Consumer Data Right

Data Standards Body Advisory Committee

Minutes of the Meeting

Date: *Wednesday 12 June 2019*

Location: *Data61, Level 5, 13 Garden Street, Eveleigh*

Time: *14:00 to 16:00*

Meeting: *Committee Meeting No: 11*

Attendees

Committee Members

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

Observers

Warren Bradey, Data61
James Bligh, Data61
Rob Hanson, Data61 (via WebEx)
Stuart Low, Data61
Terri McLachlan, Data61
Michael Palmyre, Data61
Mark Staples, Data61
Louis Taborda, Data61
Stephen Bordignon, ACCC (via WebEx)
Bruce Cooper, ACCC
Angelica Paul, OAIC
Daniel McAuliffe, Treasury

Apologies

Ross Sharrott, Moneytree
John Stanton, Comms Alliance

Chair Introduction

The Chair of the Data Standards Body (DSB) opened the meeting and thanked all committee members and observers for attending Meeting No 11.

The Chair noted that Ross Sharrott (Moneytree) and John Stanton (Comms Alliance) were apologies for this meeting.

The Chair advised that prior to the committee meeting the DSB, Data61, ACCC, Treasury and the big four banks held a teleconference with the Treasurer's Advisor on the Consumer Data Right (CDR) to clarify the Government's position and expectations on the timetable for implementation of the CDR regime. The Chair indicated the key point was that the legislation is due to be presented and passed through Parliament in the month of July 2019 to enable the previously advised February 2020 implementation date to proceed. The Chair advised that Daniel McAuliffe from Treasury will provide a further update later in the meeting.

The Chair noted that the Data Standards Body (DSB) published its recent comprehensive draft of the standards on 31 May 2019. The Chair acknowledged the huge amount of work the team did to pull together the draft. He also advised the DSB is very keen to receive feedback on the draft standards in the usual ways through GitHub and written submissions by Friday 21 June 2019.

The Chair also advised that he and Warren Bradey met with Payments NZ following an action point from an earlier committee meeting. He noted that Payments NZ are implementing a bilateral API powered payment regime. It was noted that it was not a Consumer Data regime per se or a data transfer regime, but rather a payments regime. It was noted that, similar to our CDR model, they are using some of the UK standards in that work, but fundamentally it is a bilateral contracted API regime for payments. It was noted that if there was a way we could assist them in what they are doing and vice versa we will learn from each other's work and to support this have agreed to meet on a regular basis going forward. The Chair noted he will consider further whether it would be beneficial to invite Payments NZ to be an observer at future Advisory Committee meetings. It was noted that whilst they are calling it Open Banking, it is materially different to our regime and the UK regime.

Minutes

Minutes

The Chair thanked the Committee Members for their comments and feedback on the Minutes from the 8 May 2019 Advisory Committee Meeting.

The Minutes were taken as read and formally accepted.

Action Items

The Chair noted that the Action Items were either completed or would be covered off in discussion during this meeting or future meetings.

The Chair noted that the CX Phase 2 interim update will be provided at this meeting and a more comprehensive summary of the outcomes will be provided at the July meeting.

The Chair noted that two papers were distributed by ACCC prior to the meeting. One on "Consumer Data Right - Guidelines on Insurance" and the other one on "Consumer Data Right - Guidelines on Security of CDR Data". The Chair advised that Bruce Cooper from the ACCC will provide a further update later in the meeting.

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.

A further update was provided on the API & InfoSec Security Working streams by James Bligh as follows:

It was noted that the May Draft Standards release, which was a cumulative summary of all the Decision Proposals released to date, was published on 31 May 2019.

It was noted that for a limited number of issues further specific consultation was requested as part of the May release.

As noted by the Chair the consultation phase is open through to 21 June 2019 and feedback will be received through GitHub, in formal written submissions, and at a series of planned workshops to be held within the next week in Sydney and Melbourne.

James Bligh thanked everyone for their teams' input and all the groups who up to that point had contributed in a concerted and rigorous manner. The Chair has asked James Bligh to provide a detailed run down of the feedback received by 21 June 2019 at the next meeting.

ACTION: James Bligh to provide a summary of the feedback on the standards at the July meeting.

The Chair advised that in his discussion with Adam Clark from the Treasurer's Office, he requested that if there are any tweaks envisaged for the legislation, we could get visibility on those early, so we can consider the potential implications for the standards and rules.

It was noted that the API and InfoSec stream is holding two workshops on 13 June 2019 in Sydney and 17 June 2019 in Melbourne to obtain further feedback on the May 2019 draft standards.

It was noted that a fortnightly call has been established with the Payments NZ API counterpart to identify cross learnings.

A discussion was held on the four areas of specific feedback that been requested from the community.

These areas are:

- Authorisation/Consent flows;
- Timing for inclusion of Consent API;
- Re-authorisation flows; and
- Implementation of Static or Dynamic Client Registration.

On the appropriate authorisation flows to adopt it was noted there are a number of divergent views held and further input will be sought prior to the Chair making a decision. It was noted that further CX testing is being undertaken for these flows and will provide input to the final decision as well.

In relation to the adoption of a consent API, the draft standards outline a series of three options upon which feedback is sought. It was noted that whichever position we take on a consent API it will be an incremental rather than a substantial change to the next version of the draft standards.

It was noted that the dynamic/static client registration is a decision that needs to be taken in concert with the registry design. The position currently articulated for static client registration is very much aligned with the collaboration undertaken with the ACCC. It was noted that the ACCC has published a draft working specification this week and any changes arising from that consultation will be reflected in the next version of the draft standards to ensure we stay aligned.

It was noted that the issue of an appropriate reauthorisation flow is heavily dependent on the CX testing to provide a better understanding of a customer experience perspective. Prior to making a final recommendation in this space we believe further specific community input, together with the outcomes of current CX testing, will be valuable.

A discussion was held on the divergent views on these topics and whether there has been any consideration of multiple potential future states. It was noted that for Consent API and Dynamic Static Client Registration, a dual solution is prohibitive and the standard needs to take a position on those two. For Re-authorisation, variable flows are possible and for the Consent Authorisation, variable flows are an option. Experience from other jurisdiction has indicated that variable flows can create regime wide friction and be less secure overall.

One member advised that their Board of Directors will need to be comfortable with the risks they are being required to take as some issues are far more risk based or more security based, and the preferences outlined to the DSB team are focussed on each institution's view on what they consider to be the most secure for their customers. To this end it was suggested that to accommodate these different views the DSB might consider allowing multiple implementation approaches and allow competitive forces of customers determine where they are most comfortable.

A discussion was held on the path to resolve these issues. It was noted that the DSB will receive feedback over the next two weeks and will make a decision by mid-July. The Chair noted that it is the DSB's intention to be in a position to advise of its decision on outstanding standards matters at the next committee meeting on 10 July 2019.

ACCC noted that they are on the path to work with the DSB to settle the remaining outstanding issues, such as authorisation flows and reauthorisation either through the standards or as rules. It

was noted that it will be important to keep the ACCC and the commissioner across any outcomes that might have an impact on the rules.

A member asked whether the rules will be finalised ahead of the legislation or is it dependent on the passage through parliament. ACCC advised that they can't formally make the rules until the legislation is passed but they intend to have a locked down version before legislation is passed, on the assumption that the legislation won't change.

A further update was provided on the Engineering Work stream by Stuart Low as follows:

It was noted that the draft standards were released on the 31 May 2019 and that the engineering stream has been working on alignment of its reference implementation suite to the updated standards and these will be demonstrated at the workshop that is being run tomorrow (13 June 2019).

It was noted that the DSB reference implementation suite had begun to be used for test payloads obtained from one of the banks.

One member noted that across the industry there is not a standardised product and that significant variances could arise in the published outcomes. It was noted that this is fine as long as it is conformant to the standards as the reference implementation suite is checking technical conformance to the standards. It was noted from that the reference implementation suite developed by the DSB will provide an eco-system demonstration from end to end to help participants assess product information delivery.

A further update was provided on the User Experience Work stream by Michael Palmyre as follows:

It was noted that the UX stream is reaching the end of CX round two testing which is due to be completed in late June after which the final reports will be prepared. There have been a lot of good research results provided on authentication models, authorisation flows, management dashboards and revocation and the next step is to analyse these results and provide recommendations. It was noted that regular blog updates on the research have been published for broader community review and feedback.

It was noted that the team ran a workshop last week, to close off the issues on the consent flow. The workshop was very successful, with a lot of people attending and engaged in information sharing. It was noted that there was a lot of input provided on the consent flows identified previously which were clustered. Attendees also identified potential solutions which the team will be reviewing, and which will be provided in a summary update to participants.

It was further noted that the consent flow workshop had over 40 participants including government agencies that were present. At the start of the day data holders and data recipients had the opportunity to share their current work on consent flows.

A member asked how comfortable we were with there being no consumer groups represented at the workshop. It was noted that CHOICE was represented at the meeting and whilst it was unfortunate some other groups were not able to attend this session, discussions had been held with

them on their views and input. It was agreed that advanced advice of workshop timings should be provided for future meetings to maximise collective contributions.

A member of the committee stated that his team was pretty impressed with a lot of the work to date and noted that the Data61 CX work looks like a solid ground to work from, but the devil is always in the detail when implemented. It was noted that some of this work will not get into version 1 of the standard and it was widely noted that it would have been useful if the UX work could have had a head start on the standards, which is a valuable lesson for subsequent sector implementations.

ACTION: Michael Palmyre to provide the Chair with a summary of what issues will be deferred to a subsequent version of the rules and standards.

A member asked given the timeframes, whether it would be useful for consumer organisations to send advice on consent flows to both the DSB and ACCC given the rules interact with the standards around the consent flows. It was noted that the ACCC are working quite closely with the UX team but would also be happy to receive direct feedback.

As part of a discussion on the importance of the inter-relationship between the CX, InfoSec and API work streams it was noted that the streams are having continual ongoing discussions and the CX findings will help inform any future adjustments to the technical standards.

It was noted that we have just completed 2 rounds of research across 3 streams (6 rounds in total) and engaged 64 participants on several focus areas like consent flows which has been split across steams to test variations like management of consent and authorisation, revocation flows and revoke, authentication and re-authorisation. It was noted that in total we have conducted 11 rounds of research with 145 participants in total. When we launch the second survey the numbers will increase to 195.

It was noted that in regards to the preliminary insights and proposals, the consent flow tested well and the barriers to adoption continue to be around clarity of data use and lack of transparency. It was also clear that consent depends on the value propositions being offered. This includes propensity to share, but also whether request is all or nothing, or whether it allows more granular choice.

A member asked for clarification on whether the CX team is testing different consent flows or just the one. It was noted there are slight variations to the consent flows, some might display data requests slightly differently or omit information and this is to generate insight. It was also confirmed that we are testing the redirect flow as an alternative.

It was noted that the dashboards and revocation flows were seen by respondents as intuitive, but participants looked for use cases, products/services to make sense of data sharing relationships. It also noted that showing purpose specifications and revocation messages in data holder dashboards assists informed customer management and assisted decisions regarding revocation.

A member noted that currently under version 1 of the rules there is no role for intermediaries to play. When a data recipient gets the data, they can't on share the data and there is no role for other data businesses to nuance the insights available.

It was noted that around the consent flow, some research participants showed apprehension around how the CDR data will be used post consent, stating that whether data is de-identified and re-used or deleted was not clear. Most participants expected the CDR data to be deleted post-revocation of consent. It was also noted that there is apprehension around how the data will be used after that consent period. The recommendation is likely to be that providing further clarity is necessary to facilitate trust and increase the propensity of consumers to share their data.

A member queried how much of this is initial apprehension and change resistance will dissipate over time. It was noted that in this phase of research, we selected more early adopters and younger people and noted the early adopters are still concerned about data sharing as they were not aware of how their data was being used. It was noted a lot of education is required and this may assist in concerns dissipating over time.

It was noted in respect of consent and revocation management that purpose specifications and revocation messages in dashboards assist a feeling of informed management and revocation.

A member asked whether there was any interest in people visiting their data dashboards. It was noted that this is a foreign concept at present and there were wide and varied responses on how they would prefer to do it.

It was noted that in regards to authentication, testing is being conducted across three different authentication models. These were “decoupled”, “redirect with known-channel” and “redirect with one-time password”. There was clearly a split between a desire for security and a desire for convenience in round one of the research and we are still waiting to see the results of round two. It was noted that models more closely designed to align with straight redirect models are closest to existing customer behaviours, and as such cause less confusion and result in less drop off.

It was noted in regards to the “decoupled” model that it was easily navigated by early adopters and was preferred by security conscious users, but not convenience seeking users. Some participants failed to complete this flow altogether. The instructions were very clear, and it was successful for those that were familiar with doing something like this.

It was noted that in regards to “redirect with known-channel” testing that this flow was considered successful, with low to no drop off risk. Entering a customer ID was seen as a risk by security conscious users, while others expected to put in their password. It was noted that there were concerns raised around splash screen spamming by several participants.

It was noted that in regards to “redirect with one-time password” this model mostly aligned to existing behaviour, was likened to a straight redirect flow and was completed successfully and with ease by participants. There was some limited confusion around a lack of a real password and queries around lack of details on security/privacy.

It was noted that the agencies are still working on the comprehensive findings and once we receive this it will be reviewed by the team.

One member noted that from all the feedback that he has received from their team, they are gravitating towards the redirect, one-time password option. However, it was suggested it would be

helpful if this model was covered in the independent InfoSec review to consider any issues from that perspective.

It was noted the next step will be to prepare final reports and consider the outcomes with ACCC, Treasury & OAIC prior to developing recommendations. It was noted that the team is also synthesising the workshop outputs so that we can present the consent flow and language for further consultation. It was noted we will conduct a subsequent survey on language to close off language guidance and also conduct rapid final testing of other revised flows.

Key issues for ongoing review

The Chair noted the papers included a matrix of key issues for ongoing review as Appendix A. It was noted that this is a composite list of the issues requested for further review, including whether there is consistency on their treatment between the Standards, Rules and legislation.

It was noted that the issues matrix is not a complete list of issues outstanding, and the Chair has asked all members, ACCC, Treasury and OAIC to come back with any feedback on further issues to be included. It was also noted that the matrix should include any interdependencies between agencies. It was noted that the DSB will oversee the compilation of the issues but depending on who the relevant issue owner is and the interdependencies, it will vary as to who will need to action them.

ACTION: Committee Members and agencies to provide feedback on the key issues.

Treasury update

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

It was noted that the main comment is that the government is very committed to driving the CDR regime forward quickly and that this commitment is coming from both the Treasurer's and the Prime Minister's offices.

It was noted that in the meeting prior to this the Treasurer's office indicated that they were going to reintroduce the bill into Parliament as a priority in the July sitting. It was confirmed that there is not expected to be any substantive changes to the bill when re-introduced to parliament.

It was noted that the Parliamentary timetable was issued last week, and the sitting days are the three weeks in July, there will be nothing in August and then the next sitting will be the two middle weeks in September.

It was noted that the Designation Instrument is ready to go out subject to approval by the Treasurer and that it has tightened up greatly on the extent to which derived data can be made subject to Open Banking through the rules. He noted that the actual data sets to be covered in the first implementation phase were set out in the data payload standards.

It was noted in regards to CDR implementation for energy, the next step will be to release a consultation paper on energy data sets. In regards to the timing of energy, it was noted that last year COAG endorsed an implementation in the 1st half of 2020 and that the initial implementation will focus on the electricity market. It was noted that this timing will be reviewed again.

It was advised the Government is still intending to proceed with the current implementation timetable, with the expectation to launch Product Reference Data as a voluntary implementation from 1 July 2019 and for mandatory Product Reference Data implementation to happen one month after the bill passing. It was noted that the timetable for making available phase one of consumer data is still scheduled for February 2020, acknowledging that this is based on the government being successful in getting the legislation passed in July.

It was noted that Treasury will be engaging an independent consultant to review the Privacy Impact Assessment, and this will look at the privacy risks and mitigants in the CDR regime as a whole (the Bill, the Rules, the Standards and the Accreditation Register). It was noted that this assessment will kick off shortly.

It was noted that there is a commitment for several types of testing to occur as soon as possible. It was noted that there is acceptance that we will launch when the testing determines that it is good to go and there is recognition that adequate testing is one of the points of risk for implementation. The Chair noted that when he met the former Treasurer he was very aware of that.

ACCC Update

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

It was noted that ACCC will shortly publish a position paper on the recommended data access model for energy. The question is whether or not CDR utilises AEMO as a data holder and that would lead to further work around what that means for consent flows in energy. It was noted that if it is decided to use AEMO as a data holder or one of the data holders, then the consent flow won't mirror the banking regime.

A discussion was held on policy issues that are raised by taking a different approach in energy and who has the ultimate responsibility for resolving issues like creating a pool or a gateway as this is a policy issue. It was noted that the data access model is a fundamental design issue so Treasury is working very closely with ACCC. It was noted that the legislation will specifically apply for this type of model.

It was noted that the ACCC recommendation is likely to be to use AEMO as a gateway. It was noted that no party holds all the consumer data which is part of the problem and there will need to be combinations put together to meet data transfer requests.

The Chair noted that the DSB made a submission in regards to energy model which has been considered.

A discussion was held on the fundamental question about how standardised we need the CDR to be to operate successfully across multiple sectors. It was noted the standards for the first sector were

designed to be tailored for the requirements of different sectors. However, it was agreed the gateway model looks like it could be more divergent for other sectors.

It was noted that the rules don't currently cover tiered accreditation but ACCC recognised that tiered accreditation will be essentially to facilitate transfers between sectors and to enable greater granularity in data transfers.

It was noted that there was interest in understanding the Australian position on liability issues as this was a big issue in the UK. It was noted that it is different for CDR as the legislation includes specific provisions that note that data holders do not have a liability if they have appropriately allowed a transfer and the data is subsequently misused by a receiving party. It was noted that if data is not used in accordance with the rules and standards, then the liability rests with the accredited organisation which holds the transferred data.

It was noted that ACCC have also looked at the occurrence of a malicious hacker who hacks into the data of the data recipient, or an outsourced data provider. The rules currently specifically place responsibility for security and any liability with the data recipient.

It was noted that ACCC will provide an explanatory paper on liability. ACCC asked members to provide any specific use cases they would like to see addressed in that paper. It was noted ACCC will provide this paper to members out of session of the meetings.

ACTION: Committee members to provide specific examples to ACCC on possible liability use cases.

In was noted that the draft accreditation guidelines that were circulated to members with the committee papers were also circulated to Fintech Australia, ABA, COBA and the Insurance Council. It was noted that ACCC are seeking limited consultation on these two aspects of the accreditation guidelines. The guidelines on the "Audit Template" are designed so that data recipients will be able to use these to understand what they need to do to become accredited and maintain accreditation. It was noted that it is ACCC's intention to have a streamlined approach to the ADIs. ACCC have asked for feedback on these documents by 28 June 2019.

ACTION: Committee members to provide feedback on the accreditation guidelines to ACCC by 28 June 2019 to ACCC-CDR@accc.gov.au.

It was noted that ACCC have obtained feedback from the insurance industry that the CDR risks are insurable.

One member advised that the feedback they have received is that whilst insurance cover may be theoretically possible they do not think it is practically possible to provide appropriate cover.

It was noted that ACCC will reach out to the Insurance Council and clarify that these policies are available and who is offering them.

ACTION: ACCC to clarify what policies are available with the Insurance Council.

It was noted that the ACCC have published the Registry API specifications on GitHub and are seeking comments through GitHub. The site can be found at https://cdr-register.github.io/register/

Other Business

The Chair advised that at the next meeting we will add as an agenda item a review of the implementation status of the Product Reference Data implementation.

ACTION: To include Product Reference Data Implementation as an agenda item for the July meeting.

The Chair thanked Michael Palmyre for his CX presentation and update and looked forward to seeing the full details of the CX review at the next meeting.

Meeting Schedule

The Chair advised that the next meeting will be held on Wednesday 10 July 2019 from 2pm to 4pm at the Data61 offices in Eveleigh.

Closing and Next Steps

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

Meeting closed at 16:02