ELDO

MeterStack

Submission to ACCC CDR Consultation Paper

SBC

Date 7th February 2020

To ACCC CDR Team

We write this submission as a response to the CDR consultation paper seeking views on facilitating participation of intermediaries in the CDR regime.

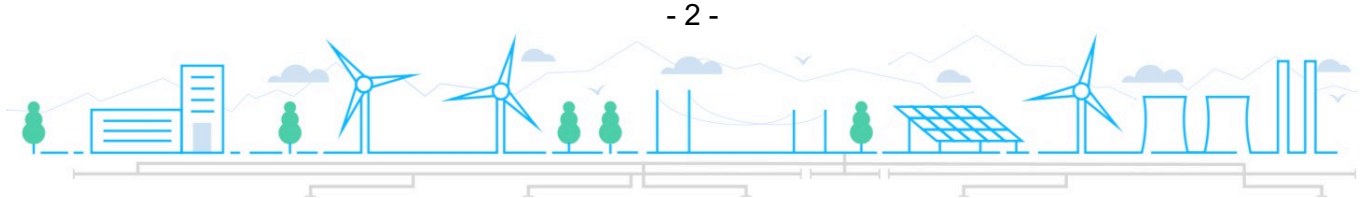
Background

We at ELDO are a South African company operating in the South African energy market since 2013. We have provided a variety of services over that time across the energy value chain and now focus primarily on delivering a vertically integrated digital utility to the market. We firmly believe that the energy networks are becoming more and more connected and thus transactional, and as such our priorities lie in digitising utilities. Our experience in being a consumer-focused company has led us to understanding the consumer at a deep level, and that coupled with a foundationally deep understanding of how data is used in the energy value chain has enabled us to bring our business to the Australian market.

Policy Overview

An ecosystem of companies in the energy value chain enable consumers to benefit with numerous innovative products and services. When a consumer shares his or her private electricity data with a certain company, there are often several firms in a "digital supply chain" that acquire and process the data to eventually deliver services to that consumer, whether the consumer is aware of those entities or not. The ACCC consultation paper has asked for a response for data rules relating to intermediaries but we believe rules need to be established for all parties in the energy value chain. We thus refer to this group as "Nth" parties and define an Nth party as any party that collects or manages certain data on behalf of another entity that serves a customer. These entities represent and enable exciting innovations in the energy sector, but they will be stifled in the absence of thoughtful, targeted policies and consumer centric data exchange mechanisms. Nth parties can be used to deliver innovative, energy-saving services to consumers and in certain countries the implemented rules and policies have been overbroad prohibitions on data sharing which have had the effect of preventing even informed consumers from exercising meaningful control over their energy data.

Optimizing costs with information technology (IT) outsourcing is prevalent, especially for companies that need to focus on their core value proposition. Far-reaching privacy policies therefore have the effect of unnecessarily increasing costs to consumers and stifling



innovation by requiring energy management firms, and other companies operating within the energy sector, to "in-source" IT functions in order to avoid violating non-disclosure rules.

POLICY FRAMEWORKS SHOULD ADDRESS NTH PARTIES

The work to date done by the ACCC has defined rules around data access for Accredited Data recipients (ADR) but rules around Nth parties are still to be determined, the first challenge is thus deciding what regulations apply to which entities. Untangling existing privacy regulations should begin with a common terminology to describe the various roles and responsibilities involved in handling energy data.

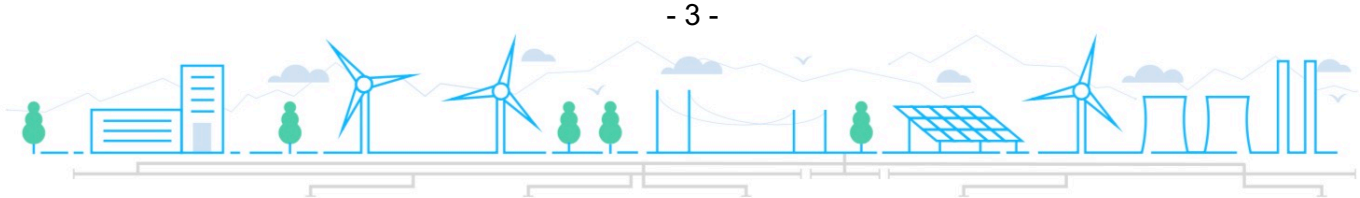
KEY RECOMMENDATIONS

- Define the different types of Nth parties that would operate in the system as (1) full access accredited, (2) accredited and (3) outsourced. Each type of Nth party should have their own rules around data access and possible role in the ecosystem.
- Authorization protocols should be expanded to incorporate Nth parties, machine readable terms and conditions, "cascading authorizations," and the tracking of the consumer consent "chain of command."
- Policy frameworks should understand and anticipate Nth parties by instituting "cascading liability" for data breaches, in which a firm is responsible for a breach caused by its downstream contractor(s), rather than rely on non-disclosure requirements, which are often unattainable in today's digital world.

We argue that what distinguishes "good" data sharing arrangements from "bad" ones is whether the data sharing is consistent with the "scope" of the consumer's original authorization, and whether the manner in which the consumer consented constitutes "informed consent." In other words, sharing personal information with Nth parties is legitimate only if doing so is directly related to delivering a product or service to which consumers have consented. Many consumers seem to be happy to have invisible entities analyse or process their data if there is some underlying benefit.

The spread of new digital services in the energy sector — such as smartphone "apps" for home energy management, and the Internet of Things (IoT) — is exciting, but imposing privacy rules on utilities that are crudely constructed, end up limiting consumer choice without meaningfully increasing privacy.

Solutions lie in both policy and technical realms. Policies should acknowledge the role of digital supply chains in helping individuals and businesses manage utility bills and lower their carbon footprint. Instead of blanket prohibitions on data sharing, disclosures of customer energy information (CEI) with Nth parties should be permitted when necessary to provide a service that a consumer knowingly consented to use. This requires bringing consumers'



wishes into privacy frameworks. Currently, many privacy laws or rules that have been implemented around the world focus exclusively on restricting access to data, not permitting it. On the technical side, well-designed permissioning systems that provide consumers with a clear view of their data authorizations, including the ability to revoke access, are essential to putting consumers in control of their data.

Analysing what has been done around the world with consumer data rights we have seen that it is all too easy for regulators to draft rules with crude oversimplifications: A customer wishes to share their information with a single entity — and that's that. A one-to- one relationship between customer and service provider certainly simplifies roles and responsibilities, but the commercial reality is more complex. Modern privacy frameworks must also address liability among a large potential number of Nth parties. Who should be responsible for making the customer whole if an Nth party, somewhere in a chain of vendors, has a security breach? Privacy frameworks must also address when and how Nth parties must be disclosed to customers in order to secure their informed consent.

In this paper we aim to answer some of these questions as to enable efficient means of sharing data to all parties that will need access to data. This will allow all companies in the energy value chain to deliver on their value proposition and create the energy sector that we strive for.

RESPONSE TO QUESTIONS RAISED BY THE ACCC

Below we have outlined out responses to each of the specific questions raised by the ACCC in their consultation paper.

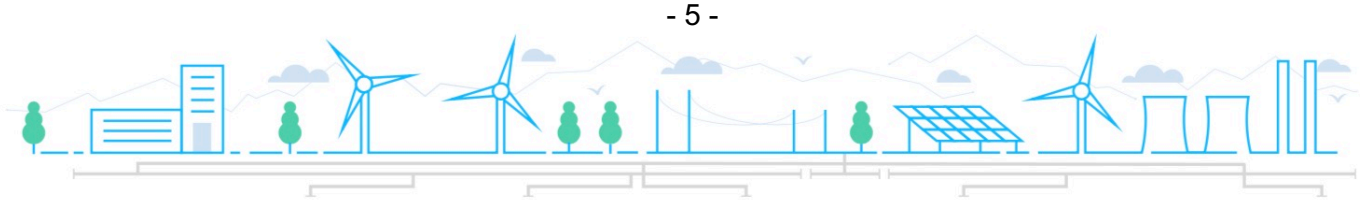
1. If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that intermediaries can bring to the CDR regime and for consumers?

We at ELDO MeterStack aim to create a consumer centric energy data marketplace where consumers take control of their data and are incentivised to share it. It provides a single platform where Accredited Data Recipients (ADR) can plug in and are able to determine which consumers data they see potential value in accessing, as well as providing a mechanism by which they are able to incentivise those consumers to share their data. This incentivization will aid in the uptake and use of CDR by end consumers, giving the average consumer a way to benefit by partaking. Once authorization is granted, we will collect the relevant data from the relevant data holder and provide it to the ADR in a unified format.

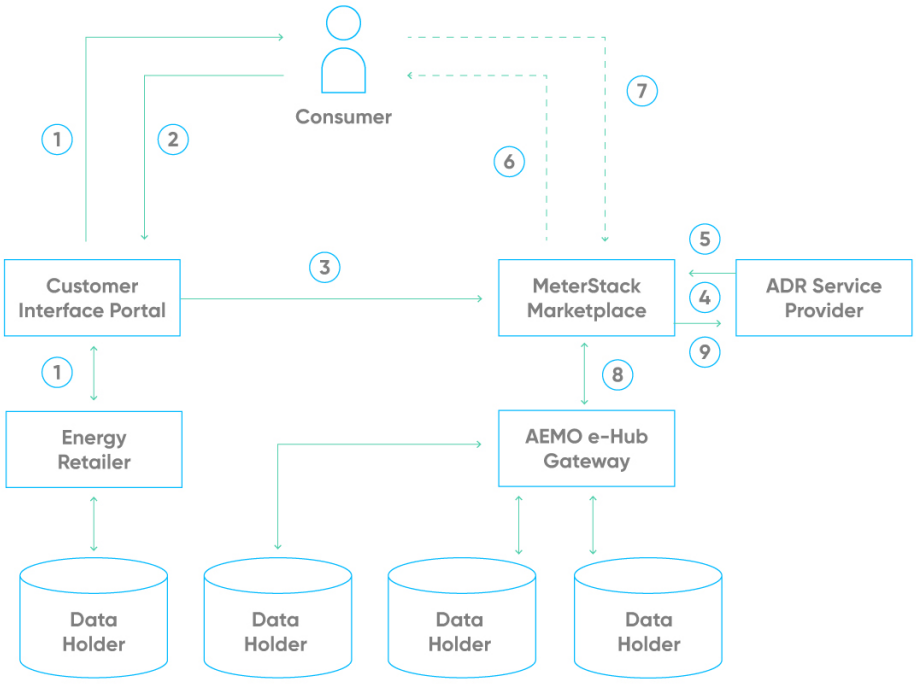
With our proposed business model, we will need to engage with consumers directly in some consumer facing app and incentivise them to participate in the marketplace. They would need to provide consent and opt in to sharing their data. We would provide the marketplace and this would be ADR facing as this would be the platform on which the ADR's engage with the data. We would also facilitate the collection of the underlying data. As such we are proposing that the data rules would allow for a business model like ours to fit into the CDR regime. We believe we can provide a tremendous amount of value by incentivising participation and drive the growth around this regime.

Meterstack could form a pivotal role in the wider CDR ecosystem through exposing certain key components of consumers data to the marketplace and enabling ADR's to request consumers consumption data in order to provide them with an array of value-added services.

Incentivising consumers to engage with ADRs in a marketplace increases the use of the preferred gateway model, supporting a more robust ecosystem of energy services and researchers. Consumers are typically incentivised and motivated by currency and convenience, which are the primary objectives of wrapping AEMO's and the ACCC's CDR efforts in a marketplace. The whole CDR initiative, and AEMO's efforts to support it, will sustain itself or die based on the level of adoption by consumers. In order for all the different stakeholders to realise their value proposition in the energy sector they are going to need access to the data.



HOW METERSTACK WORKS



1. Energy retailer presents consumer with bill through their own app or other Consumer Interface Portal (CIP)
2. Integrate an opt in module into energy retailers CIP, the module would enable the consumer to control their data through user managed access.
3. Consumer opts in and authorises certain elements of their personal information to be relayed to the MeterStack Marketplace
4. Approved ADR's sign up on a license agreement with MeterStack Marketplace
5. An ADR service provider would plug into the MeterStack Marketplace and view elements of various consumers data.
6. If they see potential value in the consumers energy data, they can then push a request (within MeterStack Marketplace) to the consumer for access to their energy data.
7. The consumer either accepts or rejects the request.
8. Upon acceptance of the request MeterStack Marketplace would, through API, retrieve the data from the data holder utilising AEMO's e-hub gateway.
9. The relevant data is then provided to the ADR

2. How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.

We believe that Intermediaries or Nth parties, depending on their level of data access, would form part of either an outsourcing model, accreditation model and we propose a third model namely an ***Accredited Aggregator*** *model. In the case of our business model, we would be interacting with the consumer and connecting the ADR's to that Data so we would need to fall into the* ***Accredited Aggregator*** *definition. We would be enabling consumer participation through incentivisation and connecting ADR's to data and interacting with a variety of datasets as well as interacting with other accredited recipients so there may be a need for additional levels of accreditation.*

We thus divide the intermediaries into 3 types;

1. Accredited Aggregator

*We define an **Accredited Aggregator** as being fully accredited as any other ADR would be, however, they are able to provide a service within the ecosystem whereby they are able to interact with everyone in the ecosystem. This includes but is not limited to; the Consumer, the data holder and the ADR's. full specialised accreditation would be necessary for an accredited aggregator due to the nature of the data they would have access to.*

2. Accredited Intermediary

*We would define an **Accredited Intermediary** as any intermediary that engages with the data directly from the host i.e. the raw data which may include various sensitive pieces of consumer data. As such these entities would need to be registered with the ACCC and be accredited.*

3. Outsourced

*For an intermediary to be deemed to be an **Outsourced**, they would need to have a narrow scope of work that has been outsourced from the ADR. For this intermediary to perform their stated objective they are dealing with data that has undergone some level of abstraction and thus limits the sensitivity of this data.*

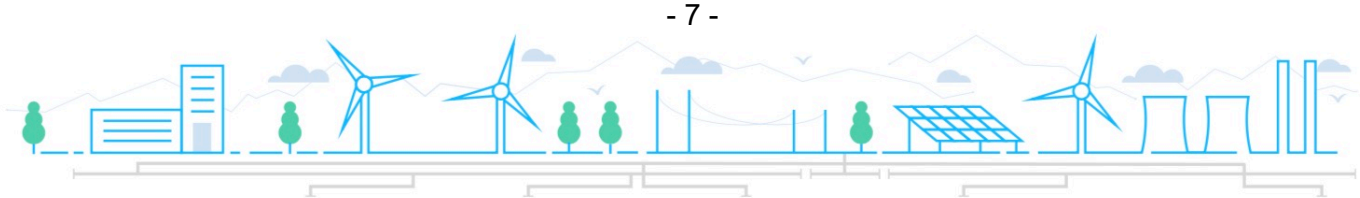
3. What obligations should apply to intermediaries? For example, you may wish to provide comment on:

a. if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards;

Intermediaries operating under the accreditation model, would potentially be collecting and processing sensitive customer data. Thus, the rules and criteria that would apply to accreditation would need to be closely aligned to that of the 'unrestricted' ADR level. They would be providing a service to the ADR's however the same data rules and standards would need to be enforced as the intermediary will handling the same data us the ultimate ADR.

b. if intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and intermediaries;

It would be important to assess the ADR-Intermediary relationship and determine if that relationship constitutes an outsourcing model. If that is deemed to be the case then there is no need for onerous regulation over these intermediaries. They would be providing a service to the ADR without the need to have access to the potentially sensitive elements of the data. Thus, cascading authorisations (discussed later) would be effective in this scenario and disclosure of what categories of companies are used under the outsourcing arrangement would be sufficient.



c. if the obligations should differ depending on the nature of the service being provided by the intermediary.

As has been outlined certain obligations in terms of accreditation would differ depending on what data they are going to need access to. Obligations should also fall on intermediaries in terms of data security but this is touched on in Question 9.

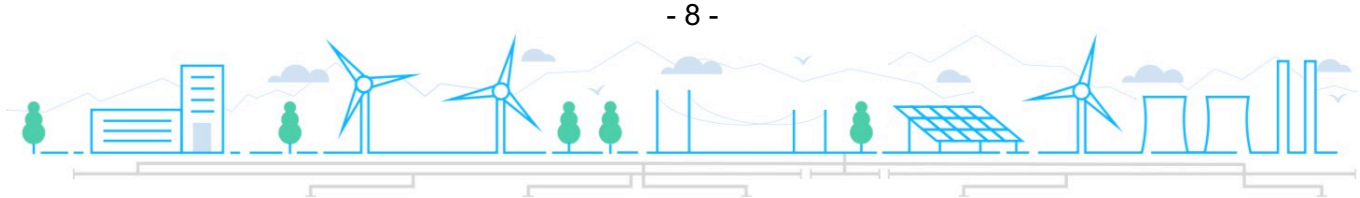
4. How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.

This information should always be accessible to the consumer that had opted in to sharing their data with the 3rd party. At the point of opt in, there would be a need for the 3rd party to disclose the relevant intermediaries used by the ADR and if the customer ever wants to review who has access to what level of their data, they are able to do this through some User Managed Access portal discussed in Question 5.

We believe that Vendor Relationship Management (VRM) should be implemented in this ecosystem. VRM is the vendor-centric equivalent of Customer Relationship Management (CRM). Companies that access private information need to reliably track which users authorized different levels of data sharing, and what data was shared with each vendor. The introduction of the GDPR has had widespread implications on vendor oversight in Europe. Websites (Data Controllers) are required to expose with which entities they share data (Data Processors) and for what purpose. In response, systems for vendor registration and tracking are being offered by major firms in the EU and innovative solutions using blockchain for tracking authorizations and data-sharing events are being explored as a possible solution. While vendor tracking has been prompted by regulations in Europe, VRM is still nascent for Australian companies. As for the level of transparency that firms should be required to provide about their vendors' access to private data, we propose that firms should be required to list the types of entities with whom they share customer data and the purpose of data sharing. This would require firms to disclose categories of Nth parties with whom data is shared, but not necessarily individual firms, which could change frequently. The goal is to increase transparency while avoiding undue administrative overhead.

5. How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.

Customers should be able to broadcast, in standardized schemas, what data they are willing to share, for how long, who can access it, whether those entities may share it with others, and for what purpose. This needs to form part of the opt in process in sharing their data to an intermediary that is then able to provide access to that data to ADR's that fit into the consumers stated aims. Open standards are needed not just to promote automation and interoperability but to help customers choose services that align with their privacy goals by having applications automatically enforce access to services that comply with the customer's stated aims. Thus, any sharing of data between accredited parties still needs to be authorised by the consumer at the opt in phase of the process. If a contract between a company and its vendor ends, all customer data records should be deleted. Additionally, when an end customer revokes access for any reason, customer data shared with Nth parties should be deleted as well.



If for example a customer contracts with an Energy Management Specialist and authorizes the Energy Management Specialist to access CEI. The Energy Management Specialist, in turn, contracts with a data aggregator to acquire the CEI on its behalf. Let's say that the CEI is made available via the B2B e-Hub API. In the current CDR framework, there is no way for the Energy Management Specialist to pass on its data authorization to the data aggregator. As a result, the data aggregator would need to request authorization directly from consumers, and this would be confusing for the consumer as this involves a party with whom the customer has no direct contract. While this process is facilitated by the Energy Management Specialist as part of their service, within the current proposed framework there isn't a technical way for the Energy Management Specialist to revoke or grant data access.

CONSUMER-CENTRIC DATA PRIVACY POLICIES

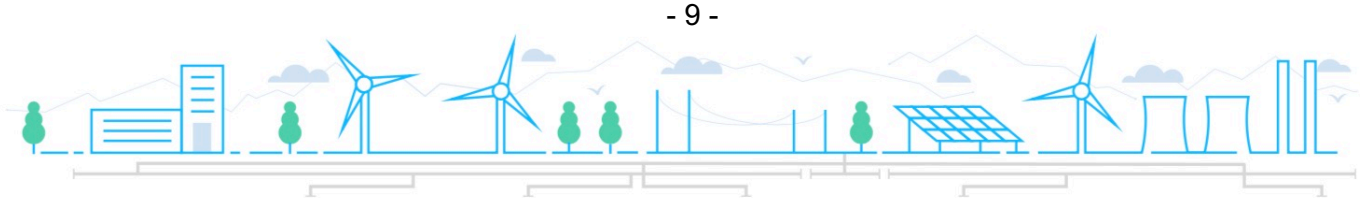
A successful data privacy policy will focus not only on restricting access to personal information but also on articulating the conditions under which it may be transferred. Ensuring that such conditions are reasonable and reflect the actual wishes of the customer requires parsing the somewhat nebulous concept of "informed consent." The US's Department of Energy, Developed DataGuard for the energy management industry and describes best practices for informed customer consent, customer control over data, cybersecurity risk management, and how data should be processed and maintained at rest. This outlines many best practices in the energy industry. As for informed consent, we specifically recommend the following requirements for the sharing of CEI:

1. *Purpose specification. A purpose statement — ideally a single sentence — is essential to informing customers. Purposes must:*
    a. *never be excessively broad — for example, "any lawful purpose" would be an overreach;*
    b. *explicitly mention if data will be used for marketing purposes of any kind; and*
    c. *not be pre-approved or policed by utilities or state regulators (in order to promote innovation and customer choice, state regulators should limit their involvement only to cases in which a purpose statement is excessively broad, deceptive or illegal).*

2. *A simple, clear, and accessible user experience using visual cues. Rather than use multiple pages of text containing difficult-to-understand legal terms, customers should be presented with simple, concise explanations of how their data will be used. Ideally, these should contain iconography to represent the types of information to be shared. To minimize the cognitive burden on customers, the authorization language should be presented on a single "screen" (whether a web page or mobile device applications) and use graphics intelligently. Ideally, various icons would be tested on a representative group to see which visual explanations are best understood.*

3. *Revocation instructions. A clear explanation of how to revoke access. Whatever method the customer used to initiate an authorization should also be available for the customer to revoke access.*

4. *Avenues of redress. Finally, an online customer authorization experience should include a description of a complaint process and different avenues the customer may pursue with state or federal law enforcement*



USER MANAGED ACCESS

We looked into how this is achievable. In doing so we did an analysis of what is being done in different markets and found that certain groups have been working on an innovative approach to standardizing user-directed preferences with User Managed Access (UMA). UMA is built on top of OAuth 2.0, and UMA uses machine-readable licenses to enable users to grant access to data. UMA is user-centric in that it gives customers the ability to leverage an authorization server to manage access to their various resources, regardless of where the resources reside. Access is determined by predefined settings, and customers do not need to be present online at the time that an Nth party requests data access. UMA stands apart from other authorization protocols in that customers can provide instructions to a service provider to grant access to other service providers using the same OAuth Authorization Server. Related to UMA is ongoing work on "consent receipt," a standard for what could be described as a reverse cookie: both the individual and the organization have a record of the consent, and the individual can use the receipt to track and profile the organization and/ or service along with consent and information sharing preferences.

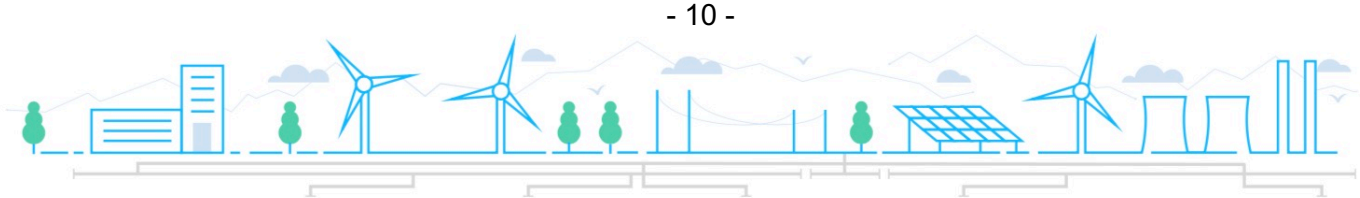
Other potential proposals to enable user managed access may be implementation of Self Sovereign identity which could have tremendous value as we start incorporating access to all other consumer data beyond energy. Australia's ***mygov*** *portal could also be leveraged to incorporate energy data management in the near term, which may be able to solve some of the initial problems but may not be the sustainable option within this ecosystem in the long term.*

6. Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?

There needs to be potential for researchers, network optimisation specialists and analytics companies to be able to access contextual models. We believe that access to large aggregated data sets or contextual models that incorporate the majority of consumers in a given network, would enable these companies to deliver value to the energy sector in a variety of ways.

This would really come down to personal vs anonymised data, if there are sufficient layers of abstraction away from sensitive personal CEI, then giving access to this information would not necessitate onerous regulation. As such there is no need for them to be fully accredited as they would only have access to certain contextual models and not the underlying raw, potentially sensitive, CEI.

Thus foundationally, the difference levels of accreditation would come in what level of access they have to data, if they are only looking at contextual data models or some other abstraction of the raw data, there is no need for this parties to be accredited and in certain cases the regulatory burden of needing all these companies to become accredited could stifle innovation in the sector.



7. If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited third parties and you intend to:

a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers;

This item is not applicable as MeterStack as we would not be a non-accredited third party

b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.

As discussed in Question 6, the only way we see non-accredited parties having access to data is when there are sufficient levels of abstraction away from the sensitive CEI, and these third parties will have access to contextual models as opposed to raw data.

8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

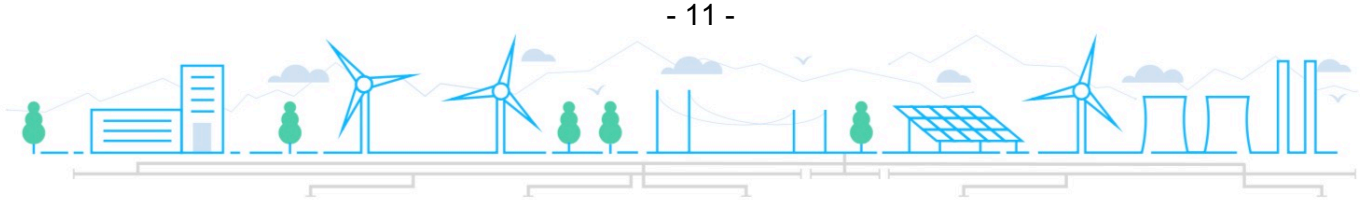
This is covered in Question 6.

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

*All non-accredited third parties should be managed in terms of the **VRM** as outlined above in Question 4. Any access is still to be managed as per the UMA outlined in Question 5, and the data owner should be able to see any outsourcing relationship that exists if they so wish. In terms of liability there needs to be cascading liability, just like there is cascading authorisations that apply to non-accredited 3rd parties. Cascading liability would mean that the ADR who has been given access to CDR data would take on full responsibility for any use of that data through an outsourced contract with a non-accredited 3rd party. ADR's should review the cybersecurity practices of their vendors in order to take full responsibility for any "downstream" privacy risks. As the liability would fall on the ADR that would need to, at all times, distinguish legitimate, customer-directed data sharing from illegitimate data sharing.*

10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?

As touched on in Question 4 the ADR should disclose the types of entities it is using for any of its outsourced services. In terms of authorisation, this would fall under the cascading authorisations and be managed under UMA



CONCLUSION

As the ACCC aims to establish the data rules around CDR in energy, there needs to be strong public AND private participation in formulating rules that are not overly restrictive or impractical and have the effect of limiting customers' ability to share their own data with any service provider of their choice and thus stifle innovation in the energy sector. There are several promising avenues that can further empower energy customers. Existing data sharing standards like Green Button Connect out of the U.S could be expanded to allow for customer authorization to "cascade" to other parties. UMA appears very promising in this regard. Terms of use should also be digitized so customers can control access differentially and have visibility and control over who has access to their data.

The scenarios illustrating the sharing of customer energy information (CEI) in this consultation paper highlight how Nth parties will be treated and enable them to help deliver innovative energy solutions to customers. Specialized Nth party services — whether visible or invisible to customers — help companies focus on their core business, thereby shortening on-ramp times to new markets, providing geographic scalability and offering advanced Analysis. As such getting these rules right will be imperative to enable all the innovative ideas within the energy sector.

Would really like to participate further in this process and work alongside you as the rules and policies are developed. As such if you would like to spend some unpacking anything covered in this submission please get in touch so that we can engage further.