Xero Submission

Consumer Data Right Statutory Review

20 May 2022

Xero Submission

Consumer Data Right Statutory Review

20 May 2022

20 May 2022

Secretariat
Statutory Review of the Consumer Data Right
The Treasury
Langton Crescent
PARKES ACT 2600

BY EMAIL: CDRstatutoryreview@treasury.gov.au

To Whom It May Concern

XERO SUBMISSION TO CONSUMER DATA RIGHT STATUTORY REVIEW

The Commonwealth Government demonstrated leadership and a clear intention to achieve an open data sharing economy in establishing the Consumer Data Right (CDR) in 2017, a world first placing Australia ahead of comparable economies at the time. Five years on, what was intended to be an innovative open data sharing regime is mired in complexity ranging from multiple friction points arising directly from the legislation and subsequent regulation-based measures in the CDR Rules that are actually preventing efficient data sharing. It genuinely pains us to submit that the cumulative impact of these decisions means there are more incentives to continue sharing data outside the regime, than within it.

Xero has always tried to share our learnings from other jurisdictions in which we operate, it's something we happily do in aid of effective policy outcomes for small businesses and for policymakers. When we apply this lens, the current situation with the CDR stands in stark contrast with the Open Banking regime in the United Kingdom (UK) which now has over 4.5 million regular users made up of 3.9 million consumers and 600,000 small businesses. Today, Xero customers make up around 10 percent of the total UK Open Banking user base. Momentum continues to increase with the addition of 1 million new regular active users every 6 months.[1] By comparison, there is a stubbornly low level of awareness of the CDR and its consumer benefits in Australia, stemming from low Accredited Data Recipient (ADR) participation, among other things.

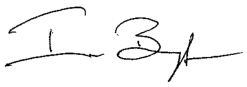
Xero welcomes the review of CDR regime, specifically of Part IVD of the *Competition and Consumer Act 2010* and the wider CDR statutory framework including the "existing assessment, designation, rule-making and standard-setting requirements"[2] (collectively the Statutory Review). This is an important opportunity to explore the extent to which implementation of the CDR regime supports the core policy objectives of driving value for individuals and business consumers by increasing competition and innovation across the economy. Xero considers the Review a significant opportunity for the Government to understand what has and has not been achieved, and to explore efficient steps that can be taken to address and improve the regime.

[1] https://www.openbanking.org.uk/news/uk-open-banking-marks-fourth-year-milestone-with-over-4-million-users/
[2] Terms of Reference

Xero offers several options for the Review to consider to fix the problems of the CDR, which we set out in our main submission. More broadly, Xero encourages the Government to decide a course of action on the principle that data changes custodianship entirely once it moves, with a customer's consent, from a data holder to an ADR. The principle (perceived or otherwise) that the holder still retains some responsibility for the data once it has been transferred, exists within this regime and no other regime globally. This reality or perception is damaging for regime participation and will hold it back from success regardless of other changes that might be proposed.

Xero thanks the Government for the opportunity to participate in the Statutory Review and we welcome any future engagement during the process. We would like to extend an open invitation for the Review or Treasury to meet with Xero's UK Open Banking subject matter experts to discuss how the regime operates in practice for small businesses, from the perspective of a platform enabling around 10 percent of all participation. Xero's Head of Government Experience in Australia Angus Capel will make contact with the Review team to arrange a further discussion.

Your sincerely



Ian Boyd
Xero GM Partnerships - APAC

DETAILED SUBMISSION

1. How Xero shares data today

1.1. Today, secure data sharing is happening between financial institutions and a range of businesses including Xero. Our expectation was that the CDR regime would be designed to eclipse existing data sharing by making it simpler, broader and more stable for the benefit of our customers. In reality, the regime as it is currently designed does not allow for these enhancements in part due to the extension of overly complex controls and requirements to both personal and non-personal information, which go beyond those afforded under existing privacy protections, namely those currently contained in the *Privacy Act 1988*. Xero securely and responsibly manages the use of data for hundreds of thousands of customers today, and has done so reliably and securely since 2006.

1.2. Xero encourages the Review to recommend the adoption of the UK approach to open banking and how that regime relates to data privacy. The UK model trusts in the privacy law to achieve its objective to regulate the use of personal information rather than incorporating privacy reforms via the open banking regime. Xero strongly supports right-sized regulation to protect consumer data, but believes protections should apply economy-wide through reform of the Privacy Act if and as required, rather than creating a separate regime for protecting CDR data, whether that CDR data is personal information or not.

1.3. A well established business data sharing framework based on the Privacy Act, the ATO DSP Operational Framework and associated Security Standard for Add-on Marketplaces (SSAM), industry best practice and contractual arrangements exists and is fully operational today (the Security Framework). This approach is working as intended and ensures the security and privacy of data transfers that occur for a business purpose. If the Review is inclined to maintain the current or similar CDR regime protections and restrictions, Xero strongly suggests close consideration be given to recognising the Security Framework as creating an appropriate privacy environment in which to share CDR data for a business purpose. Xero is confident recognising this Security Framework would materially increase ADR participation, connecting business consumers with the innovation and competition measures intended for the CDR.

2. Data deletion and de-identification

2.1. A right to data deletion is an important privacy feature for small businesses and individuals, but its intersection with other laws and obligations, including business record keeping, creates complexity in its implementation. Today, Xero, our industry and a host of business-to-business software-as-a-service (SaaS) compliance tools will struggle to participate in the CDR due to strict data deletion and de-identification requirements. These requirements could actually place Xero in the position of potentially 'managing' conflicting legal obligations. On one hand we could be obliged to comply with CDR obligations requiring data be deleted, which could be an act, if undertaken, that might impact CDR consumers' compliance with various laws relating to, for example, business record keeping, tax

and corporate reporting obligations, particularly if the requirement to delete CDR data arises due to an inadvertent lapsing of consents. This is before considering the negative customer experience of deleting or de-identifying data required to fulfil statutory record keeping obligations absent an express instruction from a customer to do so. For example, lapsed consents may mean Xero is required to delete or de-identify all CDR and CDR derived data, meaning small businesses would lose hours of reconciliation and years of statutory business reports, exposing the business to significant risk of non-compliance. However, even if these data deletion and de-identification complications are resolved, the complexity of participating in the CDR makes the decision to become an ADR unappealing.

3. Third party participation

3.1. Under the current Australian CDR Rules Xero has four options to accredit our ecosystem to maintain current digital access for our small business customers: sponsorship-affiliate model, representative model, trusted advisor model or requiring unrestricted ADR status.

3.2. Our view is that the representative model does not suit a fintech-enabled ecosystem as it would require locking apps into an exclusive relationship with Xero. Apps gain scale by operating across platforms which would end under the representative model. It would also see Xero assume liability for each representative in the ecosystem, which would come at a substantial cost subsequently passed on to our small business customers. Additionally, this outcome would likely be at odds with the stated broad policy preferences of the Government around platform openness.

3.3. For Xero, the sponsor-affiliate model would require entering up to 20,000 (commercial) sponsorship agreements in Australia, including with apps integrating with other platforms. Maintaining sponsor obligations at this volume is not feasible. Additionally, a model in which apps require sponsorship from multiple ADRs creates - in our view - an unreasonable level of red tape for all parties involved.

3.4. Requiring Xero's 20,000 Australian data accessing API connections (custom integrations and apps) to become unrestricted ADRs would create a substantial compliance cost for our ecosystem. In addition, Xero's existing SOC and ISO requirements under the ATO's existing security framework if we were operating within the proposed CDR regime, could result in Xero being required to take "reasonable care" to ensure unrestricted accreditation is genuine, and take a risk based approach to ensure apps are complying with the requirements of unrestricted ADR accreditation. We would expect that the majority of our apps would not be able to afford the compliance requirements and withdraw their offering or work around the CDR.

3.5. The impact of all this ultimately falls on our and the apps mutual customers using the underlying services, namely many small businesses across Australia. These small businesses would be deprived of a service they value and which helps them run their business, or be deprived of standard security measures provided today. On the face of it, these real world impacts may seem minor or esoteric but they stand a real chance of having quite debilitating impacts on actual small businesses who rely on

these services and the local economic contribution they make.

4. Trusted advisors

4.1. In response to stakeholder concerns in Australia, the Government has introduced rules to allow small businesses to share their banking data with certain classes of accredited trusted advisors and has established accreditation options designed to allow third parties to use permissioned data shared by their customers. However, until further legislative and regulatory amendments are actioned, the CDR will not be capable of matching the current data sharing services enjoyed, and expected, by Australia's 2.4 million small businesses.

4.2. Small businesses are not extended the freedom to choose which advisor - their trusted advisor - they share their data with under the CDR Rules. Under the Trusted Advisor rule an actual scenario that could easily arise sees a husband, acting as an informal advisor to his wife's small business, not being able to send or follow up invoices on behalf of his wife. This limitation does not align to the way in which small businesses typically operate. Small businesses cannot be expected to only share their data with a narrowly defined list of Trusted Advisors, to perform simple administrative tasks. This would either increase the administrative cost for the business, or the owner would need to perform these tasks themselves rather than undertaking revenue generating activities. Again this stands to have real implications for the small business economy. While we also understand the need to regulate the standards of accountants and bookkeepers in the industry, our concern is that the very prescriptive proposed definition of a Trusted Advisor would also effectively exclude many bookkeepers who have had relationships with small businesses for many years, and who are trusted implicitly.

5. Derived data

5.1. Another important consideration is the types of data that are valuable and will drive innovative products and services. The first designated sector for the CDR regime was, of course, banking and the relevant data being customer, product and use data, excluding materially enhanced data. Accountancy and accounting data is separate to both the sector and data designated.

5.2. However, as open banking is currently being implemented, the boundaries between banking data and other data (including accounting data) have dissolved due to the broad definition of data considered to be within the regime (CDR Data), including the novel concept of broad type of data whose primary distinguishing feature is that its said to be have been 'derived' from CDR Data (CDR Derived Data). We would submit that this latter concept and the breadth of its definition and impact are fatal to the regime.

5.3. For example, accounting data usually derives from bank statement transaction data, the latter of which is data mandated for sharing under the ADI designation instrument. However, because of the scope and effect of the CDR Derived Data concept, after that data build occurs, the accounting data is

now to be deemed as CDR Derived Data and the full suite of CDR protections and restrictions are applied to all subsequent sharing of that accounting data. This means that accounting platforms, like Xero - where business customers can share their data with advisors of their choice, will be required to heavily restrict how businesses share their data under the CDR. This is a good point at which to come back and compare this outcome with the stated intention of the regimen to *increase* a consumer's control of their data.

5.4. Along with data deletion and de-identification complexities, this is a fundamental problem with open banking in Australia for accounting platforms. This onerous application of regulation exceeds the UK Open Banking model, risking significant unintended consequences resulting from the regime. Under the UK model, the transfer of Open Banking data is regulated but the subsequent use of data derived from that data is not. This is a proportionate, sensible and evidently workable approach. UK Open Banking is a data communication model which gives customers control of their data and how it is used, and relies on privacy and data protection laws to protect customers appropriately. This is an important distinction between the UK regime and the CDR, which introduces privacy obligations within the very CDR regime itself, i.e. outside the Privacy Act. To reiterate, Xero is a strong supporter of regulations that appropriately protect consumers and small businesses, but it is critical these protections are applied in an effective and efficient manner that gives, rather than hinders, consumers' control over their own data.

ANSWERS TO CONSULTATION QUESTIONS

1. Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?

1.1. The CDR's introduction of onerous and cascading participation requirements places Australia at odds with working international open data regimes, incentivising continued data sharing outside the CDR. Specifically, the CDR framework introduces data deletion and de-identification complexities, which could contradict various laws that apply to CDR consumers relating to, for example, their business record keeping, tax and corporate reporting obligation.

1.2. Additionally, in many cases the full suite of CDR rules will apply to third parties receiving permissioned data from an ADR. Rules apply in the case of data being received by an ADR which is not "raw" CDR data as explained in a designation instrument, but rather the broadly applying CDR Derived Data. In practice, the broad definition of CDR Data including CDR Derived Data means that a catering business seeking to connect an app to their Xero subscription to predict rostering and cash flow needs on weekends based on prior weekend sales data would need to do so in compliance with CDR regulations. The result is a CDR regime characterised by high regulatory barriers compared to the more appropropriate set regulatory barriers for data sharing outside the regime.

1.3. This regime feature means businesses and potential ADRs are incentivised to continue data sharing outside the regime and will continue to do so until the CDR's regulatory distortions are addressed.

1.4. Further, the CDR introduces strict consent requirements within the regime which appear to exceed the Privacy Act and European Union's General Data Protection Regulation (GDPR). The CDR Rules stipulate ADRs must follow a rigid consent process throughout the CDR data lifecycle, which does not feature in the Privacy Act, the GDPR or other comparable privacy regimes where consent is only one of several legal bases for handling consumers' data. Xero fully supports effective and efficient consumer protection which is fundamental to the operation of our business. However, Xero is of the strong view a significant departure from established privacy protections such as those included in the CDR must be progressed through the Privacy Act reform following a full consultation process if a successful open data regime is to be achieved.

Express consent complexity and a consumer's response:

The express consent model required under the CDR will result in significant operational changes to replace existing avenues for businesses already receiving permissioned customer data under the protection of existing frameworks and legislation. It could also, unintentionally, stifle innovation by narrowing otherwise lawful uses and disclosures of data captured by the broad definition of CDR data and overwhelm consumers with multiple consent requests.

For example:

- multiple consents are likely required to facilitate data transfer (collect, use and disclose);
- specific consents would be required for each purpose (for example direct marketing, product development and insights), and
- repeated consent refresh requirements may lead to consumers disengaging and unintentionally allowing consent to lapse.

The CDR proposes no transition plan from existing consents despite the CDR's highly detailed user experience requirements. Xero is of the view transitioning consents if managed poorly will result in consumer confusion, scepticism, fatigue and lapsed consents (which anecdotally Xero witnessed in the UK), triggering data deletion or de-identification provisions.

GDPR transition experience

During the introduction of the GDPR, there were at least two consumer challenges with that regime's introduction of a more robust consent-driven approach: consumer awareness and education, and consent fatigue.

First, the population required education to understand the complex new data regime, so that consumers did not become overwhelmed with multiple new consent screens and notifications. Xero and the business community was also challenged to find ways to meaningfully communicate complex data-use scenarios to consumers, for example profile matching, which serves to benefit them, but may be confronting to the uninitiated. Organisations have a clear role to play here by

designing clear and intuitive customer journeys. However, an appropriate balance needs to be struck to ensure consumers are not overloaded with notifications and consent requests before even the most basic task can be performed.

The second challenge is consumer consent fatigue. It is clear that if a regime relies too heavily on consent, in particular stipulating multiple consents, consumers can stop engaging and simply tick the boxes without registering the information. An over-reliance on consent could possibly be more damaging to consumer privacy, with consumers ticking all consents while ignoring meaning, or opting out altogether and choosing to share data outside these schemes.

1.5. Xero strongly urges the Review to consider what optimal data sharing permission looks like and where it is working as intended today, either locally or abroad. For example, in Xero's experience, the Privacy Act combined with the ATO Digital Service Provider Operational Framework strikes an appropriate balance between protection and participation for consumers sharing data for a business purpose. Also, by rigidly defining the user experience there is a likelihood of stifling innovation in the authentication processes. It may make more sense to follow other regimes in setting a minimum standard or principles that the industry can build upon.

2. Do the existing assessment, designation, rule-making and standards-setting statutory requirements support future implementation of the CDR, including government-held datasets?

2.1. The statutory requirements, or process to enable mandated data sharing under the CDR, appears to be fit for purpose. As explored above, the design of the Rules in particular is creating high barriers to entry, reflected in low rates of ADR participation. If the Rules (and legislation) were to be amended to better support participation, Xero is very confident ADR participation would grow rapidly under the existing process.

3. Does the current operation of the legislative settings enable the development of CDR-powered products and services to benefit consumers?

3.1. Xero would require changes to the CDR legislation and Rules to become an ADR under the CDR, we would strongly support harmonising legislation with existing regimes to overcome significant operational complexity to become an ADR, and require further guidance and rules changes to facilitate a transition to participation. Outlined below are the components of the legislation and Rules that fall under each of these categories.

CDR legislation components Xero cannot comply with from a technical viewpoint

3.2. Data deletion and de-identification - inappropriate for businesses data sharing

3.3. CDR Rules 4.11(1)(e), 4.16(2) create the requirement for an ADR to offer a consumer the choice to have their redundant data deleted or de-identified. However, to provide the service requested by our customers, Xero retains customers' financial transactions until instructed otherwise by the customer. If Xero is instructed to delete or de-identify a single customer transaction, it would need to delete or de-identify all of the customer's financial records in Xero.

3.4. The requirement to delete or de-identify the entirety of customer records is due to the nature of accounting. For example, a single sale becomes a credit in a bank account. Once the data is shared with Xero it is reconciled against a user created invoice. The reconciled transaction is coded as a sale and forms part of a profit and loss statement. It is submitted to the ATO as part of a BAS report and as part of a tax return. Deleting or de-identifying a single transaction voids all other reports, forcing deletion or de-identification of those also.

> **Example**: Jane runs a business advisory firm called JBW Services offering business advice and payroll services. Jane employs accountants, bookkeepers and payroll specialists. She is required to comply with a range of business record keeping obligations, including accounting records and payroll records. Jane relies on Xero to maintain these records for her to remain in compliance.
>
> Jane catches Covid and is uncontactable for two weeks, during which time the JBW Services CDR collection, use and disclosure consents lapse, and its CDR data becomes redundant. Xero is placed in the unenviable position of deleting or de-identifying Jane's CDR data, including data Jane relies upon to meet her record keeping obligations. When Jane recovers, she learns she is now in breach of her record keeping obligations.

3.5. Broadly applied data deletion and de-identification rules under the CDR are blocking ADR participation, and in turn the consumer outcomes through innovation and competition sought. It forces data businesses to operate outside the CDR regime to avoid complex questions relating to compliance, potentially creating poor customer outcomes.

3.6. Lapsed consents triggering data deletion or de-identification:

3.7. If a CDR consumer allows its consents to lapse deliberately or inadvertently, accredited persons are required to either delete or de-identify redundant CDR data depending on the consumer's consent election (CDR Rule 4.16). Due to the nature of our product (accounting) being derived from CDR data, a customer's subscription might effectively become "redundant CDR data" in its entirety, requiring complete deletion or de-identification. This would be a catastrophic outcome for many businesses resulting from in many cases, a purely administrative error. In the UK, Xero saw many examples of businesses failing to re-consent to data sharing, including for the reason of forgetting to do so in the required time.

Example: Brad is a sole trader who owns Brad's Plumbing. Brad has requested his bank to share his CDR data with Xero. Brad has also requested Xero share his accounting data with a cash flow forecasting application, which has an integration with Brad's inventory management application. Brad's inventory, invoices and pipeline of work is combined to predict cash flow pressure points. Brad has invited his advisor into his Xero subscription to guide him on optimising his capital allocation on a week by week basis.

Brad takes off on a well earned fishing trip for a week where he is out of mobile reception. During this time his collection, use and disclosure consents all lapse and his CDR data becomes redundant, requiring Xero and Brad's apps to de-identify or delete Brad's CDR data, including all financial data in Xero and his two apps. When Brad returns, he re-consents and has to recode and reconcile hundreds of transactions to rebuild his cash flow prediction engine.

3.8. Rule 4.16 allows a consumer to elect to delete CDR data when it becomes redundant data at any point up until relevant consent(s) expire. However, noting the gravity of deleting or de-identifying data for businesses, Xero suggests consumers should be required to explicitly instruct an ADR to delete or de-identify its CDR data after it becomes redundant, else the ADR should delete or destroy it in accordance with its existing data-retention practices and obligations.

CDR legislation components which stand in the way of Xero's participation due to complexity

3.9. *Cascading CDR regulations - CDR Derived Data needs to be removed:*

The legislation outlines the definition of CDR Data, including CDR Derived Data. This expansive definition makes working out what is, and is not, CDR Data difficult, and enables CDR protections and restrictions to permeate the economy, well beyond the limitations of the designation instrument. This acceleration of regulation appears to be beyond the CDR policy intent and is contributing to low participation in the regime. This extension of privacy controls to a potentially large set of data that may or may not include personal information is more like privacy reform, which Xero considers would be better progressed through a Privacy Act reform if it is indeed required. The concept of 'derived data' should be removed from the legislation entirely, with CDR protections and restrictions applying to CDR Data as designated in the designation instrument only, which would better align the CDR with the UK Open Banking regime.

3.10. *Disclosure uncertainty - definition needs clarification:*

ADRs would benefit from more clarity of the term 'disclose'. While the legislation does not define 'disclose', Xero considers it, in basic terms, to mean a transfer or sharing of data from one entity to another. Therefore, by our definition, CDR protections and restrictions are not triggered if there is no transfer or movement of data between entities. For example, if a Xero customer who is a CDR consumer invites an unaccredited (informal) advisor to view and interact with their data within the Xero platform, CDR protections and restrictions do not apply. However, if the OAIC guideline's interpretation of 'disclose' (essentially, "to make available") applies, informal advisors would likely

require accreditation and consent flows if invited to view or interact with a CDR customer's data on-platform. Xero suggests 'disclose' is defined in the CDR legislation to limit disclosure to a transfer or movement of data [between entities].

3.11. *Complex joint accounts (business) - needs insertion*

Another example of how the CDR is yet to support the participation of small businesses is that it neglects how joint accounts are used in small business. Part 4A, Division 4A.2 of the Rules fails to appreciate the reality of how businesses work. For example, the Rules do not explore in appropriate detail, who is a "joint account holder". For individuals, identifying an account holder is simple, but requirements for business need more work. This section requires significant work to understand structures of business accounts, and who is appropriate to authorise the sharing of a business's data.

3.12. *Trusted advisor exemptions - need business exemption*

The need for a trusted advisor exemption again demonstrates the inappropriateness of the regime for small businesses. Rule 1.10C sees the Government dictate to small businesses what type of advisor they can share their CDR data with, including derived CDR data as outlined above. This is an extreme overreach for any policy, let alone a policy designed with an intention to increase competition and innovation in the banking sector. On a daily basis, small businesses share their data with any number of advisors, spanning accountants and bookkeepers to marketers and strategists. The Government should not be concerned about who small businesses are sharing their data with, as it is theirs to do with as they direct. Small businesses should be allowed to share their data with whichever advisor they choose, recognising existing data sharing protections already in place.

3.13. *Insights exemption - need business exemption*

Rule 1.10A(3) outlines the 'insights disclosure consent'. This Rule allows an ADR to follow a process to share data with unaccredited third parties. Xero expects that this disclosure consent would allow small businesses to share some (not all) CDR data with third parties in Xero's ecosystem. The Rule however requires significant additional obligations on the ADR. This includes singular transaction transmission and keeping a copy of each insight, a record of who insights were disclosed to and a record of when insights were disclosed. Again, while the intention to enable participation is apparent, this Rule does not go far enough. Businesses should be given the freedom to share whatever data they like with third parties of their choosing.

CDR legislation components which need to be considered before Xero can participate

3.14. *Transitioning consents - needs insertion*

One of Xero's major frustrations with the CDR regime is that it does not recognise secure sharing of permissioned financial data has been operational in Australia for over a decade. Xero requires a customer to consent to share their banking data into their Xero account via our batch feeds. However, uncertainty exists on how Xero would transition customers at scale onto the CDR APIs. To minimise

service disruption for our small business customers, Xero seeks inclusion of recognition of existing consents for bank accounts that are currently sharing data with Xero. This would be a pragmatic approach to ensuring small businesses are not unduly inconvenienced.

3.15. *Testing scale - needs partnership*

Xero does not trust the CDR APIs will handle the demand should accounting software providers become ADRs. The load will be over two million new CDR consumers making multiple API calls per day. The industry will require load testing to have confidence our customers will have an experience under CDR that is the same if not better than what they have today. The minimum standard under the Data Standards would be unworkable for ADRs such as Xero. We are concerned that some ADHs may look at higher access rates as a commercial opportunity where the end user of the data may be penalised because of their consumer type.

4. Could the CDR legislative framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?

4.1. N/a

5. Are further legislative changes required to support the policy aims of CDR and the delivery of its functions?

5.1. Xero strongly believes that moderate legislative changes can turbocharge consumer outcomes without sacrificing security. Xero briefly proposes an ideal state and a compromise model for the Review's consideration which we would be only too happy to discuss in detail if required.

Ideal state:

Legislative amendments should be enacted to more closely align the CDR regime with the principles underpinning the working UK Open Banking regime. This reform would see the CDR framework continue to assess, prioritise and designate sectors for inclusion in the regime. However, at a high level, privacy requirements would be decoupled from the CDR regime and housed in the Privacy Act, and the inclusion of the concept of "derived data" would be removed.

The CDR regime should be limited to facilitating the transfer of CDR Data as designated in the instrument from a data holder to a data recipient in line with a customer's instruction. CDR protections should apply to transfers of raw CDR Data (as per the designation instrument) from ADH to ADR, and from ADR to third parties providing consolidated account information back to the customer, for example a financial dashboard app. Third parties not providing consolidated account information back to the consumer, for example trusted advisers or a credit check app would be able to share data with consent, protected by existing privacy legislation and frameworks.

If it is determined that the Privacy Act is not fit for purpose to protect transfers of financial data, then reform of the Privacy Act should be prioritised.

Compromise position:

Businesses have been able to instruct their bank to share their financial data with their accounting software for over a decade. Businesses share this data with their accountants and bookkeepers, accredited and unaccredited advisors and cloud-based applications, often daily or multiple times daily. Often, their operations rely on data sharing and any break can lead to challenges.

Reflecting the difference in how businesses use their data compared to individuals, Xero proposes an exemption for business data. This exemption would be available to an ADR which had received CDR Data from an ADH on behalf of a business for a business purpose. It would mean that any transfer of data from the ADR to a third party following the business's instruction and consent would be outside the regime.

This exemption would allow a business to benefit from the CDR regime's enhanced data coverage and quality features. However, it would allow a business to retain the freedom to request an ADR, for example Xero, to share its CDR data with any third party of its choice, as is enjoyed today. The business would continue to be protected by the framework of the Privacy Act, the ATO DSP Operational Framework, the SSAM and contractual arrangements.

[ENDS]