Smart Meter Data Access Framework Options

Australian Energy Market Commission

13 August 2021

CONFIDENTIALITY

Our clients' industries are extremely competitive, and the maintenance of confidentiality with respect to our clients' plans and data is critical. NERA Economic Consulting rigorously applies internal confidentiality practices to protect the confidentiality of all client information.

Similarly, our industry is very competitive. We view our approaches and insights as proprietary and therefore look to our clients to protect our interests in our proposals, presentations, methodologies, and analytical techniques. Under no circumstances should this material be shared with any third party without the prior written consent of NERA Economic Consulting.

Project Team

George Anstey
Will Taylor
Soren Christian
Barbara Kaleff
Ravi Desor

NERA Economic Consulting
One International Towers
100 Barangaroo Avenue
Sydney NSW, Australia 2000
+61 2 8864 6535
www.nera.com

Contents

Executive Summary

On 3 December 2020, the Australian Energy Market Commission (AEMC) launched its three-year review into the smart meter regulatory framework, with the aim of determining whether further changes are needed to the regulatory framework to enhance its efficacy and efficiency.[1] The AEMC will release a directions paper in late August or early September, with a draft report due before the end of the year.

One challenge that the AEMC has identified is in respect to smart meter data access. The AEMC and industry stakeholders alike have observed that smart meters can provide significant value to the system by providing near real-time power quality (PQ) data to DNSPs and other interested third parties. As opposed to simple consumption data, PQ data generally comprises voltage, current and power factor information over a short interval.

In the case of DNSPs, this could allow for more efficient management and maintenance of their grids. However, access to this data from retailer-appointed Metering Coordinators (MCs) to Distribution Network Service Providers (DNSPs) has to be negotiated on commercial terms, and to date very little access has been provided.

To underpin part of its draft findings in August, the AEMC has commissioned NERA to examine the challenges surrounding data access in greater detail, and to develop a series of options for new frameworks to allow for greater access.

Theoretical framework of the problem

In spite of data access and use being one of the primary drivers of value to the system of smart meter roll-out, there has been very little exchange of data between MCs and DNSPs (or any other parties). At its core, this problem is a result of a challenge with transaction costs and a challenge with coordination. Any new regulatory framework must address either or both of these challenges.

Regarding transaction costs, each time a DNSP or other third party wishes to obtain PQ data from an MC, they must incur some fixed costs in doing so, in relation to negotiating access and processing the data. The MC must do the same. If MCs are fragmented, or if the scope of the data request is narrow, then the value that the data provides to the DNSP may be less than the cost required to obtain it. If the process can be consolidated and rationalised across MCs, or at least across a large swathe of data held by an MC, the value that it provides is more likely to exceed the cost of procuring it.

Additionally, because the MC landscape is fragmented among several MCs, MCs may be averse to moving first. The value that one MC's data can provide to a DNSP, and hence the price it can ask for it, increases once the DNSP has obtained access from all other MCs relevant to the request. With all MCs facing the same incentive, none of them act first and therefore data access is not provided. The economics literature refers to this as a "hold-up" problem.

To resolve these fundamental challenges, we have conducted a review of smart meter data access arrangements in other jurisdictions and developed a set of options for a new regulatory

[1] Australian Energy Market Commission (3 December 2020), Review of the Regulatory Framework for Metering Services – Consultation Paper.

framework which, to varying degrees, would address the transaction cost and coordination problems which currently impede the provision of data access.

Case studies

To inform the options for a new regulatory framework in the National Electricity Market (NEM), we have reviewed a set of case studies for how access is managed in other jurisdictions.

Victoria

In Victoria, DNSPs are responsible for installing and maintaining smart meters, and also have direct access to all of the technical data that they collect. While Victoria is of course part of the NEM, it is outside of the scope of the AEMC's current review given the different arrangements that apply for smart meters. However it serves as a useful benchmark for what an effective access arrangement could achieve. In discussions with DNSPs in Victoria (namely United Energy, CitiPower and Powercor, which are under common ownership), they told us that they collect PQ data from their meters every 15 minutes, with each transmission containing the three most recent five-minute periods. We understand around 99 per cent of residential and small commercial customers are equipped with a smart meter.

Victorian DNSPs collect data frequently enough (every 15 minutes) that they are able to manage their networks on a near real-time basis. This frequency may be necessary for some use cases, e.g. responding to outages without waiting for it to be reported.

The Victoria case study demonstrates the value of reaching a high degree of rollout, as a wide range of use cases become available which can deliver significant value to customers. Many of these use cases are not yet available in the rest of the NEM, such as phase allocation and other real-time operational uses. These potential uses may be possible in several years' time if the rest of the NEM reaches near 100 per cent roll-out of smart meters, but the present uses of smart meter data outside of Victoria is limited to those that rely more on the dispersion of smart meters across a wide area rather than a complete picture of every megawatt that is being distributed across the network.

Great Britain

In Great Britain, retailers are responsible for installing and maintaining smart meters, but each smart meter includes a specialised piece of communications equipment owned by the Smart Data Communications Company (DCC), a price-controlled monopoly entity. Retailers are required to supply data on a real-time basis to the DCC, which stores data from all smart meters in Great Britain. Provided they file a Data Privacy Plan with the energy regulator Ofgem (and all have), DNSPs can access data stored by the DCC. The Data Privacy Plans must set out the intended purpose of the data. All DNSPs collect half-hourly consumption data on a monthly interval, with the intention of using it to help plan network reinforcement on a highly localised basis. To our knowledge, no DNSP has accessed real-time or PQ data from the DCC.

The British model does not require any commercial negotiation between DNSPs and any other party, but instead requires DNSPs to apply for approval to Ofgem, who assess the applications primarily on the basis of data privacy and security.

While the ownership of smart meters is decentralised, the process of data management is centralised. The DCC bears the costs of managing a single communications network and putting data into a consistent format, but these costs are not replicated across many different retailers. Additionally, DNSPs only interact with Ofgem (in applying for access) and the DCC (in receiving the data). Therefore, unlike the present situation in the NEM, DNSPs do not need to hold many, simultaneous negotiations across a disparate set of MCs.

New Zealand

In New Zealand, retailers are required to provide consumption data to DNSPs in a pre-set format if requested, with DNSPs obligated to pay the reasonable costs that retailers incur in doing so. Retailers and DNSPs can agree to provide PQ data beyond this, but there is no defined framework for doing so.

The obligation to provide data is imposed through an appendix to the Default Distributor Agreement (DDA), which is the template use of system agreement which DNSPs and retailers must base their agreements on, but may negotiate alternative terms. Under the DDA, retailers must comply with any request for data from DNSPs, so long as it is for a permitted purpose. Ultimately, however, DNSPs are limited in their use of data to only the purpose expressly agreed to in the request. Additionally, required data transfers are limited in scope, relating only to the data that must be provided to bill retailers for their use of distribution networks.

We understand that DNSPs do not currently have widespread access to this consumption data due to a clause in the DDA which prohibits combining the consumption data with another data source without the consent of the retailer. Given the large number of retailers operating in a given network area, this imposes transaction and coordination costs in relation to obtaining a complete dataset if the DNSP wants to combine it with other datasets (such as GIS data).

For additional types of data which could be used for the use cases seen in Victoria, and to a lesser extent Great Britain, the Electricity Authority sets out only the format of the data template (for some transactions) and transfer system, but does not regulate any of the terms of access. Indeed, for PQ data there are no regulatory access obligations, templates or pricing principles. Access for this data must therefore be commercially negotiated. Of interest in the present context is that to obtain consumption data, DNSPs deal with the retailer, but for PQ data they negotiate directly with metering equipment provider (MEP). There are far fewer MEPs than retailers, which may reduce the transaction costs and co-ordination issues with obtaining this data.

Australia gas transportation access

In Australia, shippers of natural gas who require third-party access to gas transportation infrastructure are entitled to access under certain circumstances under a negotiate-arbitrate framework. Depending on the type of asset in question, access may be subject to greater or lesser regulatory control. For example, under a proposed change to the current access arrangements, some pipelines will be subject to “stronger regulation”, where any disputes will be resolved by the Australian Energy Regulator (AER) based on pre-defined reference prices. Other pipelines will be subject to “lighter regulation”, where disputes are resolved by an arbitrator based on pricing *principles* (e.g. cost based) but not based on any pre-defined reference price.

The lighter negotiate-arbitrate framework seen in the context of gas network access represents a relatively light-touch and non-prescriptive form of regulation, which gives both parties considerable leeway in determining the terms of access. While the arbitrator must follow pre-defined principles in the event of a dispute, they also have considerable leeway in determining how to apply those principles with respect to recovery of fixed investment costs and allocating joint costs.

Options against assessment criteria

We develop and discuss the following options for a new regulatory framework for smart meter data access in the NEM.

- Implement a **DCC-type organisation** and mandate the types of data that must be provided through it.
- Set **minimum standards for bilateral engagement** between retailers and DNSPs but allow for additional commercial engagements beyond the minimum standard. This is similar the system in New Zealand and also as proposed by South Australia Power Networks.
- Establish an **exchange architecture** with defined roles and partially written contracts but allow parties to participate freely within it.
- A **negotiate-arbitrate framework**, where arbitrators (potentially including the AER) are subject to guiding principles when making a determination.

We compare these options against the following criteria, informed both by the theoretical challenges and the case studies:

- **Provision of data access:** Will the framework overcome key obstacles and ensure that DNSPs and third parties are able to gain access? All of the options have been selected because they are likely to achieve the fundamental goal of providing access.
- **Cost and ease of implementation**: Can the new framework be implemented without undue burdens to the industry, both in terms of financial cost and the time and complexity of compliance?
- **Ongoing costs of framework**: What are the costs of providing data access on an ongoing basis? Do industry participants have to incur unnecessary costs that do not deliver value? Are there high ongoing costs required to enforce compliance?
- **Ease of price formation**: Is it clear how prices for data are set, and how the additional value created is split between DNSPs and MCs?
- **Flexibility to new use cases**: If a new type of data is deemed to be useful, or to have value in a new use case, can the regulatory framework easily adapt to incorporate the new use case?

Additionally, we comment on whether each option could be combined with any other option, or whether it could be partially implemented. We summarise our findings in Table 1 below.

Table 1: Appraisal of Options Against Criteria

Criteria	DCC-Style Organisation	Minimum Contents Requirement	Exchange Architecture	Negotiate-Arbitrate
Provision of data access	Highly likely to achieve core objective.	Highly likely to achieve core objective if minimum obligation includes desired data.	Should achieve core objective, but it is not mandated so perverse outcomes are possible.	Likely if "strong regulation" principles are instilled for basic data access, but otherwise unclear.
Cost/ease of implementation	Expensive to implement as new organisation and remuneration structure required.	Relatively low, as can rely on existing entities.	Some costs to implement architecture (e.g. IT costs, pro forma contracts).	Relatively easy. Framework exists in other industries.
Ongoing costs	Expensive if irrelevant data is collected.	Expensive if irrelevant data is collected and not standardised across retailers.	Relatively low as data is only collected when needed.	Low. Though arbitration is expensive.
Ease of price formation	Data provided to DCC free of charge, DCC recovers costs separately.	Unclear how minimum required data must be remunerated.	Price formation for data access relatively easy, but unclear who bears the cost of the architecture.	Unclear, still relies on negotiation as in status quo.
Flexibility to new use cases	Limited. New policies may need to be written.	Flexible, as it allows negotiation beyond the minimum requirement.	High.	High.
Potential to combine with other options	Limited. Already prescriptive roles and responsibilities.	High. Could introduce an exchange architecture to facilitate access.	High. Could underpin a minimum contents requirement.	Could underpin an exchange architecture.
Possibility of partial implementation	Yes, role of DCC could be limited.	Yes, scope of minimum requirement is flexible.	No. Architecture either exists or it does not.	No.

1. Introduction

On 1 December 2017, the Australian Energy Market Commission (AEMC) implemented a rule that introduced competition into the provision of metering services in all states of the National Electricity Market (NEM) excluding Victoria (ACT, New South Wales, Queensland, South Australia, and Tasmania). Historically, traditional electricity meters (e.g. accumulation meters) have been owned and operated by Distribution Network Service Providers (DNSPs). Under the new regulatory framework, if a meter requires replacement (e.g. if a "smart meter" is being installed), then the new metering services will be provided by a metering coordinator (MC). The MC is appointed by the retailer and this is a contestable activity, though the retailer can also serve as the MC.

When developing the rule, the AEMC recommended that it be reviewed after three years of implementation. Additionally, the AEMC observed several challenges in implementation of the new rule, such as a relatively limited uptake of smart meters.

For these reasons, on 3 December 2020, the AEMC launched its three-year review, with the aim of determining whether further changes are needed to the regulatory framework to enhance its efficacy and efficiency.[2] The AEMC will release a directions paper in late August or early September, with a draft report due before the end of the year.

One such challenge that the AEMC has identified is in respect to smart meter data access. The AEMC and industry stakeholders alike have observed that smart meters can provide significant value to the system by providing near real-time technical data to DNSPs and other interested third parties. In the case of DNSPs, this could allow for more efficient management and maintenance of their grids. However, access to this data from MCs (or the Metering Data Provider (MDP) they appoint) to DNSPs has to be negotiated on commercial terms, and to date very little access has been provided.[3]

To underpin part of its draft findings in August, the AEMC has commissioned NERA to examine the challenges surrounding data access in greater detail, and to develop a series of options for new frameworks to allow for greater access. In this report, we develop these options.

This report proceeds as follows:

- In Chapter 2, we briefly set out the background to our review, as well as the roles and responsibilities of each party within the current regulatory framework;
- In Chapter 3, we identify the theoretical challenges that limit the provision of data to DNSPs.
- In Chapter 4, we review four case studies relevant to access rights, namely smart meter data arrangements in Victoria, Great Britain and New Zealand, as well as gas pipeline access rights in Australia; and

[2] Australian Energy Market Commission (3 December 2020), Review of the Regulatory Framework for Metering Services – Consultation Paper.

[3] Unless otherwise specified, we refer to MCs to generically include the MDP they appoint.

- In Chapter 5, we develop a series of data access options and compare against an initial set of assessment criteria.

2. Background

In this chapter, we provide a brief history of the introduction of competition in the market for provision of metering services, identify the roles and responsibilities of each party and set out the current challenges in the topic of data access arrangements.

2.1. History of Contestability in Metering Services

Prior to the introduction of contestability in metering services in December 2017, DNSPs were responsible for the provision of metering services (installing, providing and maintaining meters, and collecting, processing and delivering data from meters).[4] The costs of doing so were included in DNSPs' price controlled revenue, as periodically determined by the Australian Energy Regulator (AER).

In 2015, the AEMC reviewed the then-current state of the metering industry, and found that, due to insufficient incentives to invest and innovate, the roll-out of smart metering technology was limited in the NEM excluding Victoria. In Victoria, by contrast, DNSPs were mandated in 2006 to roll out smart meters to almost all customers, and as of 2015, nearly all electricity users were fitted with a smart meter.

In order to drive incentives to invest in smart meter roll-out and innovate in product offerings, and at the request of the Council of Australian Governments (COAG), the AEMC developed a new rule which would introduce competition in providing metering services. The final rule was published on 26 November 2015, and took effect on 1 December 2017.

In contrast to the previous regulatory framework, where a single "Responsible Person" (i.e. the DNSP) was required to provide metering services, the new framework requires a retailer to appoint a Metering Coordinator (MC). Subject to fulfilling registration requirements, there are no restrictions on who can act as an MC, and we understand that this role could be filled by retailers or a specialist metering company. The new rule did not apply to Victoria.

As an interim measure, the relevant DNSP remains the Responsible Person and, hence, the MC for existing manually read meters (i.e. accumulation and interval meters). When these are replaced, the DNSP ceases to be the MC, and the retailer must appoint a new MC through a competitive process. Though some exceptions apply (e.g. where the site does not have access to communications infrastructure), new and replacement meters must generally be smart meters.

In proposing the new rules, the AEMC argued that they would drive the further rollout of smart meters, which would have a range of potential benefits:

- Customers would have a better understanding of their consumption patterns, with the option of switching to a time-of-use tariff that better reflects their needs;
- Customers could switch retailers more easily and quickly, and would be billed on actual rather than estimated consumption;

[4] Depending on the arrangement between the DNSP and the retailer, this role could also be carried out by the retailer, but this was still not contestable between them.

- Network prices could be more targeted to match the costs that individual users impose on the system; and
- DNSPs could respond more quickly to faults in their system or occurrences of poor power quality, using data from smart meters instead of customer reports to identify more precisely how their system is operating.

2.2. Current Data Access Arrangements

Whilst MCs hold overall responsibility for the both the physical metering asset as well as the data that it holds, they do so through an appointed Metering Provider (MP), who is responsible for installing and maintaining the meter, and through an appointed MDP, who is responsible for collecting and processing metering data. The MP and MDP can be the same party as the MC, and in many cases they are.

The data collected by smart meters can be classified in two categories:

- **Consumption data:** Meters collect consumption data which is required for billing. This must be provided directly to the retailer who issues the bill, to the Australian Energy Market Operator (AEMO) who settles the market, and to the DNSP for charging purposes.
- **Power quality (PQ) data:** Smart meters are capable of collecting a range of other technical data such as voltage, current and power factor. This data is not strictly necessary to any one party, but can provide value to DNSPs to help manage their networks, and could provide additional use cases to other third parties. Access to this additional data is not regulated and must be commercially negotiated between DNSPs (or other relevant purchasers) and MCs/MDPs.

Unless otherwise specified, all mentions to data in the remainder of this report refer specifically to the additional PQ data beyond consumption data. For the purposes of this report, we focus primarily on access provided to DNSPs, as the main party who would benefit from access. We define “full access” to mean access to technical data with a 24-hour lag, though faster intervals may be possible. For example, in Victoria, DNSPs read technical data with a 15-minute lag.[5]

Data access to third parties such as small generator aggregators or virtual power plant operators could be included in the framework, in order to manage their operations and those of the parties contracted to them. For the remainder of this report, we discuss access arrangements as they apply to DNSPs, because this is the largest stakeholder group that could receive PQ data access, but many of the same principles hold for access to third parties.

5 As advised by United Energy.

3. Theoretical Framework of the Problem

In spite of data access and use being one of the primary drivers of value to the system of smart meter roll-out, there has been very little exchange of data between MCs and DNSPs (or any other parties).

At its core, this problem is a result of a challenge with transaction costs and a challenge with coordination. Any new regulatory framework must address either or both of these challenges.

3.1. The transaction costs of obtaining data access from many providers may not be worthwhile for a DNSP

First, the transaction costs and complexity of exchanging data make it costly for a DNSP to acquire data from multiple different providers within their network region. Because DNSPs must arrange access from multiple MCs in a single region, they must incur the cost of negotiating a new access arrangement several times over, once for each MC. The MC will also incur costs on its side which the DNSP will have to pay for in any commercial agreement.

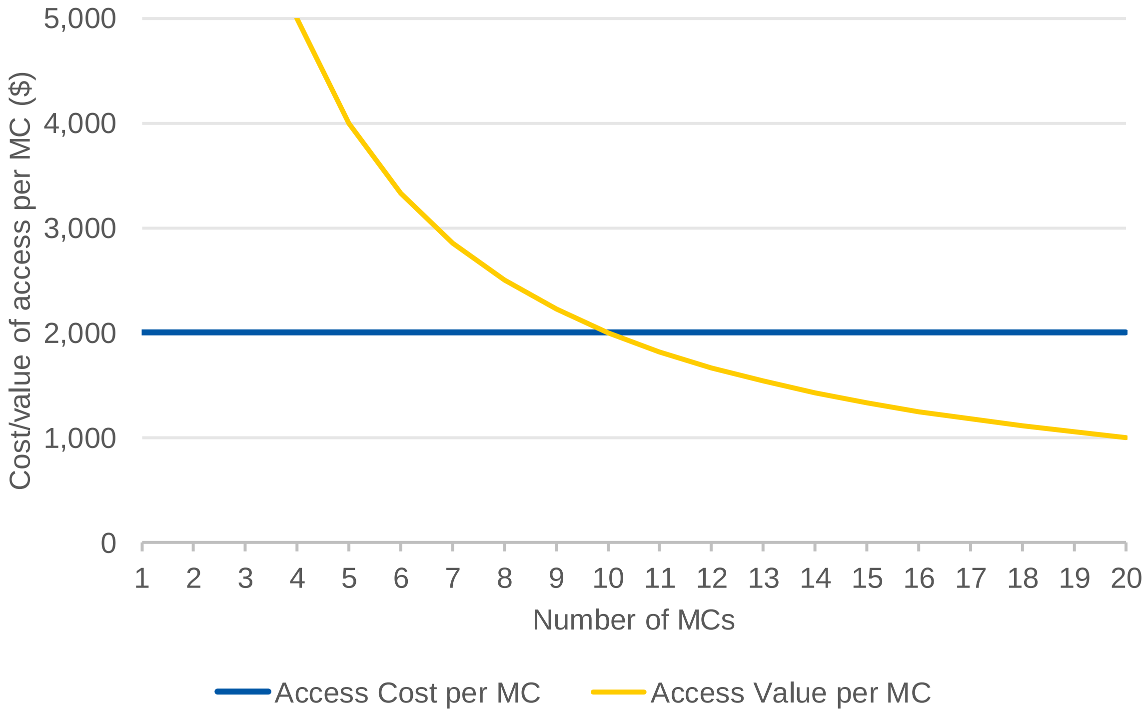
In addition, once access has been arranged, the data itself may not be in a consistent format, and it must be merged with data from other MCs before it is useful. Therefore, the processing costs must be incurred several times over, once for each MC.

As a result, the costs that a DNSP must incur to obtain access to data from a single MC may be smaller than the value that it would extract from having that access, since a single MC will only have data for a subset of a DNSP's region.

In other words, the costs of a DNSP obtaining data access are primarily a function of the number of MCs it has to engage with, while the value the DNSP extracts is primarily a function of the number of sites that that MC can provide data for. As the number of MCs increases, the value of obtaining data access from any one of them decreases, and at some point is less than the cost of access.

We illustrate this in Figure 3.1 below. Suppose that there are 10,000 smart meters in a DNSP's region, the data from each of which is worth $1 to the DNSP (irrespective of how much data it already has from other meters). Therefore, the total value of the data from those meters in the DNSP's region is $10,000. Suppose also the process of negotiating, obtaining and analysing all data from a single MC costs a DNSP $2,000 (including any payment the MC requires to cover its own costs). If there are fewer than five symmetrical MCs, then the value of the data of each one is over $2,000, and it should be in the interest of both parties to negotiate access rights. If there are more than five MCs, then the value of the data is not worth its cost.

Figure 3.1: Illustrative Example of Data Access Costs and Value



This illustration makes several assumptions that may not hold in practice:

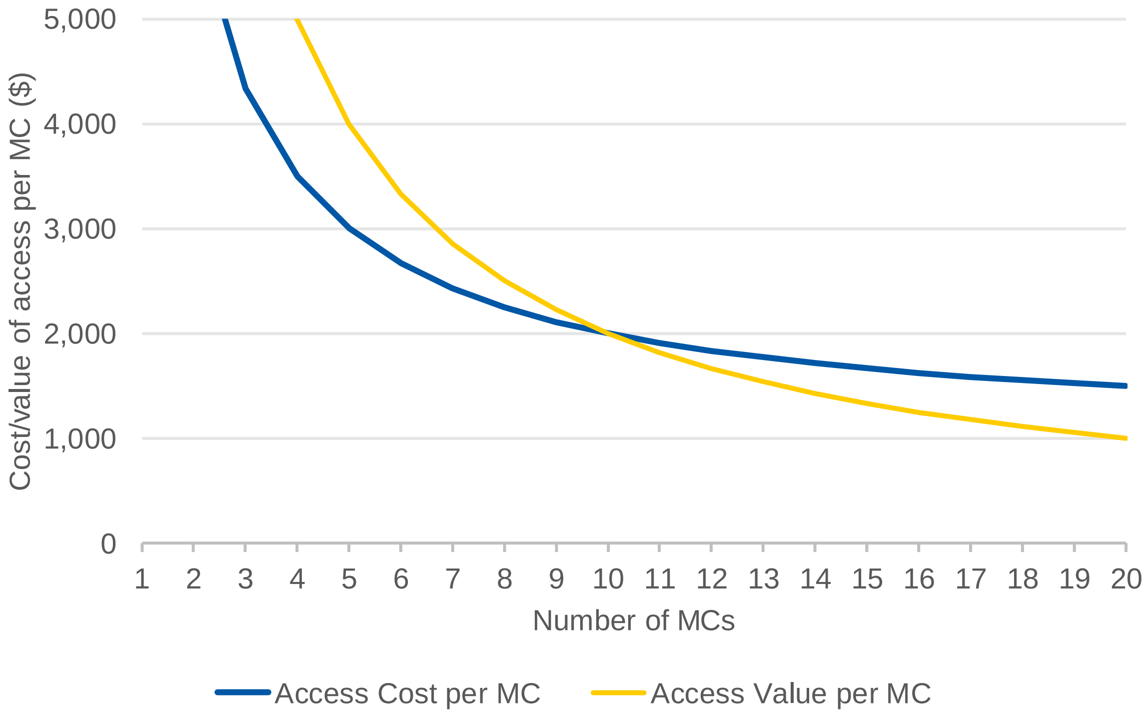
- The cost of obtaining access is fixed per MC irrespective of their size or number of MCs. In reality, it may cost more in absolute terms to obtain data from a large MC than a small one, if there are costs that vary with size (e.g. bandwidth of transmitting large amounts of data). Likewise, once a DNSP has obtained access from several MCs, the cost of obtaining access from another one may be lower, if, for instance, it can re-use some of the same templates.
- The value of data may not be fixed from each meter. For example, some use cases for data may only require data from a few well-located smart meters (e.g. to identify outages), while others may require near complete data coverage.
- The total number of smart meters in the DNSP's region is static. At present, most states have rolled out smart meters to around 25 per cent of end-users.[6] As this rollout rate increases, the total value that can be obtained from smart meter data access increases. If the number of MCs stays similar, then the total value that each MC's data contains will increase.
- All MCs are identical in the number of meter points they operate.

In Figure 3.2 below, we adjust this illustrative example to control for some of the assumptions listed above:

6 As advised by the AEMC.

- We assume that there are now 20,000 smart meters in the DNSP's region, reflecting a further state of the rollout. Accordingly, the value that can be obtained from all smart meters is $20,000 instead of $10,000; and
- We assume that the costs of obtaining data access is partly proportional and partly fixed, equal to $1,000 plus $0.50 per meter. To obtain access from an MC with 4,000 meters, for example, it would cost $1,000 plus $2,000, or $3,000 in total. This could also capture some limited economies of scale from replicating data access processes across many MCs.

Figure 3.2: Illustrative Data Access Costs and Value with Economies of Scale and Further Rollout



As the figure shows, in this variation of the illustrative example, data can be split between more MCs and still be worthwhile for a DNSP to obtain, but there is still a point (10 MCs) beyond which it is not worth the cost. In fact, so long as there is a fixed element to obtaining access (e.g. the cost of developing the agreement), there will be a point beyond which it is not worth the money to obtain access.

The analysis above describes a national market of MCs, but in reality some data requests may be geographically targeted to a specific street. If these requests are fragmented and cannot be consolidated, then the costs that an MC would incur to prepare and provide data could exceed the value that a DNSP could receive from access to that data. In addition, a single MC may hold exclusive access to all of the data in that location, giving the MC a highly localised form of market power. MCs would then be free to offer to provide data access at any price above its costs, which may be above the willingness of a DNSP to pay for it. This challenge could be mitigated by spreading the scope of any negotiations across a wider geographical region, so that the value a DNSP receives from gaining access is larger relative to the cost of negotiation.

3.2. The potential for market power introduces a challenge of coordination

In Section 3.1 above, we set out an illustration of some of the challenges of data access arrangements in a static world, where DNSPs must simultaneously seek to access data from all MCs. In reality, these negotiations would happen sequentially,[7] which introduces the potential for MCs to exercise market power to extract higher payment from DNSPs for the data.

At present, there are many MCs competing with one another in individual DNSP regions, and so market power would not generally exist if the value of the service that each could provide to DNSPs was independent of the actions of one another. However, the value that data can provide may be partially dependent on the extent of the data that the DNSP already holds. Additionally, in some jurisdictions, there may be only one or two MCs that hold significant local market power.

For example, if a particular MC is the first MC to provide data access, its data may be too limited in scope to provide any value to the DNSP. If, on the other hand, the DNSP already has access to data from several other MCs, the next MC could potentially increase the usefulness of all of the data the DNSP already has, and hence provides considerable value to the DNSP. Some use cases may require a minimum threshold of data before any is useful, which means that the MC that can push coverage past that threshold could be in a position to negotiate a particularly advantageous agreement for their data.

This dynamic presents a "holdout problem", where MCs have an incentive to not be a first mover in order to take advantage of the greater value their data could have if other MCs move first. The challenge of course is that someone must move first, when no one has the incentive to do so.

The "holdout problem" is discussed in the academic literature, particularly in the context of land acquisition. Miceli and Segerson (2012) develop a framework in the case where the government must acquire land to build a new public service project, such as a railroad or a highway.[8] In this setup, the project will only go ahead if all landowners agree to sell their land to the government.

Miceli and Segerson define three key conditions for this holdout problem to occur:

(1) there are multiple landowners and bargaining with them occurs sequentially;

(2) there is commitment during the bargaining process; and

(3) partial assembly is inefficient.

These three conditions can apply to the case of data access: (1) there are multiple MCs and bargaining happens sequentially; (2) the commercial arrangements that DNSPs have with

[7] Even if a DNSP was negotiating with multiple MDPs in parallel, it is unlikely these negotiations would all commence and conclude at the exact same time. And indeed, an MDP could hold out by waiting to either begin or conclude negotiations.

[8] Miceli, Thomas J., and Kathleen Segerson. *Sequential Bargaining, Land Assembly, and the Holdout Problem*. No. 2011-13. 2012.

MCs are presumably enforceable; and (3) existing data becomes more valuable once the full set of data is complete.

This problem can be thought of as the sum of highly localised instances of market power, where one MC holds exclusive power over all of the data in a small area (e.g. a single street). With power to hold up the process of data acquisition at any stage (and knowing that any other MC in a nearby area could equally do so), MCs face little incentive to incur the costs and act first.

Miceli and Segerson's characterisation of the holdout problem provides a useful structure for how to resolve the problem as well, as all three of the conditions listed above must hold in order for the holdout problem to exist. If a new regulatory framework can resolve any of the three conditions, then the coordination component of the challenge is mitigated (though other challenges may still exist which prevent MCs from wanting to move first).

For example, a regulatory framework that requires simultaneous commitment from MCs before any data access is provided and any payment is made could limit the ability for any MC to hold out. Likewise, if the payment structure introduces an incentive for an MC to act earlier, such as a reward scheme for those MCs who act first, this can also be used to offset the incentive to delay action.

3.3. Objectives of a New Regulatory Framework

If a new regulatory framework is to be successful in resolving the current challenges in MCs obtaining data access, it must resolve each of the two fundamental challenges described above: it must ensure that the costs of obtaining data access are lower than the value that can be generated from it, and it must ensure that MCs no longer have an incentive to holdout. This is a pass/fail criterion: if the framework fails to resolve the fundamental challenges, then the other criteria are irrelevant.

All of the options we present were selected because they are likely to satisfy this fundamental criterion. Beyond the fundamental pass-fail criterion, each potential option can be evaluated against several other secondary criteria:

- **Cost and ease of implementation**: Can the new framework be implemented without undue burdens to the industry, both in terms of financial cost and the time and complexity of compliance?
- **Ongoing costs of framework**: What are the costs of providing data access on an ongoing basis? Do industry participants have to incur unnecessary costs that do not deliver value? Are there high ongoing costs required to enforce compliance?
- **Ease of price formation**: Is it clear how prices for data are set, and how the additional value created is split between DNSPs and MCs?
- **Flexibility to new use cases**: If a new type of data is deemed to be useful, or to have value in a new use case, can the regulatory framework easily adapt to incorporate the new use case?

4. Case Studies of Market Access

To inform the options for a new regulatory framework for data access, we consider a range of different international and local case studies:

- In Victoria, DNSPs are responsible for installing and maintaining smart meters, and also have direct access to all of the technical data that they collect. While this type of model is not currently an option the AEMC is considering, it can provide a benchmark for what an effective access arrangement could achieve.
- In Great Britain, retailers are responsible for installing and maintaining smart meters, but each smart meter includes a specialised piece of communications equipment owned by the Smart Data Communications Company (DCC), a price-controlled monopoly entity. DNSPs in Great Britain collect half-hourly data on a monthly basis and use it to improve their planning processes.
- In New Zealand, retailers are required to provide consumption data to DNSPs in a pre-set format, with DNSPs obligated to pay the reasonable costs that retailers incur in doing so. Retailers and DNSPs can agree to provide PQ data beyond this, but there is no defined framework for doing so.
- In Australia, shippers of natural gas who require third-party access to gas transportation infrastructure are entitled to access under certain circumstances under a negotiate-arbitrate framework. This framework represents a model for how a negotiate-arbitrate framework could exist in the context of smart meter data access.

4.1. Victoria

In Victoria, DNSPs rolled out smart meters during 2009 to 2015, including the communications network that supports data sharing from the smart meters. As a result, they hold and manage all of the data collected by smart meters. This case study provides an example of what kind of data could be collected and used by DNSP if they had perfect access arrangements with MCs, as no access arrangement could be better from the perspective of a DNSP than already holding the data.

To learn more about how smart meter data works in Victoria, we spoke with the metering and data teams from United Energy, CitiPower and Powercor, with a particular focus on United Energy practices which are mostly applicable to all Victorian DNSPs.

4.1.1. Data collected

United Energy faces a trade-off between collecting as much data as it can possibly use, while also ensuring that it does not overload the bandwidth of the dedicated smart meter communications network. If it collects excessive data, this slows down the speed at which it can obtain this data and could impact the 30-minute billing data collection.

United Energy collects data on voltage, current and power factor, and in some cases meter temperature. Smart meters transmit five-minute interval data every 15 minutes, with each transmission containing data from the period 10 to 15 minutes previous, five to 10 minutes previous, and zero to five minutes previous. 10-second interval data is also recorded on the meters, and is collected by the DNSPs in near-real time on an ad hoc basis to verify faults based on certain meter alarms or interpretation of the five-minute data.

4.1.2. Smart meter coverage

Due to the mandate to roll out smart meters which has been in place for over 10 years, United Energy reports that roughly one per cent of residential and small business its customers are *not* equipped with smart meters. This allows for two types of benefits which might not be applicable to the rest of the NEM.

First, the high coverage means that data can be used for more detailed purposes, such as phase allocation, ensuring customers are allocated to the correct transformer, phase and transformer load profiles, accurate fault location detection, electricity theft location detection, and so on. In areas where coverage is more limited, DNSPs should still be able to identify network outages from metering data rather than from customer complaints, but most technical use cases are not possible.

Second, high coverage allows for better communication from smart meters to the DNSP, as communications can be "meshed" across the network. That is, one smart meter can communicate with another one nearby, which can communicate with another, and so forth until the data is received. In areas where coverage is more limited (e.g. houses are spaced further apart even if all have smart meters) or smart meter ownership is fragmented, some data must be communicated via cellular networks, which is more costly and slower.

4.1.3. Third-party access to data

While third-party requests for metering data are rare, United Energy tends to accommodate them free of charge. We understand that if a bespoke request requires 10 hours to prepare, United Energy (and its affiliates) are allowed to charge the user, but in practice they do not usually do so.

While DNSPs themselves use technical data on a systematic and ongoing basis, the third-party uses of data tend to be bespoke and infrequent. For example, United Energy has provided data to universities, councils, and the Australian Bureau of Statistics (ABS) for the purposes of research. United Energy reports that there has been no demand yet to provide a steady stream of data to third parties in the fashion that MCs would provide a steady stream to DNSPs. Data in these circumstances is anonymised such that no data point can be spatially identified.

4.1.4. Lessons learned

The Victoria case study demonstrates the value of reaching a high degree of rollout, as a wide range of use cases become available which can deliver significant value to customers. Many of these use cases are not yet available in the rest of the NEM, such as phase allocation and other real-time operational uses. These potential uses may be possible in several years' time if the rest of the NEM reaches near 100 per cent roll-out, but the present uses of smart meter data outside of Victoria is limited to those that rely more on the dispersion of smart meters across a wide area rather than a complete picture of every megawatt that is being distributed across the network.

Victorian DNSPs collect data frequently enough (every 15 minutes) that they are able to manage their networks on a near real-time basis. This frequency may be necessary for some use cases, e.g. responding to outages without waiting for it to be reported. The case study also demonstrates that data collection at that frequency is technically feasible, at least in areas where smart meter coverage is high enough to allow for meshing of the communications network.

4.2. Great Britain

In Great Britain, retailers are responsible for installing smart meters and for maintaining the physical asset, generally through the appointment of a Meter Asset Provider (MAP) and Meter Operator (MOp). The MAP manages the asset itself, while the MOp manages the operations and the data it contains. All of the large retailers operate as MAPs and MOps themselves. Similar relationships exist in the provision of gas smart meters, but we do not focus on them for the purposes of this report.

While the provision of meters is dispersed amongst several large, geographically overlapping retailers, the transmission of data is centralised within the DCC, a regulated monopolist company.

The DCC is responsible for the communications infrastructure than enables the secure transfer of data from smart meters to energy suppliers, network companies, energy service companies and other authorised parties (such as the National Grid). The DCC also owns the communications hub that fits on top of the smart meters. The DCC infrastructure ensures that the same smart meters can be used with different electricity suppliers and so ensures interoperability. The DCC is regulated by Ofgem under a price control regime. While the DCC transmits data, it does not own the data itself, which belongs instead to retailers.

4.2.1. DCC costs

The DCC's price control regime is based on its actual costs, submitted to the energy regulator Ofgem by July following the end of each regulatory year ending in March.[9] These are primarily external costs – those charged to the DCC by external service providers for delivering key parts of the smart metering service, including core contracts for delivery of data and communications services. A large part of this is the setting up of communications infrastructure and its ongoing provision. The DCC also incurs substantial internal costs (incurred directly by the DCC licensee) – this includes staff headcounts, overheads and the allowed margin, as well as several of their smaller contracts.

We provide the DCC's forecast costs to March 2025 in Table 4.1 below. Retailers must then pay the DCC its allowed revenue. For electricity tariffs which are subject to price caps, the price cap itself has a term that passes through the DCC cost to end users. For scale, there are presently around 15 million smart meters in Great Britain, so these costs work out to around £40 per smart meter per year (though retailers typically spread this across all their customers, not just their smart-enabled customers).

9 Ofgem (25 February 2021), DCC Price Control: Regulatory Year 2019/20.

Table 4.1: DCC Cost Forecasts

Total DCC costs	RY2020/21	RY2021/22	RY2022/23	RY2023/24	RY 2024/25
Internal Costs	96.7	89.6	79.7	73.8	70.2
External Costs	453.9	358.2	303.5	293.9	292.3
AltHANCo	25.7	24.0	16.4	16.5	15.1
Other costs	41.6	38.9	37.1	33.3	33.3
Sub total	618.0	510.7	436.7	417.5	410.9
Communications Hubs	41.4	59.4	90.6	127.3	171.9
Explicit Charge items	3.5	8.6	22.7	32.5	35.0
Total	**662.9**	**578.7**	**550.0**	**577.3**	**617.8**

Source: DCC Business and Development Plan 2020/21-2024/25.

4.2.2. Data collected

Retailers report that they share customer data with industry parties (network companies who help manage the energy supply, distribution and central industry systems), the police (for fraud detection), and to Ofgem or other public sector organisations (for research purposes). Data is anonymised unless it is part of a police investigation.[10]

DNSPs can access domestic consumption data down to half-hourly granularity without customer consent provided that they develop a data management plan which is approved by Ofgem. This plan must ensure that data is only used for regulated purposes and that they aggregate data such that it can no longer be associated with a domestic customer at an individual premise. DNSPs must also provide an explanation of the purposes for which their data access would be beneficial and to set out their IT security and data deletion practices.

All six DNSP groups have submitted and received approval for a data management plans. The networks' uses of the data is similar: All collect data on a monthly basis, though the data itself is typically at a half-hour granularity; Data must be aggregated to the level of a low-voltage feeder (which provides geographical granularity but makes it impossible to tie data to a specific premises); Data focuses on consumption at the feeder level, feeder-section level, and substation level.

To our knowledge, no DNSP has an arrangement to collect PQ data, though at least one DNSP (UK Power Networks) collects half-hourly flows of both active and reactive power, the ratio between which defines the power factor. UK Power Networks reports that it will use this data to improve planning of reinforcement of the existing network, improving design and planning to accommodate new and increased capacity connections, and build efficient networks that can use real-time data that can respond intelligently to network conditions.[11]

10 OVO Energy Smart Metering Guide.

11 UKPN (December 2019), Data Privacy Plan for Access to Smart Meter Consumption Data, p.5.

4.2.3. Lessons learned

The Great Britain case study provides an indication on how a centralised data management programme could work and what it could cost. The British model does not require any commercial negotiation between DNSPs and any other party, but instead requires DNSPs to apply for approval to Ofgem, who assess the applications primarily on the basis of data privacy and security.

While the ownership of smart meters is decentralised, the process of data management is centralised. The DCC bears the costs of managing a single communications network and putting data into a consistent format, but these costs are not replicated across many different retailers. Additionally, DNSPs only interact with Ofgem (in applying for access) and the DCC (in receiving the data). Therefore, unlike the present situation in the NEM, DNSPs do not need to hold many, simultaneous negotiations across a disparate set of MCs.

DNSPs do not pay for data access, though they will incur costs internally to process and manage data (including the creation and execution of a data privacy plan). This means that DNSPs will wish to obtain as much data as possible, so long as the value that is generated by the data is greater than the cost of processing it.

DNSPs have deemed that the most cost-effective set of data is half-hourly, locally granular consumption data, but collected only on a monthly basis. This data can improve DNSPs' planning and reinforcement practices and may reduce the likelihood of system failures (i.e. if the system is planned more effectively). However, with data received only on a monthly basis, DNSPs cannot presently use data to respond in real time to the performance of the network.

We have not found any instances of DNSPs collecting PQ data specifically, but UK Power Network's Data Privacy Plan suggests that they eventually intend to use near real-time data to respond to network conditions on an operational basis.

4.3. New Zealand

The smart meter data system in New Zealand is generally decentralised, such that industry participants exchange data amongst themselves to enable transactions. The Electricity Authority (EA) has established various Electricity Information Exchange Protocols (EIEPs) for regulated data exchanges[12] within the industry, which are mandatory to adhere to when exchanging the relevant data per the Electricity Industry Participation Code 2010 (Code), unless the relevant parties determine an agreement in their contract to do so otherwise.[13]

4.3.1. Parties' responsibilities

The EA regulates the standards, installation, testing, accuracy, reading and data security requirements for meters.

---

12 EIEPs for non-regulated data exchanges have also been established, but are only recommended to adhere to rather than mandatory.

13 Code, Schedule 12A.2, Clause 3. The agreement in a contract to exchange information other than in accordance with the relevant EIEP is only valid when the agreement has been entered after the relevant EIEP comes into effect.

Retailers are responsible for ensuring a metering equipment provider (MEP) is recorded in the registry as being responsible for each metering installation and maintenance of that meter. This MEP, therefore, retains the rights and access to all smart meter data relating to the meter installation. The MEP must provide access to this metering data to the retailer.

Retailers must also enter an agreement with DNSPs which stipulates the retailer must supply consumption data to the DNSP when requested.[14] A "default distributor agreement" (DDA), being the use of system agreement between the retailers and DNSPs, was introduced as an amendment to the Code in July 2020 to address industry concerns about efficiently obtaining consumption data.[15] The EA provides a DDA template in the Code, but distributors may alter terms that the retailer and DNSP both agree to.[16] DNSP access to consumption data is limited to the terms on which it is agreed to by the retailer and for its expressly approved purposes. Unless otherwise expressly mentioned, the DNSP does not have rights to or in connection with consumption data.[17]

4.3.2. Data collected

Retailers, by nature of obligations in the DDA, must provide consumption data to DNSPs using the relevant EIEPs. The EA has multiple regulated EIEPs relating to the exchange of volume and billing information.[18]

First, EIEP1 requires detailed billing and volume information at the residence level provided on a six-monthly basis to be provided between the retailer and the DNSP. The EIEP1 file includes, among other details, mandatory disclosures of the meter read and energy flow direction, though this does not capture the granularity of data that is collected by smart meters.

For smart meter data specifically, the EIEP3 covers half-hour metering information from retailers to DNSPs, such that DNSPs can invoice retailers for fixed and variable network charges associated with a residence where half hour metering information is required. However, an EIEP3 file is generally not required where an EIEP1 file can provide the information required for billing of network charges.[19]

When exchanging half-hourly meter data, the EIEP3 format file includes mandatory disclosures of data by residence including real energy import and export (in kWh) together with either or both reactive energy import and export (in kVArh) or apparent energy import and export (in kVAh). Unless otherwise agreed by the parties, the EIEP3 file containing half hour metering information for the previous period must be delivered by the 5th business day of the current month.

---

14 Code, Schedule 12A, Appendix C.

15 EA (July 2021), *Updating the Regulatory Settings for Distribution Networks: Improving competition and supporting a low emissions economy – Discussion paper*, p 27.

16 EA (16 June 2020), *The Default Distributor Agreement – Decisions paper*, para 2.10.

17 Code, Schedule 12A, Appendix C, para. 5.

18 EA, "Electricity information exchange protocols (EIEPs)", available at https://www.ea.govt.nz/operations/retail/eiep/.

19 EA (April 2021), *EIEP3: Half hour metering information*, available at https://www.ea.govt.nz/assets/dms-assets/25/25671EIEP3-v11-regulated-Half-hour-metering-information.pdf.

Other non-regulated EIEPs include data regarding unplanned service interruptions and fault notifications.[20] The EA encourages industry participants to use these EIEPs even in non-regulated exchanges, though we understand from discussions with DNSPs in New Zealand that very little non-regulated data is actually provided in practice.

The Code also allows for the EA to establish an information exchange system – presently, an EIEP transfer hub using secure file transfer is provided but not mandatory to use. EIEP files are required to be submitted in a comma delimited text file. Submission of files is commonly through the registry EIEP transfer hub, but other secure file transfer or email is also acceptable.

Where data is required to be provided from a retailer to a DNSP, the DDA stipulates that the DNSP must pay the retailer's or MEP's "reasonable costs" of providing the data. Additional exchanges are commercially negotiated.

The above focuses on consumption data. There is no EIEP relating to PQ data and no obligation to provide this data to DNSPs. Thus, PQ-related data access, pricing and exchange framework is completely unregulated in New Zealand.

Because this data is of little to no use to retailers, retailers have not contracted with the MEPs for this data. However, we understand that DNSPs can contract directly with MEPs for PQ data instead. There are two MEPs in New Zealand that service 75 per cent of the market with 12 smaller MEPs generally serving specific geographical regions,[21] compared to 41 retailers doing business across New Zealand. Thus, the number of parties a DNSP has to deal with in order to access PQ data on its network is smaller than the number of retailers it must interact with to access consumption data.

4.3.3. Implementation challenges

A clause exists in the existing template DDA which stipulates that consumption data received by the DNSP may not be combined with any other data without the written agreement of the retailer or MEP.[22] There are 41 electricity retailers across New Zealand – this means that the DNSP would need to obtain permission from every retailer to map the data to every dataset, and if some retailers do not agree, then the DNSP must manage dropping data out each time a consumer switches to a retailer who has not provided permission. We understand that in practice, this makes obtaining useful and easily manageable data difficult. As an example, we understand that Vector, the largest DNSP in New Zealand, has not yet received any data under the DDA.

The EA recently declined a proposal to amend the template DDA regarding this issue, but have noted that if evidence is submitted showing that this is a significant issue to distributors

---

20 EA, "Non-regulated electricity information exchange protocols", available at https://www.ea.govt.nz/operations/retail/eiep/non-regulated-electricity-information-exchange-protocols/.

21 For example, Counties Power is a certified MEP serving the Counties-Manukau region, and Network Waitaki is a certified MEP serving North Otago. A full list of the certified MEPs in New Zealand is available at https://www.ea.govt.nz/assets/dms-assets/22/22179MEP-register.html.

22 Code, Schedule 12A, Appendix C, clause 5(1)(e).

securing data on reasonable terms it may consider an amendment to the template DDA presented in the Code.[23]

Additionally, no minimum standard of data collection for metering installations has been set out in the Code, and as such we understand that many smart meters are not set up to collect additional data aside from basic consumption. This means that some PQ data which DNSPs may be interested in is not available through the meter without updates, which could require a site visit to update the firmware as not all meters can be remotely updated.

A final issue, noted with respect to purchasing PQ data, is that DNSPs have opex allowances set in a mechanistic fashion that projects forward historic expenditure, using a similar approach to the base-step-trend approach applied by the AER. Without a step change or specific additional allowance for data purchases, DNSPs would be purchasing this data without compensation.

The EA has recognised issues around obtaining the data required for DNSPs to make informed investment and operational decisions in a recent discussion paper, in which it proposes potential options to address this issue.[24] In the discussion paper, it sets out various options depending on whether the issue is determined to be a minor issue, a medium-sized issue, or a significant issue.

In the event it is determined data access a minor issue, the EA suggests taking steps to encourage distributors to collaborate themselves in finding the most efficient way of capturing and publishing utilisation data. For a medium-sized issue, the EA suggests assessing options to implement shared data arrangements and publishing guidance for distributors to report on export congestion and network investment needs. For a significant issue, the EA suggests exploring a central meter data store (which is similar to the DCC discussed in our Great Britain case study) or shared data through an application programming interface (API).

4.3.4. Lessons learned

Compared to the current set-up in the NEM, retailers in New Zealand are subject to specific standards on how they provide data. For these minimum standards, the EA is prescriptive in the format and template that it must be provided in. It also must be provided such that only "reasonable" costs are charged to DNSPs, but prices are not prescriptive.

However, the required data transfers are limited in scope, relating only to the data that must be provided to bill retailers for their use of distribution networks. For additional types of data which could be used for the use cases seen in Victoria, and to a lesser extent Great Britain, the EA sets out only the format of the data template (for some transactions) and transfer system, but does not regulate any of the terms of access. Indeed, for PQ data there are no regulatory access obligations, templates or pricing principles. Access for this data must therefore be commercially negotiated. While we understand that DNSPs do not have widespread access to PQ data yet, because they only need to negotiate with a small number of

[23] EA (July 2021), *Updating the Regulatory Settings for Distribution Networks: Improving competition and supporting a low emissions economy – Discussion paper*, p 28.

[24] EA (July 2021), *Updating the Regulatory Settings for Distribution Networks: Improving competition and supporting a low emissions economy – Discussion paper*, p 29-30.

MEPs (being the MEPs that operate in their network area, which is likely a small subset of the MEPs operating nationally), it may be that these negotiations are more successful than if they had to negotiate with a broader set of retailers.

Additionally, the default agreements written in the Code contain limited use clauses which hinder DNSPs' ability to easily make use of the data, and due to a lack of minimum data standard on meter installations, some PQ metering data may not be available without physical updates to meters.

Unlike in Great Britain, data does not need to be aggregated to the point where a DNSP cannot identify the exact premises it relates to.

4.4. Gas Pipeline Access in Australia

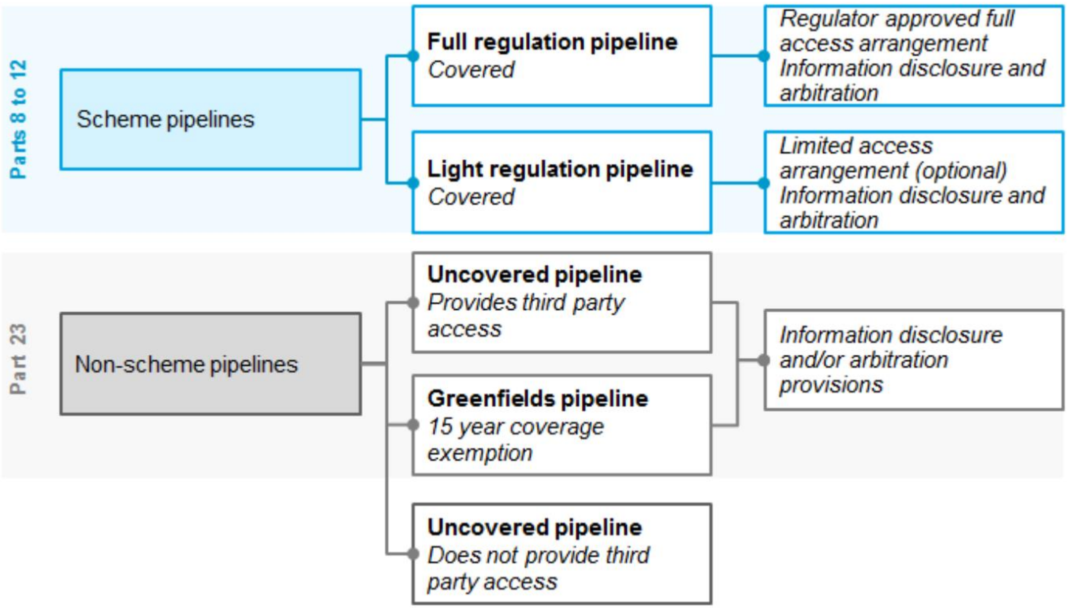
For our final case study, we depart from the world of smart meters and data management, and instead discuss gas pipeline third-party access in Australia. While the nature of the product is clearly different, the economics are similar in that one party is the sole holder of the product (e.g. the pipeline owner controls pipeline access, and the MC owns its data), and another party requires access to it that it cannot acquire from an alternative source. This case study is instructive in terms of how asymmetrical parties can negotiate with each other under a negotiate-arbitrate framework.

4.4.1. Industry and regulation structure

In Australia, producers and consumers of natural gas ("shippers") need access to natural gas distribution and transmission pipelines to transport gas. As a generalisation, the main pipelines are provided by firms who are not vertically integrated into upstream or downstream activities.

All gas pipelines that provide third-party access are subject to some form of economic regulation, unless they have obtained an exemption. The regulation of transmission and distribution pipelines is currently based on the classification of pipelines as either covered (or "scheme" pipelines) and uncovered ("non-scheme") pipelines. The current regulatory framework for pipeline regulation is captured in Figure 4.1.

Figure 4.1: Pipeline regulatory framework



Source: Figure 1.1 of AEMC (2018), "Review into the scope of economic regulation applied to covered pipelines", Final report, 3 July 2018.

The test of whether a pipeline is covered or not (the "coverage test") is based on an assessment against the following four criteria:

- Access to the pipeline would promote a material increase in competition in at least one market, other than the market provided for by the pipeline;
- It would be uneconomic to develop another pipeline to provide the pipeline's services;
- Access to the pipeline can be provided without undue risk to human health or safety; and
- Access to the pipeline would not be contrary to the public interest.

If a pipeline is deemed to meet all four criteria, then it is a "covered" pipeline. A further test then determines whether full or light regulation applies.[25] The Energy National Cabinet Reform Committee is currently proposing to reform these arrangements, partly due to the fact that there are three overlapping forms of regulation (Full, Light and Part 23) and concerns that the coverage test may be resulting in under regulation.[26] Under the preferred option, the coverage test will be removed, and all pipelines will be required to provide third-party access and be subject to a form of economic regulation, with there only being two forms of regulation:

- Stronger regulation – based on full regulation (i.e. negotiate-arbitrate with reference tariffs approved by the regulator and a regulatory-oriented dispute resolution mechanism).
- Lighter regulation – based on the existing Part 23 (i.e. a negotiate-arbitrate model with information disclosure and a commercially-oriented dispute resolution mechanism).

25 The form of regulation test considers the likely cost and effectiveness of regulation of access.

26 Energy National Cabinet Reform Committee (2021), Options to improve gas pipeline regulation: Regulation Impact Statement for Decision, 3 May 2021, pp 22-23.

The stronger form of regulation, while nominally a form negotiate-arbitrate, is essentially direct price control due to the inclusion of "reference tariffs" which are calculated using a building blocks model. If an arbitration is triggered, the tariff reverts to the reference tariffs.

For the lighter form of regulation, the arbitration mechanism is "commercially orientated", because the arbitrator is a commercial arbitrator rather than the regulator.[27] Because there are no reference tariffs, there is uncertainty as to the outcome of any negotiation, which is a design decision made to encourage genuine negotiation. If a dispute is triggered, then the arbitrator must take into the following when making their determination:

- the principle that access must be on reasonable terms (i.e. terms that, so far as practicable, reflect the outcomes of a workably competitive market);
- the pricing principles in Rule 569 of the National Gas Rule (NGR); and
- the operational and technical requirements necessary for the safe and reliable operation of the pipeline.

4.4.2. Pricing principles in arbitration

As stated above, if a dispute is triggered under the lighter form of regulation, the arbitrator must set a price for access that reflects the pricing principles of Rule 569 of the NGR, which are as follows:

1. The price for access to a pipeline service on a non-scheme pipeline should reflect the cost of providing that service, including a commercial rate of return that is commensurate with the prevailing conditions in the market for funds and reflects the risks the service provider faces in providing the pipeline service. For the purposes of this rule:
    a. the value of any assets used in the provision of the pipeline service must be determined using asset valuation techniques consistent with the objective of Part 23 (i.e. to facilitate access to pipeline services on reasonable terms, which is taken to mean at prices and on other terms and conditions that, so far as practical, reflect the outcomes of a workably competitive market); and
    b. unless inconsistent with paragraph (a), the value of any assets used in the provision of the pipeline service is to be calculated using the recovered capital method (i.e. the construction cost plus capital expenditure since commissioning less the return of capital recovered and the value of pipeline assets disposed of since commissioning).
2. When applying the principle in paragraph (1) to a pipeline service that when used affects the capacity of the non-scheme pipeline available for other pipeline services and is priced at a premium or a discount to the price for a firm haulage service on the relevant non-scheme pipeline – the premium or discount must:
    a. take into account any opportunity cost or benefit to the service provider of providing the pipeline service, having regard to any effect on the cost of providing firm haulage services or the capacity of the non-scheme pipeline; and
    b. be consistent with the price for the pipeline service providing a reasonable contribution to joint and common costs.

[27] The arbitrator is selected from a pool of arbitrators appointed by the regulator.

In other words, the price must generally reflect the cost of service, including the cost of assets used in providing the services (e.g. the pipeline infrastructure itself). The rule allows for flexibility in how the price contributes to the paying of joint costs.

4.4.3. Lessons learned

The negotiate-arbitrate framework seen in the context of gas network access represents a relatively light-touch and non-prescriptive form of regulation, which gives both parties considerable leeway in determining the terms of access. While the arbitrator must follow pre-defined principles in the event of a dispute, they also have considerable leeway in determining how to apply those principles with respect to recovery of fixed investment costs and allocating joint costs.

Nonetheless, the negotiate-arbitrate framework removes the pure commercial element, where the pipeline owner could extract the maximum value that it believes that the shipper is willing to pay, without any reference to the cost of services.

5. Options for Data Access

Having considered the theoretical root of the problem in Chapter 3, and identified lessons from other jurisdictions and industries in Chapter 4, we set out a range of options which the AEMC could consider as a new regulatory framework for data access.

As an overarching set of lessons and design principles, we conclude the following:

- Where possible, reducing the number of parties that need to negotiate with one another reduces the transaction costs of attaining access, because DNSPs do not need to negotiate with as many parties or process as many different pieces of information. Additionally, reducing the number of parties will reduce the incentive of one party to hold out, as they cannot as easily expect another party to act first and increase the value of its own participation.
- Similarly, a more prescriptive set of rules reduces the scope and associated cost of negotiation, as well as the ability for parties to hold out. On the other hand, a more prescriptive framework likely costs more to implement, may cause MCs to provide data which is not actually valuable to DNSPs and is less flexible to updating use cases.

While smart meters can collect technical data at short intervals, there are legitimate costs associated with transmitting data on a near real-time basis. In Victoria, where there is no interface between the smart meter data and DNSPs, and where smart meters are dense enough to allow a meshed communications network, DNSPs read data every 15 minutes. Even with a well-functioning access arrangement, this may not be possible at present in the rest of the NEM, where smart meter uptake is considerably lower across an area which is less dense on average than Victoria/meter ownership is fragmented so a mesh network may not be possible.

With these overarching lessons in mind, we develop and discuss the following options for a new regulatory framework, approximately from most to least prescriptive:

- Implement a DCC-type organisation and mandate the types of data that must be provided through it.
- Set minimum standards for bilateral engagement between retailers and DNSPs but allow for additional commercial engagements beyond the minimum standard.
- Establish an exchange architecture (e.g. APIs) with defined roles but allow parties to participate freely within it.
- A negotiate-arbitrate framework, where arbitrators are subject to guiding principles when making a determination.

We compare these options against the criteria we set out in Chapter 3:

- **Provision of data access:** Will the framework overcome key obstacles and ensure that DNSPs and third parties are able to gain access?
- **Cost and ease of implementation**: Can the new framework be implemented without undue burdens to the industry, both in terms of financial cost and the time and complexity of compliance?

- **Ongoing costs of framework**: What are the costs of providing data access on an ongoing basis? Do industry participants have to incur unnecessary costs that do not deliver value? Are there high ongoing costs required to enforce compliance?
- **Ease of price formation**: Is it clear how prices for data are set, and how the additional value created is split between DNSPs and MCs?
- **Flexibility to new use cases**: If a new type of data is deemed to be useful, or to have value in a new use case, can the regulatory framework easily adapt to incorporate the new use case?

Additionally, we comment on whether each option could be combined with any other option, or whether it could be partially implemented.

5.1. DCC-style Organisation

The most prescriptive approach would be to establish a new company that manages smart meter data and communications, in the mould of the DCC in Great Britain. New Zealand's EA has also suggested considering a similar solution if they determine that access to data is a significant issue for DNSPs. Under this approach, MDPs would effectively cease to exist as a competitively appointed role, and instead a single MDP would be appointed by all MCs.[28] As in Great Britain, the single MDP would be subject to prescriptive codes around what data it was required to collect, over what interval and at what reporting frequency.

In this case, there would be no price associated with the data access itself. The MDP may incur some costs in setting up the ability to collect data (including any communications infrastructure), but this could be remunerated through a separate regulated revenue control, much as is the case for the DCC in Great Britain. DNSPs would seek access to the centralised pool of data if the value it could obtain from it exceeds its cost of processing it.

With only one data manager, there would not be replicated costs to negotiating data access or processing the same data types in different formats from different providers. It would also be impossible for the MDP to hold out.

The principle advantage of this approach is that it would almost certainly work as well as it is designed to. As we have seen in Great Britain, all DNSPs now have data management plans in which they collect half-hourly consumption and load data from all smart meters (aggregated to the feeder level), on a monthly basis. As the needs of the system develop, DNSPs will use this data to more effectively plan the system. While the data required in Great Britain does not include PQ data, there is no inherent reason why it could not.

However, there are several disadvantages to this approach:

- First, it may not allow for much or any flexibility in what data is collected and transmitted to DNSPs. In Great Britain, the types of data that the DCC collects are stipulated in the Balancing and Settlement Code, and DNSPs have submitted detailed Data Privacy Plans to Ofgem to be allowed to access that data. To our knowledge, each DNSP has only

[28] As an alternative to a single national MDP, there could be a single MDP per state, or even network area. This would still address the hold out problem (because each DNSP still only deals with a single MDP), but would result in higher (NEM wide) transaction costs and also potentially higher data provision costs if there are economies of scale in data provision.

submitted a single plan, all within the last two to three years, which sets out what data they will use and how they will use it. If DNSPs wished to change how they use data, this would require at least an update to their data privacy plan, and potentially a change to the rules which say what the DCC must collect. Similar challenges could arise in the NEM. Though this could be mitigated depending on how the obligations on the MDP are designed.

- Second, it is costly to implement, primarily because the industry roles would need to be redefined, and a single MDP may need to be created with its own remuneration structure (e.g. a price control). If that company requires data communications infrastructure as well, this will come at a cost, though we understand that existing networks would be used. Extensive upfront effort will be required to determine what streams of data are most useful on average.
- Third, in setting up data access to a sufficiently wide range of metrics, this framework will inevitably result in the over-collection of certain data streams that are only occasionally useful to DNSPs. This could place a strain on communications infrastructure.
- Fourth, in order to keep the volumes of data manageable, DNSPs may not be able to access data on a daily or sub-daily basis. From our review of Great Britain and New Zealand, DNSPs only ever receive data on a monthly basis or greater (though this contains much shorter intervals within it), in part because of the burden of processing data more frequently than that. In Victoria, by contrast, DNSPs collect data every 15 minutes, but this is an internal process and they can collect only the data they want without any further negotiation.
- Fifth, this model would remove the competitive element from the provision of data collection. However, competition does not appear to be delivering large amounts of innovation specifically in the context of data access, so this may not be a clear disadvantage.

We compare this option specifically against the comparison criteria below.

Table 5.1: Assessment - DCC-style Organisation

Criteria	Comment
Provision of data access	Highly likely to achieve core objective.
Cost/ease of implementation	Expensive to implement.
Ongoing costs	Expensive if irrelevant data is collected.
Ease of price formation	Data provided to DCC free of charge, DCC recovers costs separately.
Flexibility to new use cases	Potentially limited. New policies may need to be written.
Potential to combine with other options	Limited. Already prescriptive roles and responsibilities.
Possibility of partial implementation	Yes, role of DCC could be limited.

5.2. Minimum Contents Requirement

MCs could be mandated to provide a certain level of data to DNSPs and allow for commercial negotiations above that level. This is similar to a proposal submitted to the AEMC by South Australia Power Networks (SAPN), which classifies data into three tiers: the first tier must be provided to DNSPs free of charge (technical data on five-minute intervals provided every 24 hours), while the other two tiers are not mandated (e.g. provided more frequently than daily). We show SAPN's proposal below.

Tier 1 – basic technical data, the provision of which would be mandatory as part of the standard daily meter read, including:

- Voltage, current, real and reactive power including directionality (i.e. export or import)
- 5-minute interval preferred, or aligned with the interval of billing data
- Provided at least every 24hrs along with billing data
- No charge to DNSP, amortised with other service costs

Tier 2 – additional standard data and services not included as part of tier 1, that all meters must be capable of providing, which could be activated as required under commercial arrangements and subject to a fee, e.g.:

- the capability for the provision of same data as Tier 1 but updated on a more frequent basis than the normal daily read cycle, e.g. provided every five minutes and synchronised via an Application Programming Interface (API)
- On-demand meter enquiry service ('ping')

Tier 3 –additional data and services not included as part of tier 1 or tier 2, which would not be required to be available at every meter installation, but could be activated under commercial arrangements if agreed between a DNSP and MC, e.g.

- Near-real-time outage notification ('last gasp').

Tiers 2 and 3 could be provided under a light-handed regulatory regime such as a negotiating framework to ensure that the price for the service / data would be reflective of the incremental cost of providing the service/ data.

Source: SAPN (2021), Submission on AEMC Review of the Regulatory Framework for Metering Services – Consultation Paper (EMO0040), 14 February 2021.

The SAPN proposal is conceptually similar to the status quo for consumption data in New Zealand, which also requires retailers to provide a minimum standard of consumption data but allows for negotiation above this level. New Zealand is also proposing something similar to this in the event they find access to PQ data for DNSPs is a "medium-sized" issue.

In the New Zealand example retailers ultimately own the data they supply to DNSPs, but are required to comply with a data request for consumption data so long as the DNSP's stated purpose for accessing the data is permitted. Unless agreed to by all parties separately from the terms of the template DDA, the DNSP may not use the data for purposes outside of its expressly stated purpose or requested duration (though the requested duration can be an ongoing stream of data).

Like the DCC option, this approach would certainly achieve at least its minimum desired effect, because MCs would not have the opportunity to negotiate the minimum level or their compliance with it. Insofar as there are costs to MCs associated with meeting the minimum contents requirement, these would be borne by MCs and passed on ultimately to end users.

This option is more flexible and likely cheaper to MCs than the DCC option on an ongoing basis, because the list of minimum contents does not need to be as exhaustive. This option also does not require establishing any new entities or roles for existing entities, and hence is cheaper to establish.

However, the costs associated with providing daily data transmissions may still be substantial, especially if smart meters are dispersed enough so as not to allow economies of scale to be reached. Thus, it may be incomplete to consider this option without considering how the costs of transmission are remunerated.

The costs to DNSPs will also be higher than under the DCC option, as the DNSPs will have to manage many different sources of data which need to be merged on a daily basis. Additionally, at least as designed in New Zealand, DNSPs must pay retailers their reasonably-incurred costs in preparing data requests. DNSPs may therefore not want to request as broad a set of data knowing that it comes with the burden of processing it on their end or the retailer's end.

Beyond the minimum contents, it is unclear whether DNSPs and MCs would engage on any of the higher tiers of data or if the same holdout challenges presently seen would persist. They could be further exacerbated if MCs are loss making on Tier 1 (because it is mandatory and may or may not be provided free of charge) and seek instead to recuperate costs on higher tiers.

We compare this option specifically against the comparison criteria below.

Table 5.2: Assessment – Minimum Contents Requirement

Criteria	Comment
Provision of data access	Highly likely to achieve core objective.
Cost/ease of implementation	Relatively low, as can rely on existing entities.
Ongoing costs	Expensive if irrelevant data is collected and not standardised across retailers.
Ease of price formation	Unclear how minimum required data must be remunerated.
Flexibility to new use cases	Flexible, as it allows negotiation beyond the minimum requirement.
Potential to combine with other options	High. Could introduce an exchange architecture to facilitate access.
Possibility of partial implementation	Yes, scope of minimum requirement is flexible.

5.3. Exchange Architecture

In an exchange architecture option, DNSPs and MCs would interact with each other and transfer data through a pre-defined communications structure (for example, through APIs as suggested by the EA in New Zealand) and with partially defined contracts, but without a prescriptive list of what must be provided at what price.

The precise design of an exchange architecture would need to be developed further, but would comprise at least two components:

- A standardised communications interface where suppliers would upload PQ data and DNSPs or third parties would download data, thereby reducing the costs of transferring and managing data. This could have a range of configurations, from a dedicated centralised server (not dissimilar from a DCC-type organisation) to a web-based system that all parties can access. For any configuration, there would be a trade-off between cost and functionality or security.

- A semi-standardised set of contracts that can be adapted for the specific nature of a data request. If most terms can be agreed upon in advance through the establishment and updating of the exchange architecture, then this could significantly reduce the transaction costs relating to preparing a new agreement from scratch each time.

Unlike the options above which would be prescriptive in which party is responsible for providing what, this option could be outcomes-based, in which MCs would be incentivised to achieve certain objectives or outcomes (e.g. reaching a certain data coverage over a certain area) without being as prescriptive on the actions that each party must undertake. For instance, DNSPs could pay MCs according to a set structure where MCs who agree to provide data more quickly receive a larger payment (e.g. crowdsourcing or bounty payment).

While it is not a prescriptive option, this option removes or limits the two core theoretical challenges DNSPs face in obtaining data access:

- Because it would interact with MCs only through a single exchange interface, the DNSP would not have to incur the high costs and burden of repeating the same process many times over; and
- The process of fulfilling a particular data request could be structured so that MCs simultaneously commit to providing the data, which removes the sequential element of the hold-out problem (e.g. payment is not made to any MC until a certain threshold is reached).

Because it is not prescriptive in its contents, this option is flexible to new use cases, so long as the back-end software can support the types of data that are available from smart meters. The ongoing costs of the system are also lower than in the DCC or Minimum Contents options, because data is not provided until it is collected.

However, the cost of the system and its remuneration are not clear. For instance, some current or newly created party must be responsible for developing and maintaining the framework. Most logically, this would be the DNSP because (a) they will ultimately be the party using the data; and (b) they could pass the costs into their own regulated revenue stream. However, if a single MC operates across multiple DNSP regions, they may have to familiarise themselves with several different types of exchange architecture. It is unclear how they would recuperate those costs.

This option also does not oblige MCs to participate in it, and so if the cost of participating exceeds the payment that they receive, then MCs may not provide as much data as they may in other frameworks.

We compare this option specifically against the comparison criteria below.

Table 5.3: Assessment – Exchange Architecture

Criteria	Comment
Provision of data access	Should achieve core objective, but it is not mandated so perverse outcomes are possible.
Cost/ease of implementation	Some costs to implement architecture.
Ongoing costs	Relatively low as data is only collected when needed.
Ease of price formation	Price formation for data access relatively easy but unclear who bears the cost of the architecture.
Flexibility to new use cases	High
Potential to combine with other options	High. Could underpin a minimum contents requirement.
Possibility of partial implementation	No. Architecture either exists or it does not.

5.4. Negotiate-Arbitrate

A "negotiate-arbitrate" framework is as it sounds: two parties negotiate with one another and, if the negotiation breaks down, they have recourse to arbitration. A negotiate-arbitrate framework could be included as a feature of other options, or it could be a standalone option.

As a standalone option, it is the least prescriptive of those discussed in this chapter. Effectively, arbitrators would be given a set of principles to follow when making a decision, much like those that underpin arbitration in the context of gas pipeline third-party access but would also have considerable discretion in their application. Meanwhile, MCs and DNSPs would have the flexibility to negotiate access for whatever streams of data are most useful in that context.

As in the case of third-party access to gas infrastructure, it may be desirable to separate different streams of data access into different categories with different underpinning principles. For example, for the most basic data streams (those that might be considered the minimum contents), the backstop arbitration could be conducted by the AER itself with reference to tightly defined pricing guidelines (as it does in the case of "stronger regulation" in gas infrastructure). For more discretionary data streams, it may be more flexible to allow for third-party arbitration under more general principles.[29]

This option likely would not reduce the costs of negotiation or the costs of managing relationships with many different MCs, but it would improve the status quo by tying MCs to pre-defined principles of cost reflectivity and the outcomes of a notionally competitive market. For this option to work, DNSPs and MCs would presumably need to negotiate a blanket agreement unrelated to any one data request, on which they could fall back if an MC exerts market power in a narrower context.

This option also avoids some of the unneeded costs of the DCC option and the Minimum Content options, because the data would not be provided that is not requested by DNSPs.

[29] In some sense this is similar to how "full regulation" currently works for gas pipelines, whereby a reference tariff is defined for "reference services", but not for non-reference services.

We compare this option specifically against the comparison criteria below.

Table 5.4: Assessment – Negotiate-Arbitrate

Criteria	Comment
Provision of data access	Likely if "strong regulation" principles are instilled for basic data access, but otherwise unclear.
Cost/ease of implementation	Relatively easy. Framework exists in other industries.
Ongoing costs	Low. Though arbitration can be expensive.
Ease of price formation	Unclear, still relies on negotiation as in status quo.
Flexibility to new use cases	High.
Potential to combine with other options	Could underpin an exchange architecture.
Possibility of partial implementation	No.

Qualifications, assumptions, and limiting conditions

This report is for the exclusive use of the NERA Economic Consulting client named herein. There are no third-party beneficiaries with respect to this report, and NERA Economic Consulting does not accept any liability to any third party.

Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been independently verified, unless otherwise expressly indicated. Public information and industry and statistical data are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information. The findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties. NERA Economic Consulting accepts no responsibility for actual results or future events.

The opinions expressed in this report are valid only for the purpose stated herein and as of the date of this report. No obligation is assumed to revise this report to reflect changes, events, or conditions, which occur subsequent to the date hereof.

All decisions in connection with the implementation or use of advice or recommendations contained in this report are the sole responsibility of the client. This report does not represent investment advice nor does it provide an opinion regarding the fairness of any transaction to any and all parties. In addition, this report does not represent legal, medical, accounting, safety, or other specialized advice. For any such advice, NERA Economic Consulting recommends seeking and obtaining advice from a qualified professional.

© NERA Economic Consulting

NERA
ECONOMIC CONSULTING

NERA Economic Consulting
One International Towers
100 Barangaroo Avenue
Sydney NSW, Australia 2000
+61 2 8864 6535
www.nera.com

NERA Australia Pty Ltd, ABN 34 092 959 665