Consumer Data Right

Data Standards Body Advisory Committee

Minutes of the Meeting

Date: *Wednesday 14 August 2019*

Location: *Commonwealth Bank of Australia, CBP South, 11 Harbour Street, Sydney*

Time: *14:00 to 16:00*

Meeting: *Committee Meeting No: 13*

Attendees

Committee Members

Andrew Stevens, DSB Chair
Kate Crous, CBA
Emma Gray, ANZ
Mark Perry, Ping Identity
Lisa Schutz, Verifier (via WebEx)
Ross Sharrott, Moneytree
Lauren Solomon, CPRC (via WebEx)
Stuart Stoyan, MoneyPlace (via WebEx)
Jamie Twiss, Westpac
Mal Webster, Endeavour
Viveka Weiley, Choice
Andy White, AusPayNet
Patrick Wright, NAB (via WebEx)

Observers

Warren Bradey, Data61
James Bligh, Data61 (via WebEx)
Rob Hanson, Data61
Terri McLachlan, Data61
Michael Palmyre, Data61
Mark Staples, Data61
Louis Taborda, Data61
Bruce Cooper, ACCC
HaiPei Zhu, ACCC
Angelica Paul, OAIC (via WebEx)
Daniel McAuliffe, Treasury (via WebEx)
Mike Booth, EY
Andrew Parton, EY

Apologies

N/A

Chair Introduction

The Chair of the Data Standards Body (DSB) opened the meeting and thanked all committee members and observers for attending the first meeting post the legislation being passed.

He also noted that Daniel McAuliffe will provide an update of the process on the Royal Assent in his brief introduction and noted that we are now in the phase of the rules being finalised in light of the legislation and then the standards will be reviewed in light of those rules.

It was noted that there has been some initial work done already to the standards in relation to compliance with the rules as they have been drafted. It was noted that there are a few areas where some further discussion will need to be held.

It was noted that the next step is the formal lock down of the rules and the standards for the February 2020 implementation. It was noted that everyone is working across the teams to work to that point.

The Chair advised that Viveka Weiley is moving on from Choice and will no longer be on the Advisory Committee. It was also noted that Warren Bradey has decided to depart Data61 to join a small listed company in the tech space. The Chair thanked both Viveka and Warren for everything they have done and in particular Warren for getting us to where we are.

It was noted that Mark Staples from Data61 will be the point of contact moving forward for the time being.

The Chair welcomed Mike Booth & Andy Parton from Ernst Young (EY). The Chair asked Bruce Cooper from the ACCC to extend an invitation to them to attend a meeting. It was noted that they will provide a run down in relation to the assurance process and testing at this meeting.

The Chair thanked Kate Crous from the Commonwealth Bank of Australia (CBA) for hosting the August Advisory Committee meeting.

Minutes

Minutes

The Chair thanked the Committee Members for their comments and feedback on the Minutes from the 10 July 2019 Advisory Committee Meeting.

The Minutes were taken as read and formally accepted.

Action Items

The Chair noted that the Action Item to include Product Reference Data Implementation has been included as an agenda item.

Technical Working Group Update

A summary of the progress from the last committee meeting on the Working Groups was provided in the Committee Papers and was taken as read.

The Chair noted that the way the legislation was passed was very helpful. It was noted that Daniel McAuliffe will provide an update on the amendment processes.

Product Reference Data Implementation

An update on the Product Reference Data Implementation was provided in the Committee Papers and was taken as read.

It was noted that some banks have published Product Reference Data (PRD) through APIs. The links to the APIs and general commentary are provided in the papers. It was noted that the DSB are keen to continue to work with the banks on interpretation and consistency of the data, particularly as more products are added over the coming months.

One member noted that access to "pings" on their APIs are mainly from Australia (98%), but pings from other places included the African coast, Ukraine, UK, NY, Silicon Valley, China and India. The member noted that a percentage breakdown will be provided to the Chair. The Chair noted that these metrics show interest in the CDR particularly in the Australian market and internationally as well. Another member noted that they have not looked at their ping map but will follow up on this and provide to the Chair.

ACTION: Committee Members to summarise ping data and send to the Chair.

A member noted that many FinTechs currently use an intermediary to gather product data. It was noted that feedback was received from some aggregators that they are not planning to migrate to use PRD APIs until enough other ADIs publish PRD using the APIs to avoid running parallel systems. It was noted that some of the fields that aggregators currently get (presumably) through screen scrapping won't be available through PRD APIs, but that they clearly like the conformity of the presentation of the information from the PRD APIs.

One member noted there are some issues in relation to initial implementation of Product APIs. One of the issues concerns fields that have limited ability to communicate information about tiered interest rates and fees for products. The concern is whether ADIs, in following the CDR regulation might potentially breach other regulations, as the standards cannot show the full product data. The member noted that they would like this looked at so they can be compliant. Part of that response may be to make the fields more flexible.

One member asked what the process was for gathering all the input on Product APIs. It was advised that the DSB will either do a workshop or open another GitHub process to gather the feedback. It was noted that the mode of control may change as we move from the early stage of development to production, and that feedback in relation to this would be appreciated. Another member noted that they have provided some feedback on GitHub, and DSB agreed that this would be considered.

Treasury Update

Daniel McAuliffe from Treasury provided an update on the Consumer Data Right Legislation as follows:

It was noted that the Bill was passed in both Houses on the 1 August 2019. It was confirmed that Royal Assent was on Monday 12 August 2019. An announcement is expected shortly on the DSB Body and the Chair.

It was noted that the Government undertook to introduce a Bill later this year (possibly September) to address changes about deletion of data. It was noted that the draft text for that was tabled in Parliament and is available on the Australian Parliament website.

It was noted however that the current Act gives the ACCC the power to make rules about deletion. The amending Bill would say ACCC must make rules about deletion. ACCC would retain flexibility to regulate the operation of this, including exceptions. It was noted that currently the ACCC rules require deletion or de-identification of data where an accredited data recipient has consents that expire or are revoked.

A discussion was held on how this compares to the General Data Protection Regulation (GDPR). It was noted that the amending Bill would allow the rules to go as far as GDPR. Moreover, the current draft of the rules in some ways goes beyond GDPR. For example, under GDPR consumers can contract out of the right to deletion, but that for the CDR the ACCC has decided that to protect consumers the right of deletion cannot be contracted out. It was noted that in the GDPR there are also other exceptions to do with keeping statistics, research and archiving. It was noted that those exceptions are not in the draft CDR rules currently.

A discussion was held that banks, as original data holders would not be subject to the right of deletion. The right to deletion only applies to data received under the regime by ADRs. There is a provision in the Bill that says ACCC can write rules to say data holders who are also ADRs that receive data as an ADR can in some circumstances cease to become an ADR for that data and instead be treated as a data holder for that data. It was noted for example that after using the CDR regime to support switching to a new bank, consumers would not want their new bank to be forced to delete their transferred data.

One member asked whether automatic deletion would eliminate use cases requiring ongoing access to historical data. It was noted that there are some exceptions in the Bill, and one is when ADRs are required by law to keep the data.

ACCC noted that in regard to exemptions, some will be in law and some will be in the rules. ACCC is looking to provide an opportunity for comment on new rules, to not miss important exemptions.

It was noted that the amending Bill is only for what the customer requests to delete. That will operate on top of provisions of the existing Act where when use permission run out or are withdrawn.

One member noted that a capability for consumers to withdraw all permissions would be quite useful.

A discussion was held on whether the deletion rules are only for banking, or will they flow through to other areas? It was noted that the current rules are in the context of banking and will have to be modified for future sectors.

One observer asked Treasury about the timing of the amendment Bill. If the Bill is introduced in September and goes through by February, would all participants need to comply with that by February? Treasury noted their reading of the draft amendment Bill is that existing rights to deletion in the current draft rules on the request of the consumer meet the requirements of the new Bill. If, however the ACCC does significantly revisit the current deletion rules, then that would be a matter for the ACCC.

ACCC noted similarly that the current draft rules could be taken to read to comply with the proposed obligations that the ACCC must make rules on deletion. Current powers to make rules on deletion and de identification in certain circumstances could allow the ACCC to go further, but if that was done the ACCC would need to allow for further consultation.

It was noted that deletion is triggered by loss of consent to use data. If a consumer asks a data holder to stop sharing data with a data recipient, that does not by itself trigger deletion. If a consumer has granted a consent to use the ADR, even if the data sharing arrangement finishes, the ADR may still be able to continue to use the data for that consented purpose. To trigger the deletion or de-identification obligation, the consumer needs to tell the ADR that they are no longer permitted to use the data for that purpose. It was noted that turning off the data sharing tap does not trigger deletion of the data.

It was noted that in regards to the Designation, Treasury are just turning it on for Open Banking. It was noted that lots of feedback was received in the last consultation and there will be another draft of the Designation next week. It was noted that Treasury is confident that the Designation will be finalised by the end of this month or shortly afterwards.

A discussion was held on the broadening of the regime for more banks and products. It was noted that the Designation will only say to turn on all ADIs and for all banking products as defined in the Act. It was noted that the ACCC rules determine the scope and timing of which ADIs get ruled in, and at what time.

The Chair congratulated Daniel McAuliffe for getting the legislation passed.

ACCC Update

Bruce Cooper from the ACCC provided an update on the Rules and the Directory status as follows:

It was noted that the scope in terms of which products come in and which APIs are turned on and when is still under consideration. It was noted that ACCC undertook to release a version of the rules that clarified scope for February 2020 at the beginning of August 2019. The ACCC remains keen to publish this after final consideration by the Government.

One member noted that they are already building towards a specific scope and they hope that ends up being complaint. The member noted it is now too late for them to adjust if there are major changes to the scope for February.

A discussion was held on whether if some banks were ready to publish everything, would the rules allow all the banks to launch with the minimum common level of data, which might be fairer. It was noted that ACCC would need to look at the scope first, and that there are some decision points between now and February. It was noted that the best approach would be the early announcement of the scope for February 2020 before we get to exemptions. It was noted that where there are areas where the standards are not developed for example, this would cause challenges for everyone. It was noted that in regard to an early announcement of the scope, that the ACCC have recently shared a critical time path document to the ABA and they envisage sharing something like that to the wider ecosystem.

One member noted that they are planning to do testing over the Christmas period, but if something happens in the industry like a payments issue or something that effects the economy, they will divert everything they have in the bank to solve that. The member noted that when ACCC publishes the testing timeframe, they should have a proviso allowing the banks to prioritise the economy over the legislation if some issue happens.

Another member noted that it needs to be clear in the testing plan that for them there is a month that is a complete block out as they have no access to use the test environments during that critical period. It was noted that the block out period for the banks is around the 8 December 2019 through to the 15 January 2020.

One member noted that the ACCC should have a way to adapt the timetable quickly if necessary.

One member noted that greater transparency would be useful on: the timeline to February 2020; what is going to come into play from the consumers perspective; what are the major issues that are still to be resolved within the Rules; and what is the process to engage on those issues? The member is very interested in consumer comprehension levels in the consumer experience for the standards and Rules.

One member asked in regards to the Privacy Impact Assessment (PIA), at what point would the PIA be completed on the rules and the standard in unison under the legislation. It was suggested that it would be useful to provide information on that at the next committee meeting.

ACTION: Treasury to provide an update on the PIA at the next committee meeting

A discussion was held on the communication of the regime. It was noted that now that there is legislation, Treasury could follow up on who and when public communication will emerge in relation to the CDR, and in what form it will be.

ACTION: Treasury to provide an update on the timing of the public communication

ACCC noted that they are working with OAIC and Treasury to have a common message. It was noted that the ACCC has a role around consumer experience and business guidance. It was noted that ACCC are looking to have standard messages and public FAQs.

A further discussion was held on what the UK experience meant and why there was not more take up earlier. It was noted that there were a number of issues, one was the accreditation list was 75 to 100 applications long so there were use cases that weren't accredited and therefore not available. It was also noted that after two years, several banks hadn't got to the conformance stage and that people didn't understand open banking. It was noted that the latest statistics show that there are now 135 account payment service providers in the UK for open banking. It was noted that it was low at the beginning, but there has been a reasonable amount of momentum in the growth.

A discussion was held on the accreditation requirements and process. ACCC noted that soon after the rules come out, they will publish guidance on requirements for accreditation. This will be much the same as previously exposed in terms of insurance and IT security. It was noted ACCC are on track to have the locked down version of the rules at the end of the month. It was noted that the Minister needs to approve the rules, and the rules won't clear the ACCC committee until 28 August 2019.

In was noted that the ACCC will provide guidance and explanatory notes for the rules and look to finalise in September 2019.

One member asked ACCC to discuss the registry regarding proposed differences from international standards, and how that might impact security or work required for participants. ACCC advised that there has been a request to do a workshop next week following the feedback they received from the earlier meeting today. The intent would be to get agreement on the solution and then look at impacts. One member asked why the ACCC decided to use variations from industry standards, involving a static registry. ACCC noted that they have been clear from the beginning that they don't want the register to be a single point of failure, and that this is driving the design of the register in this way.

One observer noted that there are interactions between the InfoSec standards and the register design. It was noted that the variations may not significantly increase implementation costs for participants. It was noted that the CDR standards use a number of different source standards. Most of those source standards were not designed for a many-to-many regime, nor for a regime with central control of the participants. There are some aspects of the CDR regime that have led it away from dynamic registration with a certificate authority as is used in the UK. Static registration with a central registry is a resolution of some legal enforcement scenarios in the CDR regime.

One member noted that the UK has a single registry and dynamic client works very well for that. It was also noted that the single registry talks to multiple data holders and data recipients.

One member encouraged the Chair to have another look at the registry with the ACCC, as there is a fairly widely held view among the members that a dynamic registry with off the shelf components would be more efficient and have better security.

One member asked whether there will be a security assessment over the ACCC solution similar to the Fortian review? The ACCC noted that the security of the system design has been a significant

part of work to date, that they have taken advice on it, and that there will be an independent security assessment of the solution.

A discussion was held on the ACCC workshop and ACCC have advised that the date has not yet been set. It was also noted that if the workshop is held next week, it will be too short notice for some international parties to attend. ACCC noted that they want to hold the workshop asap to look at the core problems and assess the pros and cons of each option.

One member noted that the UK would have opinions on why they decided to invest in an always up dynamic registry that everyone can talk to. One reason might be to revoke or stop false representation of accreditation. It was also noted in regards to being a single point of failure, the UK registry had been up for over 20 months without a failure.

One member asked ACCC whether there has been an update on intermediaries and / or using intermediaries to do accreditation. They noted that some FinTechs are concerned about the cost of insurance, security controls, and audit and that they would prefer to use a third party.

ACCC noted that although intermediaries are important, they are unlikely to be in the first version of the rules in August 2019, but that intermediaries may be able to be included in the Rules before February 2020. It was noted that accreditation rules will need to go out very soon to identify a core group of data recipients to be the first to go through the accreditation and testing. However, if managing the accreditation of this initial core group delays rules for intermediaries, then it is possible those rules may be delayed beyond February 2020.

A member noted that most FinTechs currently use a third party for data acquisition. ACCC noted that those intermediaries may have their own use for data, so they may want to be data recipients independently anyway. The ACCC noted that it is not yet decided whether an intermediary will have any different obligations in terms of being a participant to the system rather than a data recipient.

A discussion was held about how FinTechs could use only the insights from data rather than receiving the data. ACCC noted that this depends whether it is a genuine insight vs a subset of the consumer data being re-shared. ACCC noted that many intermediaries do share subsets to the data. It was noted that they need to treat the data going out of the system very carefully. It was noted that the idea of introducing intermediaries was to pair it with the introduction of tiering of accreditation.

One member noted that this is key to the uptake of how FinTechs in particular consume data. Also, a number of second tier banks and credit unions will consume data using an intermediary. It was noted that most organisations will go through an aggregator or through an intermediary for screen scrapping data. It was noted that for greater uptake, the CDR environment will need to show that it is better.

Treasury noted that the open banking report contemplated intermediaries and tiered accreditation. The rules contemplate that there would be data coming out of the system. The original vision was that it would not be self-contained, and that within the system there would be no more than two tiers of accreditation to facilitate all the smaller players to join the system. It was noted that the CDR needs to compete with the other systems. The goal is to reduce the overall level of privacy violations in the data economy.

One member suggested that a possible next step could be to set up an intermediary and tiers of accreditation working group. The Chair noted that the DSB could do that when it is being contemplated in the rules. The ACCC noted that they could organise a workshop around this.

ACTION: ACCC to arrange an intermediary and tiers of accreditation workshop.

ACCC advised that for testing, they are working as quickly as they can and have had discussions with the banks, ABA and individually. They also noted that arrangements for funding are in place to create a system that is secure.

The Chair invited Michael Booth & Andrew Parton from EY to provide an update on the test plan and conformance. Andrew Parton thanked the Chair for inviting them to the committee meeting and noted that they have spent a six-week period working with ACCC to define a strategy and make clear the objectives of the strategy.

It was noted that the ACCC considers that as lead regulator, they ultimately have responsibility for three things. Firstly, that the trust is established by ensuring end to end integrity within and across the CDR ecosystem for open banking. Secondly, that consumers can have confidence in the security and integrity of that regime, and thirdly that the CDR ecosystem goes into operation in line with the agreed time scales.

It was noted that there are three broad groupings of activities in regard to testing in the run up to February 2020: data holders, data recipients, ACCC and EY. Each will need to test their own technology to get to the point where they are comfortable that their technology works technically. EY then has the intent to bring these together to do industry testing incrementally. The plan is to ensure that participants can prove that they have built their API layers successfully before bringing participants together technically to share data and run a set of functional scenarios.

One member asked EY if they are clear yet on the criteria that they will apply to give their recommendation to ACCC? EY noted that they have done the strategy and the next stage is another level of detail in relation to the rules and standards to be tested, using an obligation traceability matrix. EY noted that it is their intent to make that available to participants in the coming weeks, and that this will give everyone a good view of test phases.

One member asked EY if they saw a credible path to 1 February 2020. EY noted that they see a possible path which will be continually assessed collectively.

One member noted that the committee needs to understand what EY's recommendation will hinge on, and what satisfactory looks like. EY noted that the intent is that this will be developed.

ACCC noted that they have had meetings with ABA and the big four banks and following that the ABA wrote to the Minister to say that this is possible for February 2020 even if the legislation passes in September 2019. One member noted that there was a list of things that needed to happen in order for the banks to deliver on that, but they don't believe those things were met within the timeline.

One member asked who is going to do the penetration testing of the registry and other components? EY noted that each participant would be responsible for penetration testing of their own components. It was noted that ACCC will do the testing of the registry. EY noted that they intend to do an ecosystem level penetration on the system.

One member noted that time needs to be built into the critical path to allow data testing.

One member noted that they understood all the constraints and the desire to keep the 1 February 2020 date, and that we are all going as fast as we can, but we are not far off the point of needing to understand what Plan B is.

One member noted that all the committee members received an email on 13 August 2019 from OpenID Foundation. They raised some issues stating that we may have some security attack vectors open. The Chair noted that we have had two independent reviews who have looked at the InfoSec requirements and they have said that the standards that have been developed are fit for purpose. The DSB noted that it will provide the information requested, referencing aspects of the InfoSec review and respond to their issues in writing.

One member noted that Fortian identified some areas to further improve security. Fortian notes that there is no requirement for fine-grained consent, but that fine-grained consent could further improve security by helping to limit data provided to Data Recipients to the minimum required for some product scenarios. Fine-grained consent would involve significant work in the definition and implementation of the standards. The DSB is considering a transition to fine-grained consent in a later major version of the standards, but not before February.

One observer noted that the OpenID Foundation have identified areas of departure from FAPI, but that they have not identified attack vectors or vulnerabilities arising from these departures. It was noted that the DSB is taking the feedback seriously. It was noted that some of the deviations that were identified are where we have made our regime more secure. It shouldn't be interpreted that a deviation is necessarily a vulnerability, as the CDR standards are more constrained than FAPI.

The Chair noted that the DSB will address OpenID Foundations issues and share the response with the committee.

ACTION: Chair to respond to OpenID Foundation and share response to the Advisory Committee.

One member asked that due to the breath of people who were sent the email, do we need to consider communicating this externally as people may think there is a vulnerability in the system? It was noted that if anyone has the link to the FAPI working Group repository, they will be able to view the comments directly. The Chair has asked Ross Sharrott from MoneyTree to communicate back to the OpenID Foundation to say that whilst we are taking their feedback very seriously, to avoid misinterpretation we would prefer to initially respond directly rather than in public.

ACTION: Ross Sharrott to reach out to OpenID Foundation and ask if they can hold off on wider distribution of the content

One member noted that on the InfoSec side of things, it would be very useful to have a central place for security issues.

Other Business

No other business was raised.

Meeting Schedule

The Chair advised that the next meeting will be held on Wednesday 11 September 2019 from 2pm to 4pm at Westpac Offices in Melbourne.

The Chair has advised that we will include as an agenda item for the next meeting the Operating Model.

ACTION: To include the Operating Model as an Action Item at the next Advisory Committee Meeting

Closing and Next Steps

The Chair thanked the Committee Members and Observers for attending the meeting.

Meeting closed at 16:07