. Lockstep cautions that a blanket requirement for "all communications to be encrypted" is rarely practicable. Encryption key management has long been a major challenge across different systems and has prevented widespread consumer take-up of email encryption. It is notable that encryption key management is one of the most active areas of product innovation in cloud documentation management services and consumer secure messaging. Encryption is far from being a solved problem, so it is crucial that generic encryption mandates do not lull policy makers into a false sense of security. Encryption does not necessarily in fact 'greatly minimise' communication risks, for it can introduce new risks such as reduced availability, or outright loss of valuable data in the event that encryption keys are destroyed. Encryption is only as good as the secret key management. The strength of encryption is still an open question in the Galexia report [9] so we presume there is a process in place for the DSB to resolve this issue systematically. It is essential that security specifications in general and encryption requirements in particular be methodically refined and agreed to through a formal process, with accompanying threat & risk assessment. Technical tools to support internal audit (see Mitigation 17) should be included in the security standards. Such tools would usually include logs to record the details of all accesses to consumer records. Access control requirements should be included in the security standards. Decisions should be made at the DSB level about Role-Based and/or Attributes-Based Access Control, as means to help mitigate inappropriate access to CDR data.

3. Express consent: Consents to collect, disclose, hold or use data will need to be genuine. *It is proposed that the Rules will set out requirements to ensure consent is express, informed, current, clear, specific, unbundled, and time limited. It is also proposed that the rules will ensure that consent is given by the relevant person, with the appropriate capacity, thereby helping to mitigate authorisation risks.*	Lockstep agrees with the importance of consent, and acknowledges the attention that is paid to consent in the CDR regime. Proper consent is one of the greatest sticking points in digital business practices; if CDR can bring improvements in the way consent is managed, then that could represent a watershed in privacy management. Consent rules are still a work in progress, and should be subject to further analysis in an update to this PIA. We note that concerns of the Law Council that "for a regime said to be driven by consent, there is a lack of clarity around what is meant by consent and how consent is to be evidenced" [10].

4. Data is transferred to trusted recipients: The CDR will only require data relating to identifiable individuals to be transferred to accredited data recipients. Accreditation is expected be tiered according to the risk level of the data in question. *The ACCC will be responsible for the accreditation of data recipients and will set out accreditation requirements in the Rules. … It is also expected that the Rules will provide for accreditation to be graduated – that is, data recipients who seek to have access to high risk data will be required to have a higher level of accreditation and more stringent protections in place. … The ACCC will be empowered to suspend, revoke, downgrade or impose conditions on accreditations.* *[The Privacy Act SME exception] will not be available to enterprises that obtain accreditation under the CDR.* *<u>However, the regime does not create a closed system – the rules may permit consumers to direct that data be transferred out of the system (subject to further authorisations and restrictions).</u>*	The ACCC decided, while this review was underway, to close the system to non-accredited Participants, at least for the initial rollout of the CDR. In Lockstep's view, this is prudent and substantially strengthens Mitigation 4. More detail is required, and we recommend that the PIA be revised as soon as details are available.
5. Remedies: It is intended that individuals will have access to external dispute resolution arrangements, leveraging existing sector specific schemes. The OAIC will also be empowered to provide remedies to individuals. *The ACCC will be empowered to recognise existing external dispute resolution schemes …*	No comment.

6. A privacy specific regulator: The OAIC will provide advice and expertise on privacy protection, as well as complaint handling and enforcement for privacy protections. The ACCC will have a complementary strategic enforcement role. *The OAIC will be primarily responsible for enforcing the Privacy Safeguards. It will be able to provide individual remedies to complainants. The OAIC will also advise the ACCC on privacy impacts when the ACCC is conducting sectoral assessments. The ACCC will focus on consumer and competition outcomes and on enforcing the balance of the regime.*	No comment.
7. Penalties: Breaches of specific Rules and any Privacy Safeguard can attract civil penalties up to, for individuals, $500,000 or, for corporations: $10,000,000 … These penalties align with the competition law and Australian Consumer Law penalty amounts.	No comment.

8. Broad regulators' powers … • *Criminal penalties* • *Civil penalties* • *Compensation orders* • *Infringement notices* • *Injunctive orders* • *Disqualification of directors orders* • *Adverse publicity orders* • *Enforceable undertakings* • *Investigation and auditing powers* • *Sectoral assessment/general inquiry powers* • *Information sharing*	No comment.
9. Direct rights of action: The Bill provides a right of action for breaches of the CDR. This can form the basis of class actions. *Currently, the Privacy Act does not give rise to a right of action directly to the courts by an aggrieved party.*	No comment as Lockstep is not a law firm.

10.Targeted application: The CDR is only applied to data sets after consideration of privacy impacts has taken place. *A sectoral assessment by the ACCC, in conjunction with the OAIC, will be required before data sets and data holders become subject to the CDR. The Treasurer must consider the privacy and confidentiality impacts before a sector is designated. Further, the legislation will empower the Treasurer to make regulations to accompany a designation. This power can be used to ensure that the Rules contain certain requirements, including in relation to privacy. The targeted application of the CDR will assist in ensuring that privacy impacts are at the forefront when a sector is designated.*	Lockstep endorses this approach. As with conventional security risk assessment, there should be an expectation that detailed privacy risks will vary from one market or business environment to another, and that local risk assessment should always be undertaken. A power for the Treasurer to make regulations to ensure that the Rules contain certain requirements is a welcome expression of this reality.
11.Rights to withdraw consent or delete: Individuals will be entitled to withdraw their consent to a data holder providing access to a data recipient. The CDR framework will also require data to be deleted upon any use permissions becoming spent. *…*	In Lockstep's view, this represents a major and welcome extension to generally understood consent practices as currently framed in Australia by the Privacy Act. The withdrawal of consent can be a practically difficult matter. We also note the intention for a CDR pilot to test the UX of consent, before the regime goes live.
12.Holding out offence: The Bill will make it an offence for a person to falsely hold out that they have accreditation, or have accreditation at a particular level.	No comment as Lockstep is not a law firm.
13.Misleading or deceptive conduct offence: The Bill will include an offence of misleading or deceptive conduct.	No comment as Lockstep is not a law firm.

14.Accreditation Register: All accredited entities will be listed on a publicly available register. CDR participants will be required to confirm that entities are listed on the Register before transferring CDR data to them. … *The register will, through the use of digital certificates, guard against the risk that a person may seek to impersonate a participant.*	On its own, listing on a register is not a strong mitigation. We understand that the DSB is considering *mutual authentication* through digital certification and digital signing of Accreditation Register entries. These can be strong security measures, if they are utilised by software programs accessing the register. Certificates and digital signatures can only be checked programmatically and provide no significant protection if the register is checked manually. Lockstep hopes that the DSB sets out detailed methods for Participants' software programs to automatically confirm digital certificates, to mitigate against fake registrations or tampering with registration.
15.Scope: The CDR framework can potentially apply to a broader range of data than the Privacy Act does, that is, data that relates to either a natural or legal person. SMEs are not exempted from the [CDR] Privacy Safeguards. *…* *Any privacy related Rules can also apply to all CDR data in the system.* *The CDR framework will bind all data holders, accredited data recipients and gateways.*	The inclusion of SMEs (which are exempted from the Privacy Act) would be a welcome improvement in Lockstep's view.

16.Use restrictions. *The Privacy Safeguards restrict the use of CDR data for direct marketing unless positively permitted by the rules. …* *It is also proposed that the Rules will create restrictions on the on-selling of data.* *Further, there will be a sub-class of intermediary called a designated gateway. Designated gateways will only be able to collect, use and disclose information as specifically provided for in the rules.* *Additionally, the CDR system will not authorise credit reporting agencies to undertake actions that they are otherwise prohibited from doing under the law (e.g. under Part IIIA of the Privacy Act).*	No comment.
17.General practices: there will be record keeping, audit trails and notification requirements that are intended to ensure CDR participants comply with best practice. *The Privacy Safeguards require CDR entities to keep and publish privacy policies about CDR data. …* *This record-keeping and reporting power also allows the ACCC to use new Reg-Tech based approaches to enforcement. …*	Audit trails and, moreover, regular internal review of audit logs to actively monitor for abuse of the system are important deterrents against unscrupulous employees. Mitigation 17 is important and could be strengthened by inclusion of technical audit tools within Mitigation 2. See above.

18.Education: … *The ACCC and OAIC will provide education to individuals in regards to the CDR and their rights and protections under the regime. The OAIC will also be empowered to issue guidance on the Privacy Safeguards. Data61 will have responsibility for educating CDR participants in relation to compliance with technical standards for privacy, confidentiality and information security. Education will help to ensure that individuals understand the CDR and are able to use it safely and securely.*	Mitigation 18 appears to be the only place where guidance and education are called out. We recommend that education for consumers and participants be covered separately. In Lockstep's experience, the design of consent UI and UX is complex, and can involve quite novel interfaces like dashboards. We recommend that ACCC/OAIC plan detailed software development guidance for CDR participants as well as for consumers.
19. [Existing] Privacy Act: The Privacy Act and APPs will continue to operate alongside the CDR. …	This seems obvious.
20.[Existing] Commonwealth Criminal Code: The Code includes offences prohibiting unauthorised access, modification, or impairment of data where there is an intent to commit a serious offence. *Individuals will continue to have access to remedies outside of the CDR framework where their privacy has been breached, or data misused. The Commonwealth Criminal Code currently has offences against unauthorised access to, modification or impairment of data held in a computer …*	This seems obvious.
21.[Existing] State criminal laws: All States have criminal laws against accessing restricted data. These offences may deter unauthorised access by internal parties. …	This seems obvious.
22. [Existing] Breach of Confidentiality: Banks have additional duties of confidentiality. This is a potential cause of action for individuals to pursue. …	No comment as Lockstep is not a law firm.

23.[Existing] Tort of Negligence: The common law tort of negligence and the Civil Liabilities Acts across all States provide a cause of action for individuals to seek remedy. …	No comment as Lockstep is not a law firm.
24.[Existing] Australian Consumer Law: Part 2.1 Misleading or Deceptive Conduct will allow individuals to bring an action against data recipients where they engage in misleading or deceptive conduct. …	No comment as Lockstep is not a law firm.

Other measures

APIs

The API standards as far as we can see are collected as a living document in Github. Despite being given a version number, there is not a discrete or frozen version-numbered document containing the API standards which can be referenced.

There is a trade-off between simplicity and generality of an API from the developer's perspective, the simplicity of the user experience it leads to, and the amount of general information that can be passed across the API in action. Software development can be easier, and the end user experience made somewhat more consistent, if APIs are more general-purpose in nature, so that the one API can be invoked more often when CDR data is to be transferred. However, general-purpose APIs can by design lead to more information being passed than is necessary case by case.

For example, if one Data Recipient routinely seeks to retrieve data items A, B, D and F of a consumer, and another Data Recipient often seeks data items B, C, E and G, it seems reasonable for a general-purpose API to be specified along of the lines of:

```
GET_CONSUMER_DATA(A,B,C,D,E,F,G).
```
[3]

The one API can be used by both Data Recipients to retrieve the data items they need, yet the API will lead to more consumer data being transferred than is necessary. While the general-purpose API may be attractive from the point of view of software maintenance, it leads to disclosure of Personal Information beyond what is strictly necessary, and therefore is at odds with Disclosure Limitation principles in privacy.

The draft API standards [8] appear not to incorporate any substantive consideration of these trade-offs. See for example:

> *Principle 7: APIs are simple; As complexity will increase implementation costs for both providers and clients as well as reduce the utility of the APIs, API definitions should seek to be as simple as possible but no simpler.*

This principle in our opinion is not sufficiently precise or measurable to provide practical guidance to developers. And with its sole interest in simplicity, the principle overlooks the balance that should be struck with other considerations such as privacy.

If on balance, the design approach is weighted towards general-purpose APIs, then it would be advisable for supplementary guidance to be created for developers to highlight the side effects and possible unintended

[3] Lockstep's crude pseudocode here is not meant to bear any resemblance to actual CDR APIs under development.

consequences of excess personal information being returned when APIs are called. Developers should take special care to thoroughly delete unnecessary CDR data which flows as a result of general-purpose APIs. In specific circumstances (such as call centre systems where human operators might have access via screens to such extra details) software could be written to mask the excess details, and/or training could be provided to alert operators to their obligations to not use Personal Information inappropriately.

As the CDR system continues to develop, the Data Standards Body and related Working Groups should keep close track of the competing API design objectives of reusability and disclosure minimisation, and revise the API design strategy as appropriate. Working Groups should from time to time publicise the way they have analysed the privacy-utility balance, in line with *Privacy-by-Design* principles.

Privacy-by-Design

Lockstep understands that Treasury is aware of the privacy trade-offs to do with general-purpose vs fine grained APIs. But we can't tell if the API team shares this understanding, nor (more generally) can we see if *Privacy-by-Design* is incorporated into the API working group's processes. The Data Standards Body Advisory Committee is supposed to include an observer from OAIC.[4] The Committee meeting of 11 July 2018 discussed privacy and security with consideration of whether or not they needed to be expressly enumerated in WG principles. For this to be an open question casts doubt on how much express attention is given to privacy in WG technical discussions. We note (and applaud) that the DSB works in a highly transparent way, with its minutes and draft works being made public; we suggest that similarly, the DSB and the WGs publicise how they factor privacy into their design processes.

[4] See https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standards.

Recommendations and Suggestions

Immediate recommendations for the PIA

1. Government should consider strong legal action (possibly a zero-tolerance approach) against accredited Data Recipients which are found to use or disclose CDR data without authorization, in order to help maintain confidence in the CDR system and its strategic objectives of protecting consumers who choose to have their data released.
2. Some introductory text should be added to explain the way that the CDR PIA has been framed in a novel manner, to help readers orientate themselves to the analysis.
3. The PIA must be revised when the ACCC Rules are stable, and when the proposed information security arrangements for the Accreditation Register have been detailed.[5]
4. Information flow mapping should be extended to model designated gateways as far as possible given current best understanding of how these participants will operate.
5. Because the risk of re-identification is highly context dependent, the CDR regime should require Participants to undertake their own local assessment of de-identification practices and re-identification impact in their local settings. Re-identification risk should also be revisited regularly in light of developments in data analytics, and the possibility that mergers and acquisitions cause datasets to be linked in new ways (Ref: PIA risk 6.2).
6. Noting that the CDR Working Groups are already operating in a substantially transparent manner, the WGs should be encouraged to publish their privacy considerations in relation to API design, to commit to periodic review of the API specifications, and be prepared to specify more granular application-specific APIs should inadvertent information disclosure become a concern.

Other suggestions for the PIA

a) Future CDR PIAs could include a baseline assessment of the privacy impacts when the regime is operating as intended, instead of only examining the impact of adverse events.

b) The PIA should include a discussion of acceptable residual risks, and draw a line in the sand as to what residual risk level is deemed acceptable for each identified threat.

[5] Lockstep understands that a CDR pilot is planned – to test security, evaluate user experience, evaluate consent processes and so on – well in advance of the launch currently slated for February 2020. While the exact timing is uncertain, we would suggest that a repeat PIA either follow the CDR pilot or run in parallel with the pilot, in order for further privacy analysis to inform post-pilot changes.

c) As with typical security risk management, a formal process is needed to deal with residual risks that exceed the target threshold. CDR management structures should include a Risk Committee or equivalent function to monitor risks as the CDR rolls out, and oversee continuous improvement to the mitigations.

d) Revise the language used to describe risks in line with conventional risk management standards. In particular, use the term *threat* (rather than "risk") for adverse events, and reserve the term *risk* to describe the seriousness of threats (being a product of likelihood and severity).

e) Refine and qualify the existing requirement in Mitigation 2 that "all communications [are] to be encrypted" in light of practical encryption key management challenges. Ensure that any exceptions to the requirement are well understood and promulgated, to avoid creating a false sense of security.

f) The data security standards should include handshake protocols to ensure that an individual's authorisation to disclose data is properly be received by the data holder (see risk 3.7).

g) The short discussion "Mapping Personal Information" on page 4 seems unnecessary given the detailed mapping set out in "Mapping of personal information flows" on p 41 and could be dropped altogether.

Other CDR privacy suggestions in general

h) Mutual authentication, to help mitigate against third parties posing as accredited data recipients (risk 1.1) is in Lockstep's opinion an important risk mitigation. We understand that the data standards development is considering digital certification and digital signing of the registry; we suggest that this measure is made more visible to stakeholders, and is factored into the PIA.

i) Assuming the DSB specifies digital certificates and signatures to secure the Accreditation Register, further guidance should be produced so Participants' software programs will automatically confirm digital certificates, to mitigate against fake registrations or tampering with registration.

j) State-of-the-art multifactor authentication of end users, such as FIDO Alliance protocols, should be part of the DSB's consideration of authentication standards.

k) Handshake protocols should be part of the Data Security Standards, to mitigate the risk of data being sent to the wrong recipient, or data about the wrong consumer being sent to the right recipient (to help mitigate risks 3.7, 4.1, 4.2 and 4.3).

l) ACCC/OAIC should plan detailed software development guidance for CDR participants in the area of consent and authorization UI and UX (to help mitigate risks 2.1, 3.4 and 3.5).

m) Review *Privacy-by-Design* processes in the API and Security Working Groups. Ensure that privacy considerations are embedded in decision-making around APIs. Ensure that API designers and WG members have been trained in privacy engineering.

n) Ensure that consumer data security standards (Mitigation 2) include access controls and internal audit tools to mitigate the risk of inside jobs (see risk 5.1).

o) Ensure that security specifications in general are resolved methodically by the Working Groups, and that they include Information Security Threat & Risk Assessment (TRA).

p) The Data Standards Board and its working groups should make sure that explicit protections against hacking and tampering are in scope for the security standards, so that the delivered standards will mitigate threat 3.1.

References

Project and CDR regime documents

[1]. *Review into Open Banking: giving customers choice, convenience and confidence*, The Treasury, December 2017
https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

[2]. *Treasury Laws Amendment (Consumer Data Right) Bill* 2018
Filename: Treasury-Laws-Amendment-Consumer-Data-Right-Bill-2018-1.docx
https://static.treasury.gov.au/uploads/sites/1/2018/12/Treasury-Laws-Amendment-Consumer-Data-Right-Bill-2018-1.pdf (accessed 25 Jan 2019)

[3]. *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation; Proposals*, The Treasury, 24 September 2018
https://static.treasury.gov.au/uploads/sites/1/2018/09/CDR-proposals-for-further-consultation-1.docx

[4]. *Treasury Laws Amendment (Consumer Data Right) Bill 2018 Explanatory Memorandum*
https://static.treasury.gov.au/uploads/sites/1/2018/12/Explanatory-Materials-1.pdf

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

[6]. *Consumer data right Rules outline* ACCC, December 2018
Filename: CDR - Rules Outline for publication (Feb 2020 commencement).pdf

[7]. *Consumer Data Right Privacy Protections*, The Treasury, December 2018
Filename: 181122 CDR Privacy Summary v3.docx

[8]. *Draft API Standards* v0.2.0
https://consumerdatastandardsaustralia.github.io/standards/#introduction (accessed 20 Jan 2019)

[9]. *Consumer Data Standards – Security Profile (CDS-SP) Galexia Review* v2, Galexia, 19 December 2018

[10]. *Consumer Data Right Rules – Draft Privacy Impact Assessment*, submission of the Law Council of Australia 18 January 2019
Filename: 004 LCA submission on v1 CDR PIA.pdf

External References

[11]. *Guide to undertaking privacy impact assessments*, Office of the Australian Information Commissioner, May 2014
https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf.

[12]. *Privacy for Infosec Pros*, AusCERT Tutorial, Gold Coast, 2 June 2015

Web sites

Open Banking Review
https://treasury.gov.au/consultation/c2018-t247313

Data Standards Board Minutes
https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standards