Consumer Data Right

Data Standards Body Advisory Committee Banking Sector

Minutes of the Meeting

Date: *Wednesday 11 December 2019*

Location: *CBA, Level 19, 727 Collins Street, Melbourne*

Time: *14:00 to 16:00*

Meeting: *Committee Meeting No: 17*

Attendees

Committee Members

Andrew Stevens, DSB Chair
Emma Gray, ANZ (via WebEx)
Mark Perry, Ping Identity
Lisa Schutz, Verifier
Ross Sharrott, Moneytree (via WebEx)
Stuart Stoyan, MoneyPlace
Erin Turner, Choice (via WebEx)
Jamie Twiss, Westpac (via WebEx)
Mal Webster, Endeavour (via WebEx)
Andy White, AusPayNet (via WebEx)

Observers

Barry Thomas, Data61
Rob Hanson, Data61
Terri McLachlan, Data61
Michael Palmyre, Data61
Mark Staples, Data61 (via WebEx)
Louis Taborda, Data61 (via WebEx)
Bruce Cooper, ACCC
Daniel McAuliffe, Treasury (via WebEx)

Apologies

Kate Crous, CBA
Lauren Solomon, CPRC
Patrick Wright, NAB
Ying Chin, OAIC
Matt Clifford, APRA

Chair Introduction

The Chair of the Data Standards (DSB) opened the meeting and thanked all committee members and observers for attending the last meeting of the year, meeting no 17.

The Chair noted that the first thing he would like to do is introduce Barry Thomas who is the newly appointed Director of the Data Standards Body. His previous role was as Director of Open Banking Standards with the ABA. The Chair asked Barry to introduce himself to the Committee.

Barry Thomas noted that a number of the committee members will know him already from his previous role and that he is very familiar with the whole open banking journey. He noted that prior to being involved in the open banking process he had a lot of experience with the LIXI standards body for mortgage lending which started from literally nothing, and that body continues to run to this day with membership and licensees across the mortgage lending industry. It was noted that he was also very involved in a lot of the early stages for what is now PEXA, particularly in the work to define the underlying messaging standards and figuring out what sort of messages were going to be necessary to support online conveyancing. It was noted that the ABA experience enables him to hit the ground running.

The Chair thanked Barry and welcomed him again to the role and to the implementation of the Consumer Data Right.

The Chair noted that we have managed to extend James Bligh's contract to keep him involved, which we think is very useful. It was noted that he is working on the standards in both the banking and electricity contexts.

The Chair noted that we had the second meeting of the Energy Advisory Committee meeting this morning. It was noted that even though the energy sector data is not yet designated and timing remains unclear we are, as we did well early on in banking, setting up the Framework, the ways of operating and principles. It was noted that while it has it challenges, the benefits of having a totally different sector in terms of data holders, data recipients, structure, the data itself, the industry dynamic etc. is a very useful one in terms of really exploring the requirements of an economy-wide regime.

The Chair also mentioned that Gartner are holding a Data and Analytics Summit in Sydney on the 17 & 18 February 2020 and they have asked if he would not only speak but put together a panel and thus the Chair is reaching out to see if any committee members would be interested in joining the panel. It was noted that the topic is on "How to capitalise on the Consumer Data Right in the context of Rethinking Consumer Insights Strategy in the New Data Economy". The Chair asked members to let him know directly or via the DSB if they are interested.

It was noted that Kate Crous from CBA, Lauren Solomon from CPRC, Erin Turner from Choice, Patrick Wright from NAB and Ying Ching from OAIC were apologies for this meeting.

Minutes

Minutes

The Chair thanked the Committee Members for their comments and feedback on the Minutes from the 13 November 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 scheduled discussions.

The Chair noted that it was more appropriate for him to talk about the "de-identified document" action item rather than ACCC. It was noted that we have discussed this with ACCC and a number of parties who are involved in the implementation. It was noted that, given the small numbers of organisations that are represented, it's very difficult to de-identify that document completely and the commitment made by the ACCC is that the results would not be public, nor shared publicly. It was noted that we are not in a position to provide a de-identified document and if anyone has any specific questions, they can reach out to ACCC now or later.

One member asked if the Chair could clarify why you can't tell us and were there any particular themes or things that we should know in terms of the root cause?

The Chair noted that the document shows the status of some of the 13 organisations that are involved in the assurance process, some of which are involved in the Advisory Committee, and it would be very easy to triangulate and work out who's who. It was noted for example, in the Senate Inquiry into Fintech's there were a lot of questions of Mark Staples about the status of the testing, data holders and data recipients. It was noted that it is better that we all don't know details of individual organisations so we can't inadvertently release things that are appropriately confidential.

Technical Working Group Update

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

The DSB noted that the operating model is a critical consideration for us going forward. It was noted that we have to manage the iteration of the standards and it is a complex process. It was noted that we have gone through one eight-week test cycle where we have created a process, socialised the process and got everyone involved to some degree. In the cycle we identified a range of change requests, evaluated and prioritised them, distilled them into a collection of decision proposals and put them into one document and sought approval. The resultant changes are about to be incorporated in version 1.1.0 of the standards.

It was noted that we held a retrospective where we invited feedback on that process, and we got some useful suggestions, but in broad terms, we seem to have a workable model. It was noted that

the intent is to continue moving through eight-week cycles, but with a pause at this point due to the holidays period and the double-down on final phases of testing. It was noted that we will announce a date for another cycle in due course and we continue to invite people to engage with that process and to give us feedback.

The Chair noted that in the report on page 14 under "Maintenance Outcomes" it mentioned "8 proposals resulting in material change to the standards" and noted that this means an *actual* change rather than a *significant* change. DSB confirmed that this is correct.

DSB also noted that for urgent changes, and particularly things that are coming out of the testing process, we will and have taken them out of the maintenance cycle and dealt with them separately.

The DSB noted that the UX team is moving into conducting some more research with a few items prioritised for the beginning of next year. It was noted that in the process of defining the scope of issues we've identified topics like joint accounts that we're going to address as soon as possible.

The DSB also noted that we are receiving ongoing feedback on the latest version of the CX standards and guidelines and note that there have been some requests for optionality and clarification that relate to the standards. It was noted that these will be put in the consultation drafts which will be published soon for feedback before making any changes. It was noted that some requests largely relate to the Rules, along with some items relating to data cluster and permissions language.

DSB noted that, in regards to the decision on concurrent consent being published on GitHub, the decision provides flexibility for anyone to do what they need to do and basically removes the requirement for single consent. This is a pragmatic choice for the short term and we have committed to further consultation in the New Year to re-evaluate how we approach concurrent consent in the longer term.

One member noted that there was an issue raised today on concurrent consent, suggesting that option three, where the existing refresh token is supplied to the endpoint could introduce security issues. It was noted that this is something that we should look at more carefully before providing the option to participants. DSB noted that they had not seen this issue on GitHub but they would investigate further.

ACCC noted that after the DSB consulted with them on the proposal, the ACCC undertook an impact assessment for each of the four major banks and the nine initial data recipients. The outcome of which is that the ACCC vies that proceeding with the proposal would have minimum impact for launch and provides an appropriate pathway for resolving the issue longer term. The ACCC would like to thank everybody for responding as quickly as they did so they could clarify what has been an issue for a while.

Terms of Reference

The Chair noted that the Terms of Reference have been updated with some minor changes and were taken as read.

Treasury Update

Daniel McAuliffe from Treasury provided an update as follows:

Treasury noted that the main focus is on the consideration of the request for revising the February launch date and noted that they are not able to provide much more of an update. It was noted that they have had an external consultant look at the progress of implementation and provide advice, and currently the government is considering their recommendations. It was noted that the Government realises the importance of making a prompt decision.

It was noted that in terms of the Privacy Impact Assessment which has been completed, the independent consultant has made a range of recommendations, and the government agencies have now settled their response to those recommendations. Treasury are looking at the report, and their response will hopefully be published on the Treasury website tomorrow.

The Chair asked in regards to the Minister's consideration of the February date and the consent in relation to the Rules if whether there is any nexus between those two.

Treasury noted that it is probably accurate to say that the consenting of the Rules is being held up by the schedule decision. It was noted that as soon as we have a decision on timing, the new Rules should hopefully be consented to.

Treasury noted that there is no discussion of any substantive changes to those Rules other than in respect of timing and noted that the version that has been circulated, the latest version, is the version that will probably be accepted and hopefully should give people some reassurance.

One member asked what is the approach and the timeframe for getting a decision on timing and if there was a decision to delay, when can we expect that to be delayed to?

Treasury noted that in terms of the process for getting a decision on timing, the Treasurer has been advised and we are waiting for a decision. It was noted that they are not at liberty to give an indication of what their advice was to the government.

One member asked in regards to the announcement for go live, what is the government point of view about go live?

The Chair noted that we are looking at what go live on day one really means and how big it needs to be, recognising that it's when consumers can access something. It was noted that there could be a scenario in which those who are ready to go from February could be able to go live, but the big announcement and when we're saying the systems at some scale could be at a later date. It was noted that obviously the assurance regime would then be targeted and aligned with that.

Treasury noted that this is very much in the forefront of their minds and the launch from the government's perspective needs to be meaningful with useful apps actually being there using open banking data.

One member asked, in regards to a question that came up this morning with Open Energy, if there is a higher-level roadmap, economy-side CDR policy as opposed to CDR designated sectors?

Treasury noted that there is a document that reflects that there has been some discussion at the agency level about this issue. It was noted that CDR energy is really where there are divergent opinions where people have strong views about how consistent versus how tailored it should be, and this is highlighting the need to actually articulate the design philosophy as we roll things out.

The Chair noted that the real benefit of energy is it is so different, and it's forcing us to confront those issues. It was noted that Lisa Schutz (Verifier) and Lauren Solomon (CPRC) who are members of this Advisory Committee have signed on to the Energy Committee as well, and they are playing a very strong and important role in flushing out cross-sectoral issues.

One member noted that there is a real merit in thinking through the overall framework, and which pieces need to change in order to allow a new industry to function, and then which pieces can remain the same.

The Chair noted that at the meeting this morning we discussed the standard-setting Framework for energy and noted that one of the sections in the Framework addresses the reasons why we would have common standards between the two, and what are the reasons why we would have potentially divergent standards between the two? The Chair noted that adding an Energy Advisory Committee person to this group would be useful from a cross sector and economy wide perspective, as well as provide some comfort to the energy people and that we need to work out who the right person is and determine whether they're prepared to do it.

The Chair noted that he discussed with Commissioner Court from the ACCC about this matter being as applicable to the Rules as to the standards, so we should do this together, and this is a good group to do it with, along with some of the energy sector folks.

One member noted there's still the identity issue that hasn't really, at a system level, been looked at. It was noted that identity really needs to be tackled at a higher level, involving the DTA, and further noted that "everyone keeps telling me identity is solved" despite this not being the case. The Chair noted that identity is out of scope.

One member noted that the Australian Payments Network TrustID Framework is designed to be interoperable. The Digital Transformation Agency (DTO) fed into that, so it's designed to be interoperable across government sector and private sector.

The Chair noted that we need to get together and frame up the issue in a smaller group and then bring it back to the whole group and talk about it. The Chair noted that he will work with ACCC on how we progress things from here.

One member noted that one of the classic things that happens with identification is systems like Green ID where you provide licence numbers into the system. It was noted that for fraud and theft of identities they actually never reissue a new licence number, so that perpetuates the problem. It was noted that being able to reissue a new licence number so that people do have the opportunity not to have old credentials reused for fraud somehow that needs to be introduced into the scope or conversation as well.

The Chair noted that we will write to the committee members to see if you would like to be a part of a smaller group to work on identify. It was also noted that we will invite a couple of the energy committee into that mix.

ACTION: DSB to invite committee members to be part of a smaller group to work on identity.

ACCC Update

Bruce Cooper from the ACCC provided an update on the Rules accreditation as follows:

There are currently nine data recipients who are progressing through a manual accreditation process which is tracking well. It was noted that they still aim to have the accreditation platform live in February, which is a prerequisite for inviting further data recipients to seek accreditation.

The Chair noted that Ernst Young (EY) are running the assurance process on the open banking regime and are running a series of assurance tests on connectivity and conformance, involving pairings of data holders and data recipients. It was noted that as the registry becomes available to test, they will be including connectivity with the registry in that test.

The ACCC noted that there are two elements - there is the technical testing (involving both connectivity and end to end integration testing), and assurance testing, the object of which is to ensure data holders and data recipients have in place all the things needed to meet the launch deadline at a non-technical level.

The ACCC noted they have further considered the requirement to obtain an assurance report prepared under the Australian Standard ASAE 3150 for accreditation. It was noted that assurance reports prepared under either SOC 2 or the ISAE 3000 series that specifically address the requirements of CDR, would be an acceptable alternative.

ACCC noted that if you want to rely on a SOC 2 or ISAE 3000 series report, they'd like to know why you consider the nature of your data operations makes it reasonable for you to adopt such an approach.

One member noted that the real reason why you wouldn't want to do the ASAE on top of the ISAE is really just cost and time. It was noted that it's probably something that won't matter if we said in six months or in a year you have to have the report, as long as you're willing to pay the costs - which is something in the neighbourhood of $75,000 to $100,000. The other consideration is that more companies will probably have SOC 2, as it's fairly common, but it's impossible to obtain in a short timeline. A SOC 2 requires you to have a SOC 1 initially, and then six months later you can check again and then it becomes a SOC 2.

Another member questioned what if your Australian standard gets upped in the meantime, who's monitoring that environment to make sure that any uplifts in the Australian standard don't contradict any SOC 2 or international standards? Is that something that's within the remit of the ACCC?

ACCC noted that when they obtained advice, they were provided with a digital mapping exercise, and assurance reports prepared under SOC 2 and ISAE 3000 series are international equivalent standards. It was noted that they don't know the answer to the question on ongoing maintenance of parity.

ACCC noted that if people have the SOC 2 or the ISAE reports, it's important to know that for accreditation, as well as addressing the specific Schedule 2 requirements in the CDR Rules, the international equivalent standard reports should also address any additional requirements specified in ASAE 3150. The ACCC will update their guidance to reflect this.

It was noted certification under ISO 27001 is not an acceptable alternative to an assurance report prepared in accordance with ASAE 3150.

One member noted that they are ISO 27001, but they haven't done an ASAE 3150. It was noted that the reason is that it is expensive and it's three days roughly per control, and each control has to be tested. It was noted that it is not just a cost implication, however obviously one request would be to look at the tiering, so when the intermediary model comes in, tiering might apply to mitigate a very high entry cost. It was noted that the practical implication for go live say in February (or whatever date it is) is simply the elapsed time to do that testing. It was noted that they haven't been able to get an auditor to give them a straight answer to how long assessment will take.

It was noted that the cost is prohibitive and even if we can find someone to start in mid-January, they probably couldn't delivery until after February.

One member noted that they have a quote from Ernst & Young to test for 23 controls and the amount quoted is between $85,000 to $95,000.

One member noted that they are obsessed with the privacy and security of Australians' data, and they have no problem with assessment being a barrier. It was noted that they are conscious that we want to get going, and we shouldn't trade that off, but the reason that the report's so exhaustive is because it's doing the testing for each control. It was noted that one option is not to drop the list, but to test the most crucial controls. It was noted if you assessed the risks to the security and sanctity of everyone's data and worked out the top X, it's literally a question of time and materials and thus can expand and contract.

One member noted the CDR guidance template is 24 controls, so that's the bare minimum. It was noted that the ISO 27001 controls have 114 in scope and if you are going to spend three days testing each and every control it's obviously a very significant process and takes a good amount of time.

One member questioned from a general internal audit perspective, in what circumstances would you ever have 100% of controls tested and what is the benchmark?

The Chair noted for an internal audit testing it would be slightly different, because you're not auditing compliance, you're examining controls to assess to which they can be relied on as controls. It was noted there are usually IT general controls rather than compliance-related controls at the start of a regime. It was noted in that our discussion with Treasury about the implications of what day one is has a bearing on this and on assurance because if you are in a period before the real day one, then you could buy time here i.e. these 12 have to be audited, and these 12 have to be

reviewed with a view to having all 24 covered in a 12 month period. It was noted that authorisation to operate could be progressive, rather than everybody at once, and therefore your assurance regime could reflect that as well. It was noted that we should be building up, so we've got the exponential usage curve really starting to get steep by the time we get to day one. But we've got to have protections in place, and then if you allow, say, data holder X, and data recipients Y and Z to operate, they get an advantage because they're testing their products with customers before others.

One member noted from a fintech perspective, any launch would not be an all singing, all dancing, invite-the-globe launch, it would be a graduated approach.

ACCC noted a managed rollout would allow participants to ramp up gradually when it was satisfied that their system was stable and all requirements were in place. It was noted that if the launch date was delayed this concept will need to be defined more precisely.

The Chair noted that is instead of waiting until 13 parties are fully assured and compliant, and then calling that day one, we could say start with four. It was noted that success is when consumers are using it, it's not when the registry's up or when the data holders are compliant, it's "consumers' use" that constitutes success.

One member raised a point about Grant Thornton doing a review of stage two, changing dates from February to effectively July. It was noted that their team is feeling like the change process, with the expected but unconfirmed timing change, is a little bit chaotic. It was noted that they would like some more rigour around the change process.

Treasury noted that they are very mindful of that, and in terms of changing the timetable there is quite a bit of rigour in terms of ensuring they're taking into account all the various factors, and the impacts on different participants. It was noted that one shortfall is transparency for external people about what that process is, which is unfortunately unavoidable.

Another member noted that whatever happens to the timetable happens to the timetable, but we may find ourselves six weeks out from the first phase or the second phase, or whatever it might be, still with changes taking place. It was noted that this will cost twice as much, and there'll be a lot more operational risk. It was noted we absolutely need to lock it down for subsequent phases and, if we have more time, make sure that we are very buttoned down about change protocols.

ACCC noted that it was using the test working group to determine the importance, and impact of changes and clarifications that were being raised as participants moved through testing. The ACCC noted that it was to be expected that issues would be discovered and that the ACCC was working to balance the importance of getting the build right and the need to minimise changes.

One member noted that we should have some consensus around what a good testing period looks like and, within that period, how do we manage the changes that emanate from whatever insights come to hand? It was noted that there are two issues that are coupled, the first being agreement on what are we going to commit to as a logical test period for a new big release, and then what's the process for managing the changes that emanate from that.

The Chair noted there's a scope of testing question as well, i.e. if we add one new data recipient, that's a change, does that require a retest of the whole regime, or just some assurance from that

data recipient? It was noted that if we're going to add 150 additional ADIs as data holders, and we're going to turn on reciprocity in the whole regime, that would be a very different scale. It was noted that not one size fits all if you have a soft launch it's a different approach than the one you would follow if you said we're going to wait for everybody to be ready and then fire the starting pistol.

The ACCC noted that we have to recognise that we are in a special period of start-up where testing is manual and intensive and where testing is going on at the same time everyone is doing development work. It was noted that once the scheme is a little bit more mature, we'll see much more automated testing and more clarity around what is mandated and when.

ACCC noted that, in regards to testing, EY as test partners have basically settled the industry end-to-end IT tests with everybody. This includes 211 mandatory test scenarios which cover obviously the Rules and the standards together. It was noted that this is targeted at the moment on a February go live date and, while progress is being made, everyone's tracking behind what we would need to get through all those tests for February. It was noted that the planning for the UAT which will need to follow the end-to-end is underway but is not yet complete.

ACCC noted on test execution the focus is now on completing the connectivity testing, and then moving into doing those 211 test scenarios. It was noted that seven out of the nine data recipients have successfully connected to the register, one data holder has done so and one data holder has chosen to continue to use what was the manual work around to proceed with their testing stream at present. They understand we will need to redo some of those tests once they move from manual to automatic. It was noted that the data holder is proceeding quite nicely with its work stream, and they have done 40 out of the 40 test scenarios and moving on to the next group of 36. It was noted that good progress is being made but there is still a way to go.

One member noted that they are having a hard time connecting to the register and they are getting time out responses and there is no clarity on why. It was noted that have raised tickets in Jira, but they would like more help on what exactly is not working and why it's timing out.

ACCC noted that they will go back and see if there is any chance that team can work a little bit more closely with the member team on this issue.

The Chair encouraged everyone to engage with and talk to the testing team, because sometimes they don't know the end-to-end process and who to hand something off to.

ACCC noted that one of the issues discussed in the Implementation Advisory Committee, was raising the questions and defect issues through the agreed channels, because there have been some instances where things have gotten raised outside those and fallen off the radar.

One member noted we have had some previous discussion where there were some concerns around EY, possibly unfairly, because they just commenced and only been in the role a couple of weeks but asked how's EY's performance has been subsequently.

The ACCC noted that they think EY understands the role, the importance of the manual testing process for launch to succeed and are getting through the significant volume of work reasonably well. The ACCC would welcome further feedback on this.

The Chair noted that they think they are now up to speed and aware of what's going on, but they are still working to 13 parties to be mandated on the same day to go live. It was noted that they are looking at the latest dates and the latest times and trying to shoehorn that. It was noted that if there was a different incremental approach, it might lead them down a different path.

ACCC noted that they are currently heading for February and it is unrealistic to expect all 13 to be live at the same time, but EY continues to work with all 13 to help them all get through the process.

ACCC noted that the test scenarios have been designed mainly around the timing for February and if that time is moved, some re-planning would be required, but this is not expected to be significant. The Chair noted that they are not testing every possible combination, so every data recipient is not connecting with every data holder, for example. It was noted that it would be worth asking them how many of the possible scenarios in terms of pairings they are testing, and what is the percentage.

ACCC noted that at the moment, data recipients are paired with a single bank. Some further multilateral testing is planned once the participants' systems are more mature.

One member noted that as part of the testing scenarios, they are working through the consent withdrawals, and they have some ACCC decision commentaries provided to them which concern them in regards to the Rules. It was noted that in particular they were informed that when they reconsent a consumer they are supposed to delete all of the previous data and re-download new data with the extended consent. It was noted that they think that's probably not the intention, but that was in the ACCC response to them, and asked for clarification. It was noted that the member will forward the response to ACCC and highlight it via email for clarification. The ACCC took this on notice.

ACTION: Member to forward to ACCC the response in regards to reconsent of a consumer.

The same member noted that the Rules say a data recipient must keep or maintain records that explain withdrawals of consents, consents to collect, and various other things, and that they must be kept for six years. It was noted that their belief would be that if a user of our tools said "I want you to forget everything about me", we would want to forget the CDR consents as well, although maybe the data hoarder would keep them and that doesn't appear to be listed in the Rules so we're just seeking more clarity on that. The ACCC will take this on notice.

ACCC recognised how much effort particularly the banks and the initial data recipients are putting into the testing and thanked everyone for their ongoing cooperation and effort, working to a difficult timetable at a busy time of the year.

Meeting Schedule

The Chair advised that the next meeting will be held on Wednesday 12 February 2019 from 2pm to 4pm at Data61's office in Sydney.

The proposed key issue for consideration might change as it is the 'launch review and next steps' but will advise in due course.

Other Business

The Chair noted that we're going to have a kick-off 2020 party, because we should at some point, celebrate what we've achieved to date. It was noted that it feels like it's been a grind, and for a long time, and we've made enormous progress.

The Chair thanked everybody very much for everything they have done. It was noted that we have got to a point that he is confident now that the regime we will launch will certainly change Australia forever, and it'll be a very positive one. He thanked everyone for all the help and compliments of the season to you all.

The Chair thanked Kate Crous and CBA for hosting the December meeting at their offices in Melbourne.

Closing and Next Steps

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

Meeting closed at 3:50