Consumer Data Right

Data Standards Body Advisory Committee

Minutes of the Meeting

Date: *Wednesday 10 July 2019*

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

Time: *14:00 to 16:00*

Meeting: *Committee Meeting No: 12*

Attendees

Committee Members

Andrew Stevens, DSB Chair
Kate Crous, CBA
Mark Perry, Ping Identity
Lisa Schutz, Verifier (via WebEx)
Ross Sharrott, Moneytree (via WebEx)
Lauren Solomon, CPRC (via WebEx)
Stuart Stoyan, MoneyPlace
Andy White, AusPayNet (via WebEx)
Patrick Wright, NAB (via WebEx)

Observers

Warren Bradey, Data61
James Bligh, Data61
Rob Hanson, Data61
Terri McLachlan, Data61
Michael Palmyre, Data61
Mark Staples, Data61
Louis Taborda, Data61
Bruce Cooper, ACCC
Alex White, ACCC (via WebEx)
HaiPei Zhu, ACCC
Angelica Paul, OAIC (via WebEx)
Daniel McAuliffe, Treasury
D'Arcy Mullamphy, Treasury

Apologies

Emma Gray, ANZ
Jamie Twiss, Westpac
Mal Webster, Endeavour
Viveka Weiley, Choice

Chair Introduction

The Chair of the Data Standards Body (DSB) opened the meeting and thanked all committee members and observers for attending Meeting No 12.

The Chair noted that Emma Gray (ANZ), Jamie Twiss (Westpac), Mal Webster (Endeavour) and Viveka Weiley were apologies for this meeting.

The Chair advised that the Advisory Committee has been re-constituted, and the members are again appointed by the Chair as personal appointments for their expertise for the 2019/20 year.

The Chair noted that a separate Advisory Committee will be established for other sectors, such as Energy, when the timing becomes clear. The Chair thanked the current committee members for accepting the invitation to remain as members for the forthcoming year.

The Chair noted that Australia now has available the first live publication of API-based feeds for Product Reference Data utilising the CDR standards. It was noted that the CDS team has developed a technical product comparator to ingest the API data and show the output in a human readable form. It was noted a demonstration would be provided after the meeting.

The Chair acknowledged the contribution and thanked those organisations who have published their data and others who are still working on it. It was agreed it is a good milestone, with a lot of exciting stages coming.

The Chair noted that subsequent to the release of the updated May draft of the Standards on the 31 May 2019, the DSB received submissions from 12 organisations and 1 individual with multiple submissions from the organisations. It was noted that the API Lead will provide a summary of the submissions later in the agenda.

The Chair noted that the second phase of the CX research was also completed and has provided some good guidance on key issues and highlighted other areas where the regime would benefit from further CX work. It was noted the CX Lead will provide a summary later on in the meeting.

The Chair noted that in a recent interview with the Treasurer, he noted that one of the priorities of the Government after passing tax cuts, is the introduction of the Consumer Data Right regime and delivering lower energy prices through the Consumer Data Right.

Minutes

Minutes

The Chair thanked the Committee Members for their comments and feedback on the Minutes from the 12 June 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.

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.

Summary on feedback on the standards

An update was provided on the feedback received on the 31 May draft of the standards by the API Lead, James Bligh. The presentation included the following points:

It was noted that the May draft included extensive consultation with eco-system participants in the lead up to publishing of that draft and also during the three-week consultation afterwards.

It was noted, in summary the matters that were raised consists of 18 matters related to the API standards, 6 matters related to the InfoSec Profile, 12 minor matters and 10 clarification questions. Of these matters, 3 were classified as complex i.e. they need their own decision paper to close them out, and 8 of those matters were restatements of previous feedback. Approximately 55% of new matters raised have been incorporated directly.

A query was raised on the basis for the DSB request for feedback to be consolidated through the ABA. It was noted that the banks regularly hold different views and that the ABA will not be able to bring forward a consolidated view. It was advised that the intention was not to discourage individual bank submissions but rather as part of the regular DSB-ABA Technical Working Group meetings, it was encouraged for the industry group to consider if it could find a common position on a number of the complex matters being considered by the DSB Chair.

It was noted that the amount of actual feedback was on par with previous consultation phases and the detail was a lot deeper and was much more directed to specific issues in the standards. This is considered an indication of the maturing nature of the standards and where we are in the cycle to finalising a version 1 release.

A discussion was held on the matters that were restatements and as to whether they were restated because the DSB had disagreed with those matters and did not include them in the draft standards or whether they were restated because it felt the DSB was still to consider those matters. It was noted that there was nothing submitted that hadn't previously been openly discussed and had a response provided, noting what alternative position had been decided. One member noted that they felt that the response that was provided was inadequate or their concerns had not been fully understood.

The Chair noted that before any decision is made the Decision Proposals are circulated to committee members for review and further feedback after which the Chair makes a final decision.

The Chair suggested that given there were only eight matters in this category that it might be a good opportunity for the Committee to go through them as part of the current meeting.

It was noted that one of the key pieces of feedback was that there would be benefit prior to the draft release for an independent review of the Information Security Profile. It was noted that after completing an RFP process, Fortian Pty Ltd was appointed to review the information security profile and standards for any key security issues. They were chosen based on their track record for using the protocols and their experience in financial services. They were also noted as not currently engaged in any implementation of the CDR regime to avoid any perceived or real conflict of interest.

A further discussion was held on parts of the standards relating to the interactions with the register and whether that will be covered. It was noted that the InfoSec profile that was released in May had some assumptions around the interactions with the register and have been incorporated. These assumptions are based on recent discussions with ACCC on their design thinking at the time and will be adjusted if the final design has any new implications for the standards.

A member noted that one of the most important security elements of this regime is the handshake between everyone and the register. It was noted that the component of the handshake between holders and the register is in the InfoSec profile but the final design of the register going back into ACCC is not settled. It was noted that the actual interactions between holders, recipients and the register are included in the InfoSec profile and that the only component not included is the content of the metadata payloads which would not be not considered as InfoSec profile.

It was noted that a draft of the independent report from Fortian Pty Ltd has been received and is being reviewed internally prior to publishing as part of the next version of the standards. It was noted that overall the review indicated that the InfoSec was fit for purpose for the first round of implementation. It was noted that they did raise some minor issues that will be incorporated into the next release.

It was agreed that the key matters where input was sought on the May update would be considered first, followed by a review of the current decision position on the eight other matters noted previously.

It was noted that with regards to the key issue on “authorisation flow” this covers the standard to be applied to the flow for giving consent starting from the recipient to the holder and back again for the initial provision of consent and authentication of the customer in the process. It was noted that six of the submissions contributed to this issue and also that the findings from the CX review and the InfoSec review were incorporated in reaching the recommended position. The ABA also provided in their submission three principles which were very helpful in assessing the options we had on the table.

It was noted that the InfoSec review highlighted the advantages of using a well-defined standard. The InfoSec review was completed by cyber security experts and was therefore noted to be heavily weighted towards the use where appropriate of pure standards.

It was noted the CX research identified the best low friction flows were those with a pure redirect flow.

It was noted that the ABA principles 1 and 2 advantaged the redirect flow. The first principle being the design of the authentication process in the scheme should allow for the proactive detection of fraudulent activity. The second principle being the authentication process should not require a consumer providing a banking credential to a third party.

A member suggested that the best way to drive a low fraud outcome is through the use of a decoupled authorisation flow, which is also well known and well accepted.

It was noted that of the five options that have been considered by the DSB, two are decoupled and asynchronous and three leverage a redirect model but have different forms so they have variations on pure OICD redirect but the three redirect have similar characteristics. This is confirmed from the feedback received.

It was noted that the independent information security review highlighted that all five options provided a reasonable level of security for the first implementation. It was noted by one member that re-builds and moving between options is a costly exercise and encouraged a decision that is able to incorporate expected extensions of the CDR regime for the known future states.

It was noted that the independent security review, the CX research and through industry, feedback suggests that for whilst choice of flow is important, knowing what secure behaviour looks like over time is an essential prerequisite to participating in new service delivery approach.

A discussion was held on the broader regime security profile and how there is confidence that the CDR regime is sitting in a safe ecosystem. ACCC advised that cyber security advisors have been working with them for some time and that they have identified approximately 300 potential threat vectors and prioritised what the ACCC need to do, and in what order. It was noted that security is definitely in the forefront of consideration by the Commissioners.

A member asked whether the Data Standards Body has come to a preferred position on the authorisation flow, and it was noted that they are close, but have not made a decision as yet and that the Chair would consider further input from the technical meeting to be scheduled later in the week.

It was noted that in relation to the key matter of “Consent” there are a number of matters covered under this umbrella. In particular, there was feedback from participants about the need for a centralised consent dashboard and fine grain authorisation as well as whether there is a need for a Consent API to be specified in version 1 of the standards.

A member noted that it is one thing to say the basic framework we are building might have a centralised dashboard, but the other way is that the system allows market forces to naturally come up with the solutions. It was noted that this is key consideration factoring into this choice and it was confirmed that centralised dashboards are not included for version 1 of the standards. However, the need will be monitored, and subsequent versions will implement appropriate changes to facilitate emerging needs on dashboard management.

It was noted that many potential CDR participants believe that there will be a need for finer granularity of authorisation over time. The concept of fine-grained authorisation was noted to have been raised on a number of occasions. It was also noted that this concept is not intended to be

incorporated into version 1 of the Rules, but rather it will continue to be worked through with the community needs and where consumer confidence lies in this process.

The Chair noted that this is an area where the weighting is to design for known requirements and not extrapolate for what "might be".

One member raised a matter about the consent discussion and that their view is that there is no need to consider or think about central controls points at this stage and that market participants could facilitate that where there is sufficient demand.

Another member suggested that fine grain consent does not need to be an integral part of the CDR if you allow for the role of intermediaries to provide the fine-grained consent.

The Chair noted that consent will be an important issue to get right as it will have implications across all sectors and will be critical in building consumer trust in the system and as such appreciate that there are many views on this issue and determining an appropriate balance is key to success.

It was noted with regards to the key "Operating Model" matter that there is an existing Decision Proposal on ongoing maintenance and curation of the standards for the banking sector still open on GitHub which will be important to reach agreement on during the testing phase. It was noted that the Operating Model will need to remain flexible and accommodate implementation learnings as the process moves forward. It was also noted that the likely scenario is that the regime will adopt two modes, one being more like what we have been doing, regular broad-based consultation and the other mode is more iterative for specific adjustment required to implemented standards.

One member suggested a third model will be to manage 24/7 facilitation for security patching issues, leaks and breaches etc. It was noted that this is intended to be picked up under the second mode of the iterative model but recognise this will be made more explicit in line with the feedback received.

The Chair noted that it would be appropriate for the remainder of the meeting to move to review the eight restated matters highlighted earlier, to give some further clarity on the underlying points of view.

It was noted that with regards to "Product bundling" that the current draft standards include it so that it allows for the existence of a bundle to be known and for additional information to be linked aiding decision making for a customer. It was noted the intention was to work with the community to develop furthermore detailed end points for a broader inclusion of product bundles in a subsequent version of the standards.

The feedback received concurred that product bundling needed detailed development of appropriate end points to handle the multiple product bundling that are offered by Data Holders and that product bundling should be excluded from the standards until that development work is completed. It was noted that whilst all parties agreed that a full development would not be possible for a February 2020 implementation that members had a different view on whether it would be confusing to consumers to leave product bundling out altogether or more confusing to require consumers and Data Recipients to go to another link to identify product bundles applicable to their accounts in the interim more detailed development phase.

A member noted that this is still on their list of important matters as they did not feel that the discussion had adequately addressed their concerns. It was agreed this would be discussed further at a separate meeting of the technical representatives of the Committee Members.

It regards to "Pending Transactions", it was noted the current draft standards require pending transactions to be included. It was noted that this is intended to be to the same extent that they are included in other digital channels available to consumers. It was noted by one member that the feedback received requested that pending transaction be excluded because of the institutions processes for linking pending transactions to post transactions is inconsistent across institutions and is difficult to reconcile to final posted transactions.

It was noted that with regards to "Transaction Search" the current draft standards require Data Holders to provide an ability through the API's for consumers and Data Recipients to filter on text-based data prior to it actually being downloaded by the Data Recipient. This has been included to support the Data Minimisation principle in the rules.

Feedback provided by some Committee members noted that "search" is computationally difficult and difficult to guarantee accuracy and as such were querying whether it was better done at the Data Recipient side.

It was noted this could be offered as an optional service to enhance customer engagement at a competitive market level.

It was noted that with regards to "Pagination", the main area of consideration is whether to adopt the curser-based pagination or random-access pagination. At present the draft standards have proposed a page based or random-access based structure as this provides greater flexibility to CDR participants whilst still enabling cursor-based pagination to be implemented.

It was noted that the feedback provided was a preference to only have curser-based pagination as it is the more standard approach for some banks.

In respect of the feedback on "Bulk Transaction Data", it was noted that the matter covers bulk transaction end points where a Data Recipient can ask for multiple accounts in one call. It was noted that the UK had these and made them optional with the result that very few institutions implemented the optionally end points for a variety of reasons, which meant that Data Recipients need to make an unspecified number of additional calls on the Data Holder API to receive data. It was noted that the UK regulators have encouraged us to move to a mandatory position on this matter.

As an example, provided behind the reasoning of including Bulk Transaction data as a mandatory inclusion, it was noted that in a scenario where a recipient receives consent to access say five accounts on a daily update basis then the model gives the transaction for these five accounts in a single call. The alternative where Bulk Transaction data is not mandatory would lead to Data Holders receiving additional calls each night, which when extended out over multiple consumers and multiple data recipients could affect the demand on access to Data Holders. It was noted that it was considered that the feedback concerns on high quantity of downloads at once has been addressed in the NFR's which limit the number of unattended calls a Data Recipient could make in a 24-hour period.

The Chair noted that the feedback from the banks is that Bulk Transaction Data should be excluded at least in version 1 of the standards and the call rate be monitored for any drag on the efficiency of the API calls.

In relation to the feedback on "PII Data", it was noted that the current draft standards have minimised the data to be included and aligned disclosure requirements to the Rules which itself is taken from the Designation Instrument. Taking out more data at this point means the standards would not be compliant with the Rules.

It was noted that some members held a view that too much PII data was still being required to be transferred.

The Chair noted that this is a Designation and Rules question not a Standards question. It was noted that Treasury and ACCC would further consider the points raised by Committee members.

It was noted in relation to "Scope/Data Alignment", that the current draft of the standards aligns the scopes to the data cluster language based on CX testing so that when the customer is asked "do you authorise the sharing of the data", it is meaningful to the customer based on sharing. It was noted that the key feedback was to a technical preference to align scopes to the API structure and the data entities.

It was noted the decision will need to determine a balance between the CX findings with consumers for scopes to be easily understood and the requirement for technical alignment of data scopes.

In respect of the matter raised on "Access Token TTL", it was noted that the feedback suggested that the banks should be able to set the length of time for the access token at their discretion. This compares to the current draft of the standard which stipulates a 10-minute interval and is based on the CDS teams understanding of the position put forward by the ABA. One member indicated this may be not the interpretation that the banks were seeking to suggest. It was noted that the reason we have set a fixed length is because we are using that for some of the measurements for other SLA's. We have, with an ability for banks to shorten this where they are under anomalous security attacks. To prevent over use of this period the NFR for this section proposes that an unattended recipient can only do four sessions in a 24 hours period. The InfoSec review report indicated that 10 minutes is a reasonable set of time.

A member noted that 10 minutes is unusually long time for banking sessions, and it is more generally around the 3 to 5 minutes. It was noted that the longer the time the greater the risk. It was noted that the issue mainly revolves around the ability to have sufficient flexibility to deal with threat situations.

It was noted that it would be acceptable to have more sessions, for a shorter duration as this enables a judgement to be made to weight security over capacity.

The Chair noted that an out of session meeting will be scheduled in the next couple of days to discuss the outstanding items so a definitive decision can be incorporated into the July standards update.

CX Phase Two Update

The Chair noted that the CX Lead will circulate the summary of the CX Phase 2 Results and Recommendations presentation that had been prepared for the meeting.

Product Reference Data Implementation

A demonstration of the DSB product comparator results was due to be provided at the meeting. A demonstration was offered after the meeting.

Treasury Update

Daniel McAuliffe from Treasury was due to provide an update on the Consumer Data Right Legislation at the meeting. The key items noted was that the legislation was scheduled to be reintroduced into Parliament in July.

ACCC Update

Bruce Cooper from the ACCC was due to provide an update on the Rules and the Directory status. This agenda item was deferred to the next meeting.

The Chair noted that in regards to the briefing paper on liability that was circulated by the ACCC, this paper was very helpful and that this issue needs more visibility.

The ACCC noted that if further scenarios were identified by Committee Members, ACCC would be happy to receive those directly and test them against or add them to the current guidance.

A member has asked if the liability paper will be publicity released and the ACCC advised that at this point, that isn't the intention, but that they will take it under consideration to release with the broader guidelines being developed for accreditation.

It was noted in regards to the action item for ACCC to clarify what polices are available with the Insurance Council. It was noted that the ACCC have received feedback that insurance cover will be available for CDR related risks. Some members felt this needed testing further and offered to work with ACCC on obtaining quotes.

Other Business

No other business was raised.

Meeting Schedule

The Chair advised that the next meeting will be held on Wednesday 14 August 2019 from 2pm to 4pm at the Commonwealth Bank of Australia Offices in Sydney.

Closing and Next Steps

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

Meeting closed at 16:08.