



Tide Foundation Submission

Consumer Data Right in Energy Consultation paper
“Data access models for energy data”

Tide Foundation Ltd
March 22nd, 2019

TIDE.ORG



Table of contents

1	Executive Summary	2
2	Response: Consumer Data Right in Energy	3
3	About Tide Foundation	5



1 Executive Summary

The Tide Foundation welcomes the opportunity to make its submission regarding the ‘*Consumer Data Right in Energy - Consultation paper: data access models for energy use*’ released in February 2019.

Tide wholeheartedly supports Australians establishing and maintaining control over the collection and use of their personal data and is dedicated to providing technology solutions to help achieve this via the Tide Protocol.

The Tide Protocol is an open source, blockchain based technological solution which enables consumers to reclaim control of their personal data while removing the liability organisations carry when holding personal data.

Using cutting edge blockchain and encryption technology, the Tide protocol encrypts the personal data held within an organisation’s database and provides the consumer with the only key to decrypt their data. The only way the data can be shared is if the consumer provides permissions to access this key – which means their express consent is required for it to be used.

We have previously met with and made submissions to the ACCC regarding how this technology could be used to help implement robust protections for consumers as per the CDR and streamline accreditation and compliance.

As per previous submissions, we believe Distributed Ledger Technology, such as the application of blockchain and encryption, will offer the energy sector the best solution for the collection, sharing and protection of personal data.

This protection is best offered under Model 3 – an economy-wide CDR model which provides an impartial solution that is accessible freely by the entire industry. This gives each player in the industry an equal say in its development and will result in a true community-driven governance for the progression of its technology.

We provide this feedback as an organisation led and supported by global leaders in data privacy protection with advanced technologies and look forward to working with the ACCC in accelerating a more effective application of the CDR in banking and energy, as well as any future industries which it will apply to.



2 Response: Consumer Data Right in Energy

Question 1: Are there any other assessment criteria or relevant considerations which the ACCC should use to determine a preferred model for consumers to access their energy data under the CDR?

Tide believes the following criteria to be critically important when determining a preferred model:

- **Security** – there is a growing demand from consumers for greater privacy protection and the intent of the CDR is to provide for this, therefore security of data is paramount for any model. There also must be a system in place for detecting and managing breaches with an appropriate governance structure in place to monitor and enforce this.
- **Scalability and affordability** – the consumer energy market is massive with millions of consumers and a number of different providers therefore any solution must be scalable to accommodate this market.
- **Reliability** – the model must be resilient and fault tolerant to ensure the Service Level Agreement (SLA) is reliable.
- **Impartiality** – the model must allow all players in the industry fair access which requires a solution that can be driven by everyone in that community.
- **Testability** – the model must have the ability for participants to verify their implementation.
- **User experience** – the model must be user-friendly, with clear and transparent processes for the collection and sharing of data, and control placed in the hands of consumers who are the rightful owners of their personal data.

Question 2: Having regard to the assessment criteria, what are the advantages and disadvantages of each of the models?

1. Model 1 AEMO Centralised Model

Likely to be the most problematic when it comes to reliability and security due to the heavy reliance on AEMO being the centralized point of data accumulation. It's likely this model would also be the most expensive to implement due to high costs incurred in building a centralised system, not to mention the high costs incurred by each of the Data Providers building and running recurring processes to replicate their data over to a centralised system.

If centralised systems are to be adopted more broadly (aka in other industries regulated by the CDR) this has the potential to create major inconsistencies for the consumer, adding complexity and slowing adoption and participation.

2. Model 2 AEMO Gateway Model

Similar to Model 1, the high reliance on AEMO as the gateway could create issues with reliability and security, as well as inconsistency and complexity for consumers to engage with the CDR wide ecosystem.

However there may also be benefits in having an aggregate, integrated interface for this data as opposed to the multiple, diverse interfaces that currently exist.

In saying that, we believe the gateway model would not benefit the consumer over the long-term as it introduces another intermediary in the value chain and therefore raises some questions around security, incentives and consumer data control.

3. Model 3 Economy-wide CDR Model

Places control of the data in the hands of consumers themselves and therefore likely to offer greater security and protection. This approach is as well in line with the approach in other industries adopting the CDR such as banking and soon telecommunications.



Consistency across those industries will provide better benefits to the consumer by emulating the development of an ecosystem of service providers across the CDR wide economy.

Relying on a specific closed standard, single vendor or closed-source solution will benefit some players (usually the biggest) while leaving smaller players at great disadvantage having to suffer huge costs (relative to their size) and lose on the greater benefits.

An impartial solution that is accessible freely by the entire industry and also gives each player in the industry an equal say in its development will result in a true community driven governance for the progression of its technology.

This model is also in line with the concept of 'trustlessness' which allows all parties of an ecosystem (such as the CDR) to engage with each other in a way where actual trust is not required as it is imposed via encryption and other means. This means even if there is data leakage from the system, it is meaningless to a third party as it is encrypted to the point where it is anonymised.

Question 5: What emerging technologies do stakeholders believe will have an impact on the energy sector with respect to the CDR?

The emergence of Decentralized-Ledger-Technology (e.g. blockchain) introduces the new concept of "trustlessness" – a concept that allows all parties of an ecosystem (such as the CDR) to engage with each other in a manner that removes the need for trust between those parties. But rather, behaviour and trust are mathematically imposed.

A blockchain based, open sourced, technological solution will shift accountability and control over personal data in line with the CDR framework while providing additional incentivisation for sharing it.

Question 7: What is the competitive impact, if any, of accessing data through AEMO rather than through a retailer?

We believe that any competitive impact potentially brought in by accessing data through AEMO rather than through a retailer will be jeopardised by the increase in security risk due to the introduction of this single point of failure.



3 About Tide Foundation

Overview

Tide Foundation is an Australian not-for-profit whose primary responsibility is the stewardship of the Tide Protocol; a technological infrastructure that is designed to underpin a fair and sustainable personal data economy.

The Tide economy is designed to bolster the right of individuals to maintain control over their personal data, while businesses and marketers can utilize it in a mutually beneficial environment.

Tenets

Tide Foundation will be governed by the following underlying tenets.

- **Sovereignty:** the belief that individuals are the rightful owners of their personal data, and should have ultimate discretion over its use.
- **Consumer value:** if an individual provides their personal data and gives permission to be identified, then any monetization opportunities that arise through those insights or value-adds should be shared proportionately with that individual.
- **Business value:** conversely, the data insights generated by businesses through their interactions with their customers is value that is generated by those businesses, who are therefore entitled to benefit from them.
- **Ethical commerce:** commerce that occurs in an economy that is driven by permissioned and compliant access to personal data. Organizations operating in this environment have the ability to unlock and leverage the power of their unique data insights.
- **Trust:** provided through a means of absolute trustlessness:
 - o *Transparency:* open source software that is publicly available and easily accessible.
 - o *Integrity:* ensuring that when we can't use mathematics to guarantee integrity, we act as though we are programmed to do so.
 - o *Decentralization:* no data is held by, or accessible by, any other parties in the chain. Only the source and target parties have visibility.
 - o *Immutability:* once a transaction is initiated, everything about it is stamped and recorded in perpetuity.
 - o *Accountability:* actions of entities and individuals who data share are open to scrutiny and feedback.
- **Independence:** broad stakeholder community management, free from commercial or political interests, in order to provide infrastructure that benefits everyone in the value chain.
- **Stability and scalability:** the design of the growth engine and the open sourced nature of the protocol has future-proofed the infrastructure. No single failure, entity or process can hinder effectiveness.
- **Mainstream:** accessibility and usability for all stakeholders, agnostic to geography, culture, language and means.

Mandate

Tide Foundation, in operating the Tide Protocol, will be charged with the following mandates.

- Aim to ensure personal data is fully secured and that value is rightfully attributed.
- Cooperate with industry, government and stakeholders to form strategic partnerships that grow the economy in accordance with the established principles.
- Educate and promote the personal data economy to the wider community. Encourage new ideas and development on top of the open source protocol.
- Provide guidance to legislators who have an objective of protecting Consumer privacy, alongside commercial considerations.
- Foster innovation and engage with the development community to continually build upon the foundation technology. This will improve ease of adoption and utility for all stakeholders and ensure future viability.
- Govern the personal data economy infrastructure (i.e. the Tide Protocol).