Structure of the Consumer Data Standards

In giving an overview of the consumer data rights standards. It is good to keep in mind the various components that have been designed into the standards. So the standards are not just one thing. They're actually sub components of different technical concerns for different technical purposes and potentially for different audiences.

When the standards are being implemented by an organisation, they tend to be implemented by different parts of that organisation if the organisation's large. So for instance, [one of] the major components are the Consumer Data Right CX standards. So these govern guidelines and required aspects of things that our customer will actually see. Things like security dashboards and the consent flow when they're actually giving a consent. And these are important because we need a consistent experience so that if a customer shares data from one bank to a FinTech and then they share the same from a different bank to a different FinTech because many customers are with many banks, they have a consistent experience cause consistency will increase usage and also consistency leads to security, better trust, better understanding of what is happening. And that's been demonstrated over and over in the technology industry.

Next part of the standards is the information security profile, so the information security profile covers, you know, the low level technical details. You know, what encryption algorithms, how are tokens transferred, all those kinds of things. The kinds of things, and this is what this is why, and it's specifically targeted security implementers and security architects. It is how this stuff is going to be transferred, how the data is that it belongs to a customer and is really important is going to be transferred between two entities in a secure, predictable way and that information security profile has been the topic of a great deal of consultation and industry analysis and external reviews to ensure that it meets those goals.

The third part of the standard is the overall overarching standards for how APIs will be built. These cover things like errors, general payload structures, URI taxonomies, how header are managed, how particular HTTP mechanisms are used. Again, quite low level technical details, but this is common standards that apply regardless of sector.

These common standards that are overarching are important because as new sectors come onto the consumer data right regime, they shouldn't change. They should change in response to changing additions but not because of new sectors. And the advantage of that is that as new sectors come on, the fintechs don't need to just be fintechs. That can be energy techs, they can be wealth techs, they can be any number of startups that are looking across multiple sectors of the Australian economy and building services that we've never seen before because they're not siloed in their industries anymore. And the overarching security, the overarching standards that govern how API work mean that a startup that wants to implement across industries is going to have a much easier time at doing this, going to be much simpler.

Another question that is asked frequently is what are the nonfunctional requirements for the regime, under the consumer data rights standards? Now within the standards there is a section articulating nonfunctional requirements. Those nonfunctional requirements can and will change based on the requirements of the regulator to manage the environment and to support those nonfunctional requirements there are various administration API so that holders can report their actual performance against those nonfunctional requirements, because a nonfunctional requirement is only able to be observed in action if you like. So something like availability, if you're not reporting downtime then you can't indicate whether you're actually meeting an availability nonfunctional requirement for instance. So within the regime, the vast majority of the nonfunctional requirements apply to the holder and this is because the holder is in effect providing an availablee service. So there were availability, transaction thresholds, response times and a range of other nonfunctional requirements that are that a holder has to comply with.

There are however implications in the nonfunctional requirements the holder has to comply with that have impact on a data recipient. For instance, there is a separation between attended and unattended traffic. Attended traffic being the recipient is making an API call because the customer is actively using one of their websites or their app and is expecting a response versus unattended, which is for instance, overnight I might get the last, the latest transactions for a particular customer and the customer's asleep. They're not logged into anything but the service is still going and getting data on their behalf. Now within those two models, holders have different obligations. In an interactive attended scenario, they have to respond faster, more frequently and at a higher threshold than in an unintended constant context. Step maintenance becomes incumbent on a data recipient to make sure they are managing their unattended calls and keeping them, if you like socially aware, not being overly chatty, not calling too much because if they do, the holder will be entitled to decline the request if they exceed certain thresholds.

So any requirement on a holder is in effect also requirement on the ADR, how they behave and act. In addition, there are specific nonfunctional requirements on that applicable only to the ADR, but they are more generic and they're mainly to a given indication of the standard of behavior of an idea and an implementation that is expected. So for instance, an ADR that is overly chatty, calling too often or is likely to be in breach of some of those qualitative nonfunctional requirements. And that will result in the questions being asked and the conversation being had between the regulator and that recipient.

The final component of the standards is the APIs themselves. So these are the actual application programming interfaces. That’s what API stands for. These are the end points that are, that a recipient of data will call to get the actual customer data. So once they've got consent, once it's secure, once they've done all of the setup required, and then they say, well, I want the transaction data now that I'm now authorized to receive, these are the end points that will actually be called to receive that data. And if you like of it, this is the meat. Everything else is around it is to allow for this transfer to occur. But the API is themselves are the meat. They're

the ones that they're the end points that will actually be called to transfer the data. And those four components make up the consumer data rights standards.