Verifier Submission
28 February 2019
Treasury Laws Amendment (Consumer Data Right) Bill 2018

Senate Standing Committee on Economics – CDR Bill
PO Box 6100
Parliament House
Canberra ACT 2600
By My Parliament Upload

Verifier Holdings Pty Ltd

Submission to the Senate Standing Committee on Economics on Treasury Laws Amendment (Consumer Data Right) Bill 2018

About Verifier

Verifier is a permission-based private data exchange platform for regulated markets that applies renowned Privacy-by-Design principles, respecting the information security needs of consumers and income data providers. Our clients include banks and non-bank financial institutions.

Lisa Schutz is Verifier's founder and CEO. Lisa was instrumental in founding the RegTech Association in 2017 and is currently a director of that Association. She was awarded the inaugural *FinTech Leader of the Year* in the Women in Finance Awards of 2017 and the *Thought Leader of the Year* in the Women in Finance Awards of 2018.

Verifier welcomes the opportunity to make this submission in respect of the Treasury Laws Amendment (Consumer Data Right) Bill 2019.

Verifier's comments and recommendations

We note specifically the goals expressed in the *Final Report* of the Review into Open Banking in Australia, published on 9 February 2018, being the creation of a system that:

- is customer focussed
- promotes competition
- encourages innovation, and
- is efficient and fair.

The purpose of our submission (and therefore the focus of our submission) is to advocate for the implementation of regulation that is efficient and fair and which embodies competitive neutrality.

Verifier Submission
28 February 2019
Treasury Laws Amendment (Consumer Data Right) Bill 2018

1. Prohibit Screen Scraping

A fundamental shortfall of the Bill is that it does not address the practice of "screen-scraping".

Our strong view is that the government should follow the lead of the European Commission's revised Payment Services Directive (PSD2), which (from mid 2019) prohibits accessing data through the use of screen-scraping techniques.[1] France, the UK, Germany, Luxembourg and Poland have finalised implementation of PSD2 and a number of other EU member states are working towards implementation.[2].

We note too that the Australian Government has taken the exact same stance – requiring that no corporate pretend to be a citizen. No one is allowed to "screen-scrape" Government data – that is why the Attorney-General's department built the Document Verification Service for identity data. If screen-scraping is not tolerated by the Government, why is the Government allowing it to happen in the corporate sector?

Competitive neutrality:

Aside from community trust and safety, there is another compelling public policy basis for our recommendation that screen scraping be prohibited. That is, in order to facilitate market efficiency, regulation should not create a competitive bias in favour of particular products or providers within a given market segment.

One of the principles of "good" regulation is that it should not impose competitive disadvantages – it should embody competitive neutrality. If screen-scraping is not prohibited by legislation, there will be a "race to the bottom" by those who use the "back door" to avoid the significant regulatory burden (including costs) of accessing and sharing CDR data in the transparent and informed consent driven model contemplated by the data right. A consequence of this would be to create a data access and sharing environment that lacks both competitive neutrality and appropriate protections for CDR data.

Verifier's recommendation:

We strongly recommend that screen scraping be prohibited. As this sentence is read, thousands of Australians are probably being asked to share their passwords and IDs to bank accounts, super accounts, telco accounts. They are at risk, as is the whole community due to the threat of identity theft. Do we want to sanction that,

[1] European Commission – Fact Sheet. *Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling customers to benefit from safer and more innovative electronic payments* MEMO/17/4961, Brussels 27 November 2017
[2] http://www.hoganlovellspayments.com/PSD2#

really? On a personal note, I would note that while companies like Verifier work tirelessly to make submissions to inquiry after inquiry, the majority of screen-scraping organisations just get on with their day job of harvesting consumer data to generate economic gain, safe in the knowledge that participation in the CDR conversation is optional.

We expect that this policy position will ultimately end in community outrage – privacy is not dead as the discussions around My Health Record have made all too clear. The Productivity Commission Inquiry into Data Availability and Use highlighted the value to the economy of more widespread data sharing. Why put that at risk and let this be the next topic of a Royal Commission.

2. Consent data designation

Consumer consents associated with CDR Data are a critical element of, and a necessary pre-condition for, access to and sharing of CDR data.

However, in the CDR Bill, consent data is not either directly or indirectly derived from CDR data, and therefore does not itself fall within the definition of CDR data unless and until that class of data is also designated by legislative instrument.

We strongly recommend that consent data should be a designated class of information in each of the sectors that are designated sectors. This will ensure that consent data, the "oil" that keeps the open banking system moving, meets all of the same standards as the CDR data it relates to and is managed appropriately by data holders and data recipients.

3. Complexity of privacy protections – modify the Privacy Act

The CDR Bill does address the proposed interaction between the Privacy Act and the Privacy Safeguards.

However, we remain concerned about the complexity and uncertainty that will result from a multi-layered approach to privacy protections. Particularly given the Privacy Safeguards will be supplemented by rules that are yet to be made by the ACCC under its rule-making power.

The complexity of this approach will significantly increase the cost (and time) of implementing the open banking data sharing environment, and will disproportionately disadvantage emergent market participants who cannot marshal teams of internal legal and compliance professionals to enable the required business outcomes.

Verifier's recommendation:

We recommend the multi-layered approach be abandoned. Instead, the existing privacy protections (under the Australian Privacy Principles and Part IIIA of the Privacy Act) should be modified as required to ensure appropriate privacy protections for CDR data.

4. Acceleration requires allowing for emergent data sharing

The time is now for increasing data availability because Australian industry and the community will benefit. Ironically, data sharing is the only thing likely to bolster Australian corporates against the domination of global tech platforms. The clamour of second tier banks to join up to CDR suggests that corporates realise the imperative to start sharing now – or become irrelevant.

A bit of history: We get to the Consumer Data Right as a result of a string of policy reviews the last of which, the *Final Report* of the Review into Open Banking in Australia, published on 9 February 2018 probably unfairly skews debate about the Consumer Data Right to banking.

The **problem with the Consumer Data Right** is that at the pace it is going it is not going to deliver any time soon on the policy goals of the Productivity Commission Inquiry into Data Availability and Use (No. 82, 31 March 2017), and its antecedents - both the 2014 Financial System Inquiry (the Murray Inquiry) and also the 2015 Harper Review of Competition Policy.

The brief given to the Productivity Commission from the Australian Government was:

The Australian Government seeks to consider policies to increase availability and use of data to boost innovation and competition in Australia and the relative benefits and costs of each option.

In our view the question is how to pick up the pace! Our thoughts are logged below but most of all we would like to task Treasury and the ACCC with an "acceleration KPI" in both the Bill and the Rules and see what the teams in both organisations can deliver. Our suggestions are:

- That the CDR Bill incorporate the potential for other sectors to opt-in ahead of Government designation
- Consideration be given to the introduction of an Assisted Compliance Period, with limited sanctions, to make it safer to opt-in, sooner
- That data holders who are not initial data holders (subsequent and reciprocal) can elect to be on the same timetable as the initial data holders
- That standard setting not be assumed to always be run by a single Data Standards Body – as is the case now. We would like to see provision for sectors to submit alternatives – which might be existing forums with deep domain knowledge. This would require a review and endorsement process to make sure all the requirements for a Data Standards Body are in place. This, we believe,

would share the load and prevent creation of bottlenecks in the path to CDR delivery.

- The same logic applies to the Accreditation Registrar. As we have said in previous submissions to Treasury - we see a need for the Accreditation Registrar to take the role of orchestration an accreditation industry rather than being a single utility (and point of failure). And, since this is a Bill designed to promote competition in the economy, it hardly seems appropriate to create a new oligopoly. As a result, some serious thought is needed to work out the right way to orchestrate such an industry. We see the potential to leverage the existing accreditation and audit teams out there - for instance in the infosecurity space - and believe that tapping into those resources to remove another bottleneck should be a goal of the CDR scheme.
- Moreover, we are sure that this list above is by no means exhaustive – we would like to see within the Bill, clarity around the importance of speed in all of this so that all parties within the CDR regime are incented to move at pace. Hence our earlier “acceleration KPI” comment.

5. One more thing – it's a customer data right – let's get the name right!

At the risk of creating marketing mayhem, this is actually a customer data right not a consumer one – it envisages sharing data for business as well as natural persons.

To aid clarity, our view is that references to "consumer" (including all of the definitions) should be changed to "customer".

In conclusion

Thank you for the opportunity to contribute to the review of the Consumer Data Right Bill.

We reflect again on the brief given to the Productivity Commission Inquiry into Data Availability and Use:

The Australian Government seeks to consider policies to increase availability and use of data to boost innovation and competition in Australia and the relative benefits and costs of each option.

We believe that the CDR has "good bones". Our recommendations are designed to support and strengthen the CDR and accelerate the outcomes it seeks to achieve.

Finally, we would be happy to discuss any aspect of our submission with the Committee. Please contact me in the first instance.

Sincerely
Lisa Schutz, CEO
Verifier Holdings Pty Ltd