ERANZ SUBMISSION TO THE ELECTRICITY AUTHORITY CONSULTATION PAPER ON MULTIPLE TRADING RELATIONSHIPS

How can consumers choose multiple electricity service providers?

27 February 2018

Electricity Retailers' Association of New Zealand
PO Box 25596 | Featherston Street | Wellington 6146

ERANZ welcomes the opportunity to comment on the Multiple Trading Relationships (MTR) consultation paper. We appreciate the Electricity Authority (EA) seeking input from industry before assessing whether change is warranted. We are pleased the Authority is thinking about data issues generally as the sector changes with emerging technologies.

ERANZ was established in August 2015 to promote and enhance an open and competitive electricity market that delivers value to New Zealand electricity consumers. ERANZ represents Genesis Energy, Contact Energy, Mercury, Meridian Energy, Trustpower, Nova Energy, Pulse Energy, Prime Energy, Powershop, Black Box Power, Bosco, Energy Online, Just Energy, King Country Energy, Globug, Grey Power Electricity, Electra Energy, Powershop, Flick Electric Co., Wise Pre-pay and Tiny Mighty Power, equating to around 99% of the market by ICP count.

ERANZ submission comprises of six sections:

1. Executive Summary
2. Access to Data – reframing the issues
3. Multiple Trading Relationships – Practical considerations
4. An Eye to the Future
5. Responses to the specific questions contained in consultation paper
6. Appendices with supporting documentation

1. Executive Summary

1.1. ERANZ supports initiatives that have long-term benefits for end consumers. Part of the value that retailers provide is understanding the needs of their customers and creating services in response to those needs. Consumer impact must be at the forefront of thinking when considering the costs, risks and unintended consequences of changes required to enable innovation.

1.2. The MTR paper conflates two distinct issues:

- third party access to consumers electricity consumption data; and
- changes to the current rules, processes and systems required to allow more than one trader at an ICP.

ERANZ believes the MTR project should focus on the latter - changes to rules and processes.

1.3. Access to data is a much wider issue that touches not just on electricity industry issues, but also wider societal issues of trust and privacy. As such, access to data issues need to be considered beyond the context of MTR. We suggest that access to data should be the focus of a separate issues paper and seek to engage with others outside of the sector, such as the Office of the Privacy Commissioner. There are international and national developments regarding data and privacy that need to be considered.

1.4. We believe the barriers attributed to access to data in the MTR paper are overstated. A customer can access their own data at no cost. A customer can pass that data on to a third party. If a third party has the customer's consent, they can obtain a customer's electricity consumption data on their behalf. Different parties have different rights and interests to customer consumption data based on their contractual relationship with the customer.

1.5. As a principle, ERANZ supports market-based arrangements for the collection and sharing of data to ensure a level playing field for all potential business applications, both current and future. ERANZ is of the view that there are currently no barriers to any interested parties reaching appropriate contractual or commercial arrangements for the sharing of consumption data, provided that the rights to privacy of individual customers are reconciled.

1.6. There are a number of practical issues that would need to be considered to enable MTR, including:

- responsibility for vulnerable and medically dependent customers;
- disconnection;
- notification of outages; and
- the customer compensation scheme.

Each of these issues is complex and of significant importance to maintaining the integrity of the system for customers.

1.7. We propose that a thorough cost benefit analysis (CBA) needs to be applied to this MTR proposal to determine if the costs and risks of implementation outweigh the benefits to customers. We note that the Australian Market Commission (AEMC) investigated MTR from 2014-2016 and concluded it was unlikely to deliver material benefits for most customers, and therefore decided not to make rule changes.

1.8. It is possible that much of the functionality of the existing metering technology will be able to be replicated by a variety of emerging technologies, therefore a singular regulatory focus on issues pertaining to the relationship at the meter will be increasingly superseded via technological evolution.

2. Access to Data – reframing the issues

2.1. Access to Data – the fundamentals

2.1.1. First, ERANZ wants to state clearly that we support the development of processes to enable consumption data to be shared in an informed and confident way.

2.1.2. Secondly, all customers have the right and ability to access their own data at no cost. The way to do that differs between retailers, but most customers can download their data through a digital portal, therefore no interaction with their retailer may even be required. A customer can share their own data with whomever they choose.

2.1.3. Third, there is a clear distinction between personally identifiable data and anonymised data, in both systems and processes that are required to facilitate the sharing of either. As an industry we need to be clear about the form of data to which we are referring and what form of data is required to serve the purpose for which it is needed. Whomever is in the role of gathering, sharing, using or storing personally identifiable data (i.e. consumption data at ICP level), needs to be satisfied that consent was obtained from the customer or the other legal considerations involved.

2.1.4. Fourth, different parties have different rights and interests in consumption data, including customers. These rights and interests are determined by legislation, regulation, and contract. Retailers receive requests from many different parties; from internal to the electricity sector, but also external to it. Different considerations need to be applied depending on who is requesting the data and what is being requested (see the third point above).

2.1.5. Fifth, data has value. Many companies now trade services for data, such as Facebook. There are commercial and intellectual property implications that cannot be overlooked or downplayed. The tools to collect, store, secure, use, share, analyse, cleanse, and destroy data all require investment and resource. The value in data is changing due to technological advances, therefore the conversation about the systems and processes for data-sharing, and how costs should be allocated, is timely.

2.1.6. Finally, sixth, the discussion about access to data in New Zealand has been rapidly evolving over the last twelve months and will continue to do so. This is not a static issue. Retailers, as well as others in the sector, have been learning and adapting their processes and systems to adopt best practice and meet the needs of those requesting the data as much as possible, as well as meeting the needs of their customers.

2.2. Means, motives and barriers - misrepresentation of the issues at play

2.2.1. ERANZ does not accept the view put forward in the EA's MTR consultation paper that there are material constraints to accessing consumption data because of retailer practices.

2.2.2. The MTR issues paper identifies the barriers to enabling multiple trading relationships as:

(a) Current industry rules (described as a 'hard constraint'); and,
(b) systems and processes that limit a customer's ability to share their consumption data with electricity service providers (described as a 'soft' constraint).

2.2.3. The paper, in several parts, has made inferences about the means and motives of retailers to use these hard and soft barriers to limit competition. The consultation paper states that retailers are incentivised to use these barriers to their advantage:

> *"Under the current arrangements, a retailer at an ICP has the ability and incentive to impair or prevent other parties from forming a contemporaneous relationship with a consumer at the ICP. The ability to do this is provided through market rules which impose restrictions (constraints) on consumers establishing multiple trading relationships at an ICP – the hard constraint. The incentive arises because an incumbent retailer may lose revenue and profits from assisting its customer to obtain competing services on a contemporaneous basis from another provider*[1]*.*
>
> *The soft constraint exists because the retailers have some incentives and ability to delay sharing the data. They have the incentives to do so where prompt access to data will mean they face more competition for their customers. Retailers have the ability to take up to twenty business days to satisfy itself that fulfilling the request would meet its obligations under the Privacy Act. Once the retailer has satisfied itself*

[1] Electricity Authority Consultation Paper: 'Multiple Trading Relationships: How can consumers choose multiple electricity service providers?', Page 20, para 3.45

that the request is legitimate, it has a further 5 business days to fulfil the request. This gives retailers up to 25 business days to fulfil a request[2]*.*

As discussed above, retailers have incentives to provide the data no faster than necessary if the request comes from a competing provider[3]*."*

2.2.4. The paper appears to have been pre-emptive of other EA processes, such as the annual retail data request, which has asked retailers for the same information which would quantify timeframes taken to respond to requests. Assertions have been made about retailer motivations or practices which may not be the case under current practices, or may be based on abnormal circumstances.

2.2.5. The paper suggests that the need to address 'hard constraints' - that is rule changes and changes to systems and processes - would be negated or significantly reduced simply by addressing the access to data issue - the 'soft' barriers.

"In contrast, however, it's unlikely that many, if any, of these changes to industry rules and processes would be needed if we focused on removing retailers' incentives to inhibit consumers establishing multiple trading relationships[4]*."*

To improve competition and provide long-term benefits to consumers it may not be necessary to address both the ability and incentive constraints—potentially *only one of these factors has to be addressed.*

For example, if the incentives on a retailer to influence the format and timeframe (up to 25 business days) in which a third-party provider can access their consumer's data could be removed, then it is likely that the soft constraints identified above could also be lessened or removed. In this case, it may be unnecessary to address the hard constraint.

Accordingly, the degree to which industry rules and processes need to be changed, if at all, will depend on how these constraints are addressed."[5]

2.2.6. We contend the paper is weak and displays a lack of nuance and understanding of the actual circumstances surrounding the practical, contractual and legislative parameters that retailers operate under.

2.3. A framework for safe information sharing

2.3.1. The impression given from the MTR paper is that the "soft" barriers are an inconvenience and can be "removed". We are concerned that the dynamics of ensuring data is shared in an informed and confident way are misunderstood by the Electricity Authority. We do not see the Privacy Act as a barrier, but rather a consideration that anyone in the position of collecting, storing or using personally identifiable data should be aware and factor in to their processes.

[2] Ibid, Para 3.49
[3] Ibid, Para 3.50
[4] EA MTR consultation paper, page v., last para of Executive Summary
[5] EA MTR consultation paper, page 20., para 3.51 - 3.53

2.3.2. Let us look to the words of the Privacy Commissioner on this point. The Commissioner expressed his concerns with the electricity industry in a public statement issued in May 2017[6] on the bulk disclosure of smart meter data (Appendix A).

> *"Bulk disclosure of ICP-level smart meter data risks infringing individual privacy, and damaging trust in how the sector handles customer data."*

Concluding:

> *"A data breach or demonstrated misuse of such detailed and potentially sensitive data could lead to serious consequences for the individuals affected and retailer reputation".*

2.3.3. The Commissioner's letter recommended that greater aggregation of data could be used to allow the benefits of smart meter data whilst safeguarding the privacy of individuals.

> *"Aggregating the half-hourly data by households would be one way of alleviating the privacy concerns identified by retailers, allowing for provision of rich data while still protecting electricity consumers' reasonable expectations of privacy. Other solutions could be discussed with retailers and metering companies. If a satisfactory resolution can be arrived at that allows for provision of rich data while still protecting electricity consumers' reasonable expectations of privacy, it is unlikely I would need to consider taking more formal steps in relation to smart meters."*

2.3.4. Retailers must manage requests from many different sources, including those outside the sector. This includes the Police and other government agencies. If there are not checks and balances to ensure customer consent for sharing of their data retailers can face very real consequences. Currently a case is before the Supreme Court regarding a customer who did not agree with his information being shared with the Police under a Request for Information procedure[7]. Another was before the Privacy Commissioner when a retailer failed to verify a customer's identity before establishing an account and passing on details to a third party. There was a concern that agencies were not taking steps which were reasonable in the circumstances to ensure personal information, including account information, was accurate before use. The case also reinforced the importance to take reasonable steps to verify the identity of any person requesting access to their personal information.

2.4. Assumptions and assertions

We explore some of the assertions in the paper around data access which we believe are weak, as it is important to test assumptions:

- Data portability – access to consumption data;
- Development of processes to share consumption data in a safe and confident way;
- Time taken to fulfil requests from third parties for customer data (personal and/or anonymised);
- The Privacy Act is not a barrier to information sharing, but it must be a consideration for anyone accessing consumption data.

[6] Office of the Privacy Commissioner: Public Statement about bulk disclosure of smart meter data, 26 May 2017

[7] Refer Alsford v the Queen (SC 12/2016 [2017] NZSC42)

2.4.1. Data portability – access to consumption data

2.4.1.1. The papers premise that access to data is a barrier is flawed by the simple fact that customers can access their own data and are then able to provide their data directly with whomever they choose.

2.4.1.2. We accept there are issues around file formats, and we support efforts to standardise and smooth those processes. We are aware there is a process underway in the Standard Data Formats Group to improve the EIEPs in this respect.

2.4.1.3. Retailers have different systems, but most customers can either download a file of their own consumption data directly via web-portals, thereby no interaction with their retailer may even be required. Other retailers may have a manual process and will send a customer their data file upon request by phone, email, or via their website. Customers are then not limited in sharing these files with whomever they like.

2.4.1.4. Customers can also authorise others to access their consumption data on their behalf. In this case, different retailers have developed different verification processes and systems to be able to share the customer's data in a trusted and confident way.

2.4.1.5. Retailers cannot take this verification lightly. As referenced above, these issues are live before the courts and the Office of the Privacy Commissioner to ensure that the verification processes are robust and credible. Naturally, retailers are cognisant that these processes should be reasonable and sufficient to discharge the retailer of their duties to the customer and not be overly burdensome for the agent. As the case with the Privacy Commissioner, simply providing "commonly known" information (such as name, date of birth and address) to verify an identity was not deemed to be "sufficiently reasonable steps" for the purposes of IPP 8. Further steps were required, such as a verification code, or other identity verification steps, allowing the retailer to accurately establish a connection between the requestor and the personal information being requested.

2.4.1.6. Retailers have developed verification tools to ease the process and allow the authorised third party to obtain the customer data. Some retailers have developed separate portals to deal with authorised agent requests for customer data (i.e. the EIEP 13C process). Here, the requestor gets direct consent from the customer and submits their request with that consent to the retailer. An ERANZ survey of our members found routine third-party data requests were typically processed in five days. Retailers continue to refine and develop these processes.

2.4.2. Development of processes to share consumption data in a safe and confident way

2.4.2.1. 2017 saw a marked change in the nature of data requests, in terms of frequency and quantum. This prompted ERANZ to set up an Access to Data Working Group which focuses on issues involving the use, security and sharing of data with a view to improving retailer and sector-wide understanding and processes. The group has engaged with key stakeholders such as the Office of the Privacy Commissioner (OPC), Data Futures Partnership, MBIE, as well as other sectors dealing with 'Big Data' issues, and some EDBs. The issues around Access to Data

are ones that ERANZ and members have been thoughtfully considering and engaging in over the past twelve months and continue to do so.

2.4.2.2. This has already resulted in:

(i) **a standardised data request template** (Appendix B) – developed with involvement from EDBs and the OPC, which:

- standardises the way in which networks and others make ad hoc customer data requests from retailers to ensure all necessary considerations have been made;
- assists retailers to assess in a consistent fashion whether a request is reasonable and how to facilitate the sharing of information in a way that complies with the Privacy Act principles and other legal obligations; and,
- streamlines the process with the intention that it facilitate a smooth and quicker process for all involved.

We are aware that this template is already in use between retailers and EDBs.

(ii) a set of **Core Data Values** to provide transparency for customers about what data is gathered, used and shared and how that is managed (Appendix C). This was developed because it became apparent that a customer-centric discussion around consumption data needed to start at the very basics – to clearly explain in a transparent way what it is, why it is gathered, what the uses might be and how retailers are managing some of the risks. This work was heavily influenced by discussions with the Data Futures Partnership which developed Guidelines for Trusted Data Use[8].

The core data values are:

- **Value 1**: Privacy will be an objective at the highest levels within ERANZ members' organisations, and responsibilities for securing that objective will be clearly identified by each member.
- **Value 2**: Customer data will be managed in a way, as much as possible, that is open and transparent to customers so that they know that it is being collected, how it will be used, what the value is to them in sharing their data, and what their choices are in respect of their data.
- **Value 3**: The primary purpose for the use of the data is to supply customers with electricity. Important secondary purposes may be to provide a benefit to customers, improving electricity retailer service or the services of the electricity sector as a whole.
- **Value 4**: Before disclosing customer information, members will consider whether the purpose of disclosure can be satisfied by disclosing anonymised and aggregated data so as not to reveal identifiable personal information.

[8] Data Futures Partnership- A Path to Social Licence: Guidelines for Trusted Data Use, 2017: https://trusteddata.co.nz/organisations/

- **Value 5**: Clear disclosures about who will or may have access to identifiable customer data will be made, as much as possible.
- **Value 6**: Customer data will be stored securely.
- **Value 7**: A comprehensive response programme will be maintained and if a data incident occurs, prompt steps will be taken to mitigate the impact of the incident and, where unauthorised access to personal information is likely to have occurred, consider notifying impacted customers and relevant authorities.

These set the minimum standards that ERANZ members have agreed to promote. We would encourage the EA to consider that these values should be incorporated across the sector as basic principles.

2.4.3. Time taken to fulfil requests from third parties for customer data (personal and/or anonymised)

2.4.3.1. Provision of data to third parties has been something that has been adapted into process via the Use of Systems Agreements, the Code, and the EA's Retailer Data format work, court orders or warrants, requests under specific legislation, or requests to release information backed up by a statutory power to require disclosure.

2.4.3.2. EDBs can request customer data through their contracts with retailers for both billing and reconciliation purposes, and for network planning purposes. Requests may also come from entities such as the EA, New Zealand Police, Ministry of Social Development and others.

2.4.3.3. Electricity retailers do not automatically release customer information when they receive a request. For each request received, electricity retailers must assess it to see whether it is consistent with their terms and conditions with the customer, the retailer's policies and contractual obligations, and the Privacy Act,

2.4.3.4. The process to release consumption data can take time, as it is not always a routine request, clarification or verification may be necessary, the retailer may not actually gather the data being requested from the MEP, and it may be a manual rather than an automatic process. We stress the difference between different types of data requests. If the request is for data that can and should be anonymised, then that is a process in itself, which may or may not be contracted out to a third party depending on the retailer or the nature of the request.

2.4.3.5. The inference in the MTR paper that any delay is due to an anti-competitive motive is not justified without further explanation or investigation as to the materiality of the issue. A recent ERANZ survey of our members indicates that data requests from third parties are typically fulfilled in 5 working days. The EA has recently requested data request timeframe information from retailers as part of its annual retail data request. We hope that the information received by the EA will be cross-referenced into this consultation process.

2.4.3.6. We are certainly aware of instances where requests have taken longer to fulfil by some retailers. However, we are also aware that these are instances are when

third party requests may have been novel and not followed previously established processes; the request may have been for data that the retailer did not collect itself, therefore interaction with the MEP was necessary; the request may have lacked sufficient detail for a retailer to make an assessment as to whether the form of data was necessary to meet the needs of the requestor (e.g. whether anonymised data was sufficient); whether customers had provided consent; whether the request was valid under the terms and conditions the retailer has with the customer; or whether reasonable costs were incurred for the handling process.

2.4.3.7. We believe it is these atypical cases that have been reported to the EA as examples of retailers 'implementing barriers', but which we consider are not necessarily reflective of the general situation of what is, for most requests, an established and well-trodden path. We also note that the situation as it was twelve months ago, is not the same as it is now. The development of the standard data request template was designed to ask a number of the basic questions upfront in order to remove a back and forth of emails to gather that information. It has been reported to ERANZ that the template is helping to smooth the process and improve understanding of some of the basic points that need to be covered.

2.4.4. The Privacy Act is not a barrier to information sharing, but it must be a consideration for anyone accessing consumption data

2.4.4.1. The MTR paper suggests 'removing the retailer incentive' as way of removing barriers to MTR. What this means is not detailed. The paper may have been intending to note that the obligation comes from the relationship between the retailer and the customer, and the terms and conditions of that relationship. Therefore, it may be that when/if other parties form a relationship with the customer (via, for example MTR) then that relationship will allow a different form of data collection, and corresponding Privacy Act obligations.

2.4.4.2. This would necessitate renegotiation of existing commercial agreements retailers have with their consumers and the MEP. We stress that Privacy Act obligations are universal regardless of which party is mandated with overseeing third party access to customer's data. Therefore, privacy and trust considerations should not be seen as a barrier, but rather a consideration in the process.

2.4.4.3. The Privacy Act contains twelve privacy principles. Through work with legal and privacy experts, ERANZ developed its Core Data Values, which were based predominantly on the Privacy Principles that are most relevant to consumption data. These are of relevance to anyone in the sector that is dealing with personal information (i.e. ICP level consumption data):

- Principle One - Purpose for collection of personal information: Personal information cannot be collected by any agency unless it is collected for a lawful purpose connected with the function of that agency and is necessary for that purpose.
- Principle Five - Storage and security of personal information: Steps must be taken to prevent data being accessed, used, or disclosed.

- Principle Eleven - Limits on disclosure of personal information: Data collected cannot be used for purposes other those for which it was collected.

2.4.4.4. Retailers are mindful that they have some consumers who do not want smart meters and who do not want their data to be shared beyond what is strictly necessary. We are also mindful that there are some consumers who are perfectly happy for their data to be widely shared. Systems and processes must be established so that either consumer has the requisite reasonable information, control and choice to allow that to happen.

2.4.4.5. In this wider context it is essential that the sector has a robust and mature discussion about consumption data, so that we can apply best practice in the early development of the uses of this data and we bring consumers along with us.

2.4.4.6. In his 2017 briefing to the incoming minister, the Privacy Commissioner noted:

"The operation of an innovative and vigorous economy and an efficient government depends on confidence in organisations' ability to treat personal information appropriately. Companies and government agencies have found that inadequate attention to privacy of customer and client data can erode trust and confidence, impede the delivery of essential public services, and wipe out shareholder value."[9]

2.4.4.6 In a recent blog post, the Privacy Commissioner, pushes back against the view that privacy obligations are a barrier:

"Privacy is sometimes wrongly seen as antithetical to information sharing. It is not. Privacy and information sharing are different sides of the same coin. Our Privacy Act could just have easily and just as accurately been called the Information Sharing Act. Rather than arbitrarily limit what information can be shared, with whom, and for what purposes, the Privacy Act provides a framework for safe information sharing."[10]

2.5. Big Data – balancing opportunities and responsibilities

2.5.1. The great promise of so-called "Big Data" technologies is more efficient allocation of resources, more micro segmentation of the population to better target goods and services, and improved monitoring and evaluation of the efficacy of those allocations. There are many beneficial consumer outcomes that can come from the confluence of machine learning with Big Data, and more.

2.5.2. The increasing sophistication of data-analytics means that granular consumption data is becoming increasingly valuable and sought after. Electricity consumption data can be used

[9] Briefing to the incoming minister of justice: Hon Andrew Little, from the Office of the Privacy Commissioner, October 2017

[10] Office of the Privacy Commissioner Blog Post: 'Information sharing: Learning from overseas experience', John Edwards, 30 January 2018

to identify subsets of consumers of particular interest or value to retailers and third parties. For example, consumers with consumption patterns complementary to certain products or service offerings, such as solar and battery providers, or suitability for participation in demand side initiatives.

2.5.3. Ready access to consumption data for large numbers of consumers on an ongoing basis will be highly valuable to third parties as a marketing tool. However, the requirement for consumer consent can make obtaining large data-sets time-consuming and costly. Responsible and ethical collection, use and management of their data are matters of increasing interest for consumers across many sectors, and electricity is no different.

2.5.4. ERANZ acknowledges this consumption data is an important resource for individual consumers and for the electricity sector and has value in a wide range of applications including for network planning and enabling new forms of consumer participation in the market. However, to maintain consumer trust and confidence in the electricity industry it is essential that any use of a consumer's private data is made with their knowledge and consent, and only used for the purposes authorised by the consumer.

2.5.5. A survey undertaken in 2016 by the New Zealand Privacy Commission[11] showed that:

- two-thirds (65%) of New Zealanders were concerned about their data privacy
- 58% were very concerned with businesses sharing their personal information with other businesses without their permission
- 37% do not feel in control of how businesses use their information
- nearly half (46%) have become 'more concerned' about privacy issues over the last few years. The proportion saying that they feel more concerned has risen in three consecutive polls
- the majority wanted to be able to opt-out of sharing data and wanted strict controls on access.

2.6. The international trends in data sharing and security

2.6.1. Information privacy and data protection is a dynamic field that has developed rapidly against a background of technology changes such as cloud computing and data analytics; social networking; cross-border data transfers; the Internet of Things; artificial intelligence and robotics.

2.6.2. Data privacy is an area of increasing academic research internationally. Researchers are raising concerns about privacy and data collection and aggregation[12]. The conclusions are that more safeguards are required, not less.

> *"We argue that this line—and the attendant standard practices—should shift. A spectrum of choices for the line exist, with the endpoints completely prioritizing data access or privacy, and current standards lean too far towards data access."*

[11] Privacy Concerns and Sharing Data survey commissioned by the Office of the Privacy Commissioner and conducted by UMR Research from 30 March to 18 April 2016

[12] Narayanan, Arvind, Joanna Huey and Edward W. Felten: 'A precautionary approach to big data privacy', March 19, 2015

2.6.3. The European Union and Australia have recently moved to grant more protections for consumers of their data. For example, the European Union's General Data Protection Regulation (GDPR)[13] brings a new set of "digital rights" for EU citizens in an age when the economic value of personal data is increasing in the digital economy. GDPR standards lift the baseline internationally in response to the challenges to consumers and data protection in today's global digital economy.

2.6.4. In his briefing to the incoming minister the Privacy Commissioner recommended some reform of the Privacy Act in order to bring it in line with overseas developments:

> *"There is an urgent need for privacy law reform. All key international instruments on information privacy on which domestic privacy laws are based have been reviewed or updated in the last decade including, most relevantly for NZ, those of the OECD (2013), EU (2016) and APEC (2016). Most existing privacy laws around the world have been reformed in the last 3 years or are currently being reviewed and updated."*[14]

2.6.5. A review of the operation of the Act was undertaken in 2016 and that report was presented to Parliament in January 2017. It is important for the EA and the sector to be aware of these wider discussions and considerations so that we are applying best practice and knowledge for the long-term benefit of consumers.

2.7. Data has value

2.7.1. The provision of data to retailers from metering equipment providers (MEPs) is subject to clear obligations under the Code and is governed by contract under which services are remunerated. At present, retailers contract with MEPs for the installation, use and maintenance of the meter at a property. These arrangements ensure that the costs of the MEP in providing data are recovered and that metering services are sustainable into the future, including providing a basis for on-going investment and innovation in the development of new services. Retailers have invested in systems and resources to store, secure, cleanse, analyse and format the data they receive from MEPs.

2.7.2. As a principle, ERANZ supports cost reflective and market-based arrangements for the collection and sharing of data to ensure a level playing field for all potential business applications, both current and into the future. This position aligns with that outlined by the EA in their recent letter to the Distribution Pricing Reform Technical Implementation Working Group (TIWG)[15].

> *"Our view is data is owned by the consumer, and the consumer permits participants to collect and use their data through their agreement with the participant. Where the consumer has agreed, the Code currently permits participants to share consumer data. The Code requires contracts to be in place between sharing participants, allowing the participants that have invested in gathering and storing data to reach commercial agreements with other participants for access to this data. These*

[13] https://www.eugdpr.org/
[14] Ibid at 9.
[15] Letter from Carl Hansen, EA Chief Executive, 'Issues to refer to the SDFG's 31 January Meeting', 19 February 2018.

commercial agreements are for the cost of gathering, storing and accessing the data, not for the data itself, which is owned by the consumer."

2.7.3. We need to be mindful of the hard-fought commercial value retailers have invested in acquiring and keeping customers, and the reputational risks for retailers if a data breach were to occur. We reference the cases before the Supreme Court and the Privacy Commissioner to exemplify the fact that these privacy and trust concerns are real and relevant.

2.7.4. Many companies now trade services for data, such as Facebook. There are commercial and intellectual property implications that cannot be overlooked or downplayed. The tools to collect, store, secure, use, share, analyse, cleanse, and destroy data all require investment and come at a cost. The value in data is changing due to technological advances, therefore the conversation about the systems and processes for data, and where costs are allocated, is timely.

3. MTR: Practical and technical issues that will require further investigation

3.1 Beyond the access to data issues, there are several practical and technical facets which will need to be considered in the context of enabling MTR, such as:

- Responsibility for vulnerable and medically dependent customers
- Disconnection process
- Notification of outages
- Customer compensation scheme
- Emergency management
- Customer complaints
- Cost sharing of metering and data handling
- Responsibility for site safety

3.2 Each of these aspects are complex and a detailed investigation should take place before any changes are enacted. ERANZ is not engaged at an operational level, and as such at this stage we cannot provide a detailed assessment of the technical and practical challenges presented by MTR. Where relevant, our members who have specific interests in the various detailed matters will respond to those directly.

3.3 The consultation paper suggests the next step for MTR will be to undertake a more detailed investigation:

> *"If comments suggest there are benefits from further investigation, the Authority is likely to request the Innovation and Participation Advisory Group to consider how to make multiple trading relationships easier and whether doing so would deliver long term benefits to consumers."*[16]

The standard way to achieve satisfaction that costs (that will be recovered from consumers) is in the long-term benefit of consumers is to apply a cost-benefit analysis (CBA). CBA should be included as part of a detailed investigation.

[16] EA MTR consultation paper, page 7., para.1.4

3.4 We note that the Australian Market Commission (AEMC) recently investigated MTR and concluded it was unlikely to deliver material benefits for most consumers but would likely impose significant costs.[17]

4. An eye to the future

4.1 Unlike overseas jurisdictions, the New Zealand electricity sector has been notable in rolling out smart metering technologies without regulatory mandate. While these technologies enable more timely collection and remote reporting of electricity consumption data without estimation, they involve inherent constraints. Foremost is the fact that smart meters collect data at ICP level, not consumer level. As such, there is a possibility that the meter may be leapfrogged by emerging technologies that will enable real-time, consumer-level electricity consumption to be accurately estimated. These technologies could be as simple as being able to remotely identify what internet-connected devices a consumer is using at any given time, given the known power consumption characteristics of a given device. Hence, competition to understand consumers' behaviours and preferences may advance through technologies other than smart metering.

4.2 The MTR paper has focused on the meter, and access to data from that meter, as the key to enabling MTR. However, questions around access to smart meter data, and whether it should be open access to enable innovation may likely become moot as and when alternative technologies give rise to superior data. Regulatory treatment should allow for the possibility of this longer-term outcome and ensure regulation does not impede it – provided that is in the long-term interests of consumers.

4.3 ERANZ is supportive of a broader debate on access to data in the context of what is best for the customer. There are a number of issues that need to be addressed into the future, including the ability to gather and use half hourly consumption data. Data from distributed energy sources or "behind the meter" sources, such as solar, batteries, electric vehicles, energy monitoring devices and more are likely to be increasingly part of the mix. We must be cognisant of the balance of open data access with the need to drive investment and innovation in data-driven capabilities, which may have proprietary rights over the data, and may also be of great benefit to the customer. This all reiterates the need for the sector, and the regulator, to be clear about what data is important for what reasons, what level of access is necessary, and under what circumstances. ERANZ looks forward to continuing to be involved in these discussions.

Thank you for the consideration of this submission. We are happy to discuss any parts of this submission in more detail if required. If you have any queries, please contact Jenny Cameron: jenny.cameron@eranz.org.nz

[17] AEMC, Final Rule Determination: National Electricity Amendment (Multiple Trading Relationships) Rule 2016, National Energy Retail Amendment (Multiple Trading Relationships) Rule 2016, 25 February 2016

Yours sincerely

Jenny Cameron
Chief Executive
Electricity Retailers' Association of New Zealand

5. Responses to the specific questions contained in consultation paper

Q1: How material are the constraints to consumers establishing multiple trading relationships at a single connection identified above?	The EA identifies the barriers to establishing multiple trading relationships as: 1. Current industry rules 2. The consumer's ability to share their consumption data with third parties The EA paper posits access to data as the predominant barrier and suggests the need for changes to exiting industry rules would be negated or significantly reduced simply by mitigating barriers to accessing to data. Access to data is not a material barrier. As detailed in the body of our submission, there is nothing preventing a consumer sharing their consumption data and it is easy to do so. A third party can also obtain a consumer's electricity data from the consumers retailer, typically within five-days, once they have that consumers consent.
Q2: Are there other constraints that prevent multiple trading relationships from efficiently occurring? If so, please describe them.	A potential barrier to efficient MTR uptake not covered in the paper is the variance in use of system agreements and tariff structures between the 29 different EDBs. Whilst not preventing MTR, the effort required to assess the impact of regional variances in tariff structures and contractual arrangements may delay niche energy service providers from expanding their service offerings to consumers in other regions, particularly those with lower populations. Another potential barrier is the increased complexity for consumers which may serve to reduce wide-spread consumer appeal for engaging multiple energy service providers. We are unaware of any consumer research undertaken in New Zealand on MTR. However, Australian Market Commission (AEMC) has recently completed a detailed investigation of MTR in which they reported: *'Stakeholders generally considered that while a small subset of active and engaged customers may be interested in transacting with multiple FRMPs at a premises, the broader market was not ready for or demanding these kinds of more complex retail arrangements'*[18].
Q3. What do you consider to be the	A potential indirect benefit from MTR in New Zealand is that if MTR resulted in increasing numbers of

[18] Ibid.

benefits of multiple trading relationships?	energy service providers, the mounting volume of new players may provide greater impetus for faster implementation of cost reflective distribution pricing, and greater standardisation of tariffs and use of system agreements across regions. This would serve to reduce overall costs for consumers.
Q4. What other services could be enabled by reducing or removing the barriers to multiple trading relationships?	-
Q5. What changes, if any would be needed to the switching and disconnection/reconnection processes if a consumer were able to have multiple retailers?	ERANZ is not engaged at an operational level, and as such at this stage we cannot provide a detailed assessment of the rules changes required, and technical and practical challenges presented by MTR. Generally, we note that cost benefit analysis (CBA) will need to be applied as part of a detailed investigation into MTR to determine if the costs of resolving the technical, and process and systems issues introduced by MTR outweigh the benefits to consumers.
Q6. What other data exchange processes that have not been identified in this paper need to be changed to accommodate multiple trading relationships?	Please see our response to question 5.
Q7. How could the data exchange processes be modified to accommodate multiple trading relationships?	Please see our response to question 5.
Q8. What other services, if any, would have to share costs between multiple users?	Please see our response to question 5.
Q9. How could the cost of these services be shared amongst multiple users?	Please see our response to question 5.

Q10. Could consumer data be more efficiently shared with service providers that have a legitimate claim for access to their consumer's data? If so, how?	As detailed in our submission, ERANZ view is that that the existing processes and systems allow for the provision of data.
Q11. How much value is there in making it easier for appropriately authorised firms to access information such as a consumer's tariff structure, the smart meter functionality that is used by the consumer's MEP, a consumer's controllable appliances?	Please see our response to question 5.
Q12. Are there other industry participants that may need to amend their systems to operate in an environment with multiple trading relationships?	Please see our response to question 5.
Q13. What are the costs of the above changes recognised in questions 10-13?	As a principle, ERANZ supports cost reflective and market-based arrangements for the collection and sharing of data to ensure a level playing field for all potential business applications, both current and future. The provision of data to retailers from MEPs is subject to clear obligations under the Code. At present, retailers contract with MEPs for the installation, use and maintenance of the meter at a property. These arrangements ensure that the costs of the MEP in providing the data are recovered and that metering services are sustainable into the future, including providing a basis for on-going investment and innovation in the development of new services.
Q14. What other obligations need	Please see our response to question 5.

to change if multiple traders can serve an ICP?	
Q15. How could the obligations discussed above be amended to accommodate multiple traders at an ICP?	Please see our response to question 5.
Q16. What costs would be involved in amending consumer-related responsibilities to accommodate multiple traders at an ICP?	Please see our response to question 5.
Q17. What additional matters would need to be considered if we were to introduce multiple trading relationships? What amendments would need to be made to the Code to facilitate multiple trading relationships?	Please see our response to question 5.
Q18. What is the cost of the changes needed to enable multiple trading relationships?	Please see our response to question 5.

6. Appendices with supporting documentation

- **Appendix A**: Letter from the Office of the Privacy Commissioner
- **Appendix B**: Data request template
- **Appendix C**: Core Data Values

Appendix A: Letter from the OPC

For public release

26 May 2017

Public statement about bulk disclosure of smart meter data

Under section 13(1)(h) of the Privacy Act 1993, I have the ability to make a public statement about any matter affecting the privacy of an individual or classes of individuals. Smart meters raise potentially complex issues of involuntary collection and device-based surveillance[1] as well as the definition of personal information.[2]

Discussions with sector stakeholders (retailers, metering companies and distributors) between October 2016 and March 2017 have revealed that bulk disclosure of smart meter information is taking place under existing Use of System (UoS) Agreements.

Bulk disclosure of ICP-level smart meter data risks infringing individual privacy, and damaging public trust in how the sector handles customer data.

In order to avoid these risks, New Zealand electricity distributors should, in summary:

- review their privacy statements and consider updating them to include assurances regarding the use of smart meter data;
- review whether the individual household level data currently being provided by retailers could be aggregated and still meet network planning needs;
- ensure that personal information is not collected unnecessarily, or held for longer than necessary; and
- aggregate meter data where individual household level data is not required to meet network planning needs e.g. through amalgamating half-hourly data from small groups of households, or by receiving the half-hourly data at the street level.

Regional retailers and metering companies could also benefit from reviewing their privacy statements and policies around smart meter data to ensure they accurately reflect how they use and disclose customer data.

Background

Between October 2016 and January 2017, my office received enquiries from several

---

[1] Case note on smart meters and personal information: https://privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-251185-2015-nz-privcmr-3-use-of-smart-meters-by-utility-companies/

[2] Advisory opinion issued to the New Zealand Fire Service about what constitutes personal information: https://www.privacy.org.nz/news-and-publications/advisory-opinions/addresses-of-fire-incidents/

electricity retailers expressing concerns about bulk disclosure of detailed smart meter data to electricity distributors for network planning purposes.

Approximately 70% of households in New Zealand currently have smart meters and this is likely to increase to 90% within two years. These smart meters can automatically record and transmit power usage data in half hourly intervals, which can reveal significant detail about a household's movements and patterns. This is in comparison to traditional electricity meters, which tend to be used for monthly or even bi-monthly manual readings of total consumption. In its raw form, the data collected by smart meters is associated with an ICP number that identifies the meter itself, rather than any particular person. However, usage information collected from smart meters can become personal information once it is associated with an account holder. For instance, if a person were to claim to have been in their house at a given time, the meter data could provide evidence to support or disprove that claim.

A University of Auckland academic conducted a review of privacy and technology issues around smart meters and noted "There is general consensus that smart meter data should be managed according to the provisions foreseen for personal data".[3]

In 2011, the Article 29 Working Party, an influential body composed of privacy authorities from European Union member states, released a Working Paper, "Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy". The paper contained eight recommendations setting out an approach that ensured electricity consumers would have the privacy of their data respected without the need to take any specific actions (privacy by design). In particular it noted that "research has shown that utilities may not need detailed energy consumption information about individual consumers to perform load balancing functions. To achieve as little personal data flow as possible utilities may use techniques such as anonymisation, pseudonymisation, or data aggregation".

Following that paper, the EU Data Protection Supervisor prepared a 2012 opinion on preparations for the roll-out of smart metering, concluding: "considering the risks to data protection, one of the key pre-conditions for the rollout of smart metering systems is to ensure a high level of protection of personal data."[4]

Discussions with sector stakeholders

In discussions with my staff, retailers said their three key concerns about bulk disclosure of smart meter data were that:

- the disclosures, though made in accordance with UoS Agreements, were excessive as distributors did not appear to need half hourly data at the individual household level in order to do network planning;

---

[3] https://www.cs.auckland.ac.nz/~asghar/papers/asghar12-smartgridsec.pdf

[4] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

- the information may be insecurely stored by the distributors; and
- the distributors may use the data for purposes other than network planning.

The retailers were also concerned that, should the data held by the distributors be used inconsistently with the purpose for collection or inappropriately disclosed, they risked significant loss of customer trust and reputational capital as a result of actions that weren't in their control.

Electricity sector agencies have the following obligations under the Privacy Act 1993:

- principle 1 – individual households' data should only be collected where the collection is necessary for the agency's lawful purposes;
- principle 5 – reasonable steps should be taken to prevent data being accessed, used or disclosed in an unauthorised way; and
- principle 10 – data should not be used for purposes other than that for which it was collected unless an exception applies.

Staff from my office discussed the issue with the Electricity Authority, and were told that it supports efforts to improve security, clarity and transparency around information sharing in the electricity sector, such as by aggregating meter data, so long as this does not increase barriers to new entrants and innovative services or prevent better outcomes for consumers.

Staff from my office also met with representatives from electricity metering and distributing companies to discuss retailers' concerns. A representative from a metering company at these meetings stated that:

- metering companies would be an appropriate medium through which smart meter data could be aggregated and then passed on to distributors; and
- having retailers aggregate the data themselves before passing the information to metering companies could cause data quality issues especially if retailers act independently from one another and therefore do not apply a consistent standard.

Conclusion

A data breach or demonstrated misuse of such detailed and potentially sensitive data could lead to serious consequences for the individuals affected and retailer reputation. For instance, electricity usage tracks closely with house occupancy. If detailed usage information became publicly available it would be possible to track and anticipate a household's movements and use that information in ways the individuals neither expected nor wanted.

In order for distributors to carry out their role efficiently and cost effectively they require a certain level of detail about the network. However, based on my investigations it does not appear to me that they require household level data for network planning. Aggregating the half-hourly data, whether by street or even by small group of houses, would appear to meet both the retailers' concerns and the distributor's needs. If not, the onus would then be on distributors to demonstrate how more detailed information was necessary for them to carry out their functions effectively.

While the privacy interest in a given person's ICP level meter data is, in most circumstances, marginal, the privacy concerns being raised by retailers about bulk disclosure of data are genuine, particularly in the context of significant and growing threats to privacy from Internet of Things devices. Loss of trust from deliberate or accidental disclosure is likely to impact strongly on retailers. Finding a privacy-friendly solution is in the interests of both consumers and businesses.

In order to avoid this risk, while ensuring that retailers and distribution companies can continue to make appropriate use of customer data, I propose to NZ electricity distributors that they should:

- review their privacy statements and consider updating them to include assurances regarding the use of smart meter data;
- review whether the individual household level data currently being provided by retailers could be aggregated and still meet network planning needs;
- ensure that personal information is not collected unnecessarily, or held for longer than necessary; and
- aggregate meter data where individual household level data is not required to meet network planning needs e.g. through amalgamating half-hourly data from small groups of households, or by receiving the half-hourly data at the street level.

Regional retailers and metering companies could also benefit from reviewing their privacy statements and policies around smart meter data to ensure they accurately reflect how they use and disclose customer data.

Aggregating the half-hourly data by households would be one way of alleviating the privacy concerns identified by the retailers, allowing for provision of rich data while still protecting electricity consumers' reasonable expectations of privacy. Other solutions could be discussed with retailers and metering companies. If a satisfactory resolution can be arrived at that allows for provision of rich data while still protecting electricity consumers' reasonable expectations of privacy, it is unlikely I would need to consider taking more formal steps in relation to smart meters.

The retailers also brought to my attention some current research competitions that are using smart meter derived data to encourage innovation in the sector. I encourage and support research and innovation; however companies should be mindful of the ability of researchers or the public to re-identify the data they disclose. Retailers and distributors should also ensure any research initiatives have security protections against inappropriate access to data.

I am grateful to electricity retailers for bringing this matter to my attention and to other sector stakeholders for their cooperation.

Yours sincerely

John Edwards
Privacy Commissioner

Appendix B: Data request template

NETWORK DATA REQUEST
FOR CUSTOMER AND/OR CONSUMPTION DATA ("customer data")

As holders of customer data, **[insert name of Retailer]** is responsible for ensuring that personal information is handled in accordance with the Privacy Act 1993 and our contract with the customer.

This document has been developed in order to ensure, as much as possible, that appropriate considerations have been made to make the process for accessing customer data more streamlined and so that all parties involved are aware of their obligations for the use of customer data.

For the avoidance of doubt, the above processes exclude the standard data sharing EIEP data exchange protocols that are currently in place for (a) network billing and (b) faults and outages, and (c) when a customer requests their own data directly or via an agent.

This document has been developed in accordance with feedback from the Office of the Privacy Commissioner.

THE PROCESS

(a) Please complete this document to make a request for customer data. Please email the form to **[insert name of Retailer contact]**.

(b) Please note that completion and submission of this document will not automatically lead to receipt of the customer data requested. We will also need to consider your request in accordance with our legal obligations, our privacy policy, and the ERANZ Core Data Values.

(c) We will endeavour to respond to your request within **(XX)** working days. If you have questions, please contact **[insert name of Retailer contact]**.

1	**Date**	
2	**Name of party requesting**	
3	**Participant Identifier (if applicable – data will be sent via Registry hub)**	
4	**What customer data is being requested?**	
5	**Is this a once-off request or an ongoing request for the supply of data?** **If it is a request for the ongoing supply of data, please state why that is needed.**	☐ Once-off request ☐ Ongoing request

6	**Please provide the clause number in the relevant Use of Systems Agreement, or any other agreement, under which you are requesting the customer data.**	
7	**Please provide the purpose of the customer data request.**	
8	**Please explain what customer/network/sector/or other benefit the data will help deliver.**	
9	**What is the level of customer data requested? For example:** • **half hourly consumption data, day readings, event/log data?** • **anonymised (at ICP level) or aggregated (at distributor attribute level e.g. GXP, feeder etc)?** **If you require identifiable customer data, please provide reasons why anonymised or aggregated data would not be sufficient to meet your needs.**	
10	**What is the volume of customer data required? For example, the date range for which data is required? The quantum of customers? Geographic size?**	
11	**Please explain who will have access to the customer data?** **What security measures will be implemented to ensure the customer data is not circulated beyond those people?**	
12	**Will the customer data be shared with a 3rd party?** **If yes, please provide reasons and intended use.** **If the data is to be shared with a 3rd party, please provide details on the 3rd party's security measures, including references to non-disclosure agreements (if any).** ***[Please note that consent from retailers may be required for disclosure of customer data to be made to a 3rd party].***	

13	**How will the customer data be stored?** **What security measures will be put in place to ensure the customer data is not used for other than the intended purpose?**	
14	**When and how will the customer data be destroyed after it has been used for the purpose(s) described above?**	
15	**If you intend using the customer data to conduct a trial, survey or similar activity, would you be willing to share the results of that trial, survey or similar activity with [insert retailer name]? If not, please share your reasons.**	

ERANZ CORE DATA VALUES

Responsible and ethical collection, use and management of customer data are matters of increasing interest for customers. Privacy, security, and driving innovation from customer data are all important considerations as technology allows us to better understand use of energy systems and help lower costs for individual consumers.

These Core Data Values are the electricity retailers' commitment to a culture of best practice and enhancing customer confidence and trust in the data practices of ERANZ members.

What do we mean by customer data?

When we talk about customer data, we are referring to data about how much and when electricity is used by a customer linked to their household or business, as well as personal information such as name, address, medical dependent status or other matters, and payment details.

Why are we talking about data?

Smart meters have been rolled out to over 75% of New Zealand connections with an expectation of around 90% coverage within the next few years. Smart meters record the amount of electricity a customer has used on a half-hourly, daily or monthly basis. These meters have meant that readings are no longer estimated but are always based on actual readings. As technology develops, there is the potential for smart meters to help customers better understand what electricity they use or produce or store. It also means other services can develop to improve and manage use of household appliances, and for the whole system to become more efficient as use of electricity, at a more granulated level, becomes more visible.

The New Zealand Data Futures Partnership realised in their work that there was a need to talk about data and data use more so that New Zealanders can understand their feelings and perspectives on data use and to help organisations build and maintain the trust of those whose data they wish to use. This is part of that process for electricity retailers.

Customers' right to their data

Electricity customers in New Zealand can easily get their electricity consumption and connection data from their electricity retailer at any time (and up to four times a year at no charge). To request this information a customer simply needs to contact their retailer by

phone, email or through their website. Customers can also authorise others to access their consumption data on their behalf.

This information can help customers make an informed choice, for example to decide whether they want to switch to another retailer or stay with their current one, or to understand how energy management services could benefit them to reduce costs.

Why is customer data shared?

Electricity retailers also receive requests for customer data from a number of different parties.

Some of that data is shared when required by law or when it is requested by a government agency. Sometimes it is shared during the switching process. Sometimes it is shared to enable research or innovation.

These other parties' requests for and access to customer data are carefully considered to ensure that a customers' privacy rights are protected, as well as enabling the benefits and value from that data to be realised.

Who can request customer data?

Electricity network operators (the lines companies) can request customer data through their contracts with retailers. There is certain data necessary for the management of the use of the electricity distribution network.

Requests may also come from entities such as the Electricity Authority, New Zealand Police, Ministry of Social Development and others. Requests can take the form of court orders or warrants, requests under specific legislation, or requests to release information backed up by a statutory power to require disclosure.

How do retailers handle requests for data?

Electricity retailers do not automatically release customer information when they receive a request. For each request received, electricity retailers will assess it to see whether it is consistent with the Privacy Act, the retailer's policies, the terms and conditions with the customer. They will also consider whether it is reasonable and necessary to meet the stated aims of the party requesting the customer data. If a retailer is not satisfied of all these things, then they may refuse the request or seek further clarification. Not all requests are the same and each one has to be assessed on its own merits.

Principles used in developing the Core Data Values

These values were developed following consultation with the Office of the Privacy Commissioner and the Data Futures Partnership.

The principles used in developing the values were:

- The values should not replicate the obligations that ERANZ members already have under the Privacy Act or the Electricity Industry Participation Code.
- The values will support members' open communication and management of information.
- The values will raise awareness about issues relating to customer data.

The following Core Data Values reflect the approach ERANZ members aim to achieve in their management of customer data and when assessing whether, how and when to use and share data to bring about value and benefit for electricity customers and New Zealand.

The intention is to give customers confidence that their data is secure and being dealt with in an appropriate manner.

The values are applicable to, and intended to be voluntarily adopted by, ERANZ members.

Value 1: Privacy will be an objective at the highest levels within ERANZ members' organisations, and responsibilities for securing that objective will be clearly identified by each member.

Guidance: *ERANZ members should:*

- *Regularly review their customer data practices for compliance with these values.*
- *Ensure that an effective means of addressing customer concerns regarding customer data is available.*
- *Conduct regular training and ongoing awareness activities for relevant employees on their privacy policies and practices.*

Value 2: Customer data will be managed in a way, as much as possible, that is open and transparent to customers so that they know that it is being collected, how it will be used, what the value is to them in sharing their data, and what their choices are in respect of their data.

Guidance: *ERANZ members should:*

- *Collect, use and disclose data consistently with their applicable privacy policies and privacy statements and the Privacy Act 1993.*
- *Notify customers as to the collection, storage and use of their data at pertinent times including if there is a substantial change in a procedure or service that may impact customer data.*
- *Notify customers as to how their customer data will be secured throughout its lifecycle and explain how the customer can exercise their choices regarding customer data.*

Value 3: The primary purpose for the use of the data is to supply customers with electricity. Important secondary purposes may be to provide a benefit to customers, improving electricity retailer service or the services of the electricity sector as a whole.

Guidance: *Disclosures of customer data will be to support these purposes where possible.*

Value 4: Before disclosing customer information, members will consider whether the purpose of disclosure can be satisfied by disclosing anonymised and aggregated data so as not to reveal identifiable personal information.

Guidance: *Aggregated data is a combination of data elements for multiple customers to create a data set that is sufficiently anonymous so that it does not reveal the identity of an individual customer. Anonymized Data is a data set containing individual sets of information where all identifiable characteristics and information, such as name, address, or account number, are removed so that an individual customer cannot reasonably be re-identified based on, for example, usage, rate class, or location.*

Value 5: Clear disclosures about who will or may have access to identifiable customer data will be made, as much as possible.

Guidance*: Members are encouraged to have policies and statements that explain the circumstances under which they will share identifiable customer data, including circumstances where they will disclose data without first obtaining a customer's consent.*

Value 6: Customer data will be stored securely.

Guidance*: ERANZ members will:*

- *Design and organise their security (including encryption) in accordance with recognised industry standards as appropriate to the nature of the data being held.*
- *Ensure any contractors and/or employees responsible for data storage and data security understand the applicable obligations.*

Value 7: A comprehensive response programme will be maintained and if a data incident occurs, prompt steps will be taken to mitigate the impact of the incident and, where unauthorised access to personal information is likely to have occurred, consider notifying impacted customers and relevant authorities.

Guidance:

- *Data security incident response programmes will address the identification, mitigation and resolution of any incident that causes or results in the breach of customer data security.*
- *Members will consider notifying any incident on a case by case basis, taking into account factors such as the likelihood of unauthorised access, how certain the member can be of whose information has been compromised and the risk of harm.*

Application

The values are applicable to, and intended to be voluntarily adopted by, ERANZ members.

These Core Data Values do not affect an ERANZ member's obligations under the law. In particular, these Core Data Values do not:

- limit the principles of the Privacy Act 1993 or an ERANZ member's privacy policies, which ERANZ members will also comply with; or
- restrict any ERANZ member from doing (or not doing) anything it considers necessary for compliance with law or regulatory requirements, including the Privacy Act.