EnergyAustralia
LIGHT THE WAY

7 September 2018

EnergyAustralia Pty Ltd
ABN 99 086 014 968

Level 33
385 Bourke Street
Melbourne Victoria 3000

Phone +61 3 8628 1000
Facsimile +61 3 8628 1050

enq@energyaustralia.com.au
energyaustralia.com.au

Daniel McAuliffe
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

Submitted electronically to: data@treasury.gov.au

Dear Mr McAuliffe

Submission on the Treasury Laws Amendment (Consumer Data Right) Bill 2018

EnergyAustralia is pleased to make this submission on the exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill* 2018 (**Bill**).

EnergyAustralia is one of Australia's largest energy companies, with over 2.6 million household and business customer accounts across NSW, Victoria, Queensland, South Australia and the Australian Capital Territory.

We support transparency in the energy retail market and measures to support customers making informed decisions, such as the creation of the consumer data right. EnergyAustralia believes that the proposed consumer data right is a significant step towards facilitating a more transparent retail energy market that makes it easier for customers to choose the right energy product and service for them.

The introduction of a consumer data right is consistent with the approach that EnergyAustralia has been undertaking with respect to consumer's data. We currently provide our customers with access to their energy information through our online portal, *My Account*. This service allows customers to see their usage data, pay bills, set payment and usage reminders, update account information and seek payment extensions. We have seen a significant growth in use of *My Account* since it was introduced in 2014.

However, we note that the introduction of a consumer data right across the energy sector will have significant implications. At a time when energy affordability is an extreme focus Government must ensure that any regulatory costs are demonstrably outweighed by the resulting benefit.

We therefore urge the Treasury (and other Commonwealth agencies) to take into account the need for comprehensive industry consultation to ensure consistency and efficiency with respect to the scope of data provided, interaction with various regulatory regimes and operational compliance. We consider it imperative that energy sector participants are heavily involved in the process of defining the scope of CDR data and the consumer data rules that will be applied across the energy sector. We welcome the opportunity to make a submission on the Bill, and will continue to be involved throughout the process to ensure that the consumer data right is tailored to meet the specific regulatory challenges and needs of the energy sector.

The enclosed submissions contain our key comments regarding the current Bill.

In summary, we consider that the Bill could be strengthened to ensure there is a robust consultation process, including appropriate cost-benefit analysis, applied throughout all stages of the designation of the relevant sector and development of both the consumer data rules and the data standards. In particular, this consultation process should be designated to ensure that there is sufficient consideration of the unique aspects of the energy industry, such as the range of regulatory frameworks already in place, the availability of data and the interaction of various market participants with consumers and the data that relates to them.

Additionally, in our view, further thought should be given to the proposed scope of CDR consumers that have rights under the Bill as well as the definition of CDR data. In particular, the breadth of the concept of derived data is problematic and we consider that the scope of this concept should be limited. Related to this, we support the ability of data holders to charge a fair and reasonable fee for access to CDR data, particularly in relation to value-added data, to the extent that data is required to be disclosed.

We also have concerns regarding the overlap between the Australian Privacy Principles (**APPs**) and the proposed privacy safeguards, noting that the proposed regime adds a layer of privacy protection for the CDR data of businesses that extends well beyond current statutory regimes.

Finally, we note the significant scope of penalties proposed in the Bill. In our view, these penalties are overly harsh and do not take into account the nature of the obligations that have been proposed or the approach taken in similar contexts, such as equivalent obligations under the *Competition and Consumer Act 2010* (Cth) (**CCA**) and the *Privacy Act 1988* (Cth) (**Privacy Act**).

We appreciate the invitation to provide comments on the Bill and encourage the Treasury, the Department of Energy and Environment, ACCC and OAIC to continue to engage and consult with the energy sector, as well as the relevant energy sector regulatory bodies, on the issues that concern the energy industry. EnergyAustralia looks forward to continuing to work with the Government as discussion regarding the application of the consumer data right in the energy sector evolves.

Yours sincerely

Lee Evans
Policy and Advocacy Lead
EnergyAustralia

The EnergyAustralia submission on the Treasury Laws Amendment (Consumer Data Right) Bill 2018

7 September 2018

1. Designation of energy sector

The Treasury Laws Amendment (Consumer Data Right) Bill 2018 (**Bill**), explanatory memorandum and supporting documentation, including the underlying analysis upon which some policy decisions have been made, appear to be largely focused on the banking sector. In our view, there will need to be significant work and consultation undertaken to adapt them for the energy industry prior to any designation by the Minister.

In particular, significant regulatory, operational and technical hurdles remain to be considered and consulted on with respect to the energy sector, to ensure that the consumer data right is effective and fairly considers the unique nature and use of data in the energy sector.

We understand that a report has been produced by HoustonKemp Economists at the direction of the COAG Energy Council in relation to the implementation of a consumer data right in the energy sector. While a useful starting point, the energy sector's experience with similar changes (such as the implementation of the *Power of Choice* regime for the roll-out of smart meters, which took effect in December 2017 and was the subject of many years of consultation and joint effort by regulators, market participants and consumer bodies) demonstrates that a much more comprehensive consultation process is required, given the complexity and number of stakeholders that should be considered.

While we have previously provided a separate response to Government on the HoustonKemp report, we reiterate that there are issues which were not adequately dealt with in that report. These include the appropriate data access mechanism, the absence of a cost-benefit analysis for the application of any changes to the energy sector and inadequate details relating to verification of consumer identities. In light of these concerns and the limited consultation that has taken place to date, we would not expect the HoustonKemp report to be used in lieu of more fulsome public consultation with the energy sector. In particular, we strongly believe that any exemption to the consultation process (as was made for the banking sector under section 56GH of the Bill) would be inappropriate.

Further, as currently drafted, we believe that there is a risk that designation could be issued without proper consultation with the applicable sector, leading to unforeseen consequences. To address this, in addition to the requirements at section 56AD, in our view the Bill should include:

(a) minimum requirements for any consultation process (for example, a requirement that the period for submissions remains open for a minimum period of time);

(b) a requirement for the Minister to take public consultation into consideration when drafting the designation, including the proposed scope of CDR data and CDR consumer, with a requirement to take into account concerns that participants in the sector broadly agree are an issue; and

(c) a requirement for the Minister to undertake a cost-benefit analysis as part of considering the exercise of its designation powers.

For the implementation of the consumer data right in the energy sector generally (including with respect to the designation of a sector by the Minister and the development of any proposed consumer data rules by the ACCC), we suggest that the same process is implemented that currently applies in relation to the National Electricity Rules affecting data access (such as the recent Power of Choice program). This would include a formal AEMC rule change and comprehensive cost-benefit analysis of the proposed right.

Further, it is difficult for us to comment on all issues which may arise in connection with the potential designation of the energy sector prior to seeing the proposed consumer data rules and data standards alongside the Bill, given the interdependencies between these documents.

2. Consumer data rules

2.1. Particular issues under the consumer data rules

EnergyAustralia supports the creation of a legislative framework that enables the ACCC to tailor the consumer data rules to different sectors.

Nonetheless, we are concerned with the extent to which the scope and operation of the consumer data right regime is deferred to the consumer data rules (which we note will not become available until after the consultation period on the Bill has closed). In our view, much like with the proposed framework for the exercise of the Minister's power to designate a particular sector, extensive consultation with data holders within the designated sector will be essential to ensure that all applicable consumer data rules are relevant, practical and fairly-balanced. Ideally, stakeholders such as EnergyAustralia should be able to see the proposed legislation and the consumer data rules side by side, to fully understand the impact of the proposed model on the energy sector.

In the context of the energy sector, the consumer data rules will need to be tailored to address (among other things):

(a) the number and diversity of energy sector participants who may hold or require data (eg retailers, distributors, third party sales and comparison websites, other service providers, metering coordinators and meter data providers);

(b) the existing legal and regulatory regime relating to the retail energy sector, including the handling of metering data, and the differences between various legal and regulatory regimes, which differ significantly in some States and Territories;

(c) the nature of data held by energy sector participants, and how they differ from other industries (such as the banking and telecommunications sectors);

(d) the nature of CDR consumers in the energy sector;

(e) the cost-benefit to the energy sector participants and consumers of introducing any new consumer data rules (whether as part of the Ministerial designation or as part of a formal rule change by the Australian Energy Market Commission (**AEMC**)); and

(f) the state of competition in the energy sector, including existing mechanisms in the sector that have been designed to enhance competition.

Accordingly, we believe that extensive consultation with energy sector data holders will be vital to ensuring that a fair and workable set of consumer data rules is applied to the energy sector.

2.2. Consultation

We are concerned that the Bill does not include sufficiently strict processes around the consultation process for the consumer data rules. We believe that the Bill should include a consultation process that requires the ACCC to undertake similar steps to those we outlined for the Minister in section 1 of this submission.

We note that, under section 56BO(3), consumer data rules that are made by the ACCC are not invalidated by a failure to follow the existing consultation processes. This is a concerning addition, as it effectively permits the ACCC to make consumer data rules without any consultation with the energy sector. Given the breadth of the application of the consumer data right and the significant consequences for the energy sector as a whole if the consumer data right is implemented without sufficient consultation, we suggest that this exception is removed.

In our view, it is unlikely that the consumer data rules from one sector can be directly lifted and transferred to another. Each sector will have its own complexities, and the issues that result from the consumer data rules in each sector may not be fully realised until they are used in practice.

To accommodate this we also recommend that a trial period for implementation of the consumer data rules be used for each sector. If each sector were provided with a reasonable period to trial the rules and provide additional feedback without the risk of penalties, this would assist significantly in avoiding unforeseen consequences.

2.3. Application of consumer data right to businesses

Application of consumer data right to large businesses

We strongly believe that the extension of the consumer data right to businesses in relation to their energy data requires further consideration, particularly with respect to how this right may work in practice.

EnergyAustralia is very supportive of a consumer data right which enhances competition in the energy retail sector by granting energy data access to individuals and small businesses who are "small customers" under the National Electricity Retail Law and Victorian Energy Retail Code. However, in our view, it is unnecessary to characterise other commercial and industrial businesses as CDR consumers in the context of the energy retail sector.

In many cases commercial and industrial businesses are account managed and are provided with access to detailed reports about their energy usage. They are already managing their energy data in a highly sophisticated manner, therefore extending the CDR to this customer cohort is redundant.

We believe that the protections provided in relation to "small customers" under the energy sector rules should be applied to any consumer data rights for consistency in regulation. In addition, we do not believe that the CDR regime should be used as a vehicle to change the existing status of customers.

To the extent that businesses will have rights under the CDR regime, the consumer data rules should make distinctions between residential consumers and businesses. This is because the time required to compile the requested CDR data may be longer for businesses, given the complexities of businesses as compared to residential consumers. These complexities grow with the size of the business.

We also note that the Minister's designation of a sector of the economy under section 56AC(2) occurs by the Minister specifying information held by, or on behalf of, specified persons. Further, under the consumer data rules, different rules may apply to different classes of CDR data or classes of persons. We agree with the inclusion of this flexibility, and noting our comments above, we expect that this flexibility should be exercised to reflect the differences between customer classes that currently exist in the current energy sector regulatory regime.

Application of privacy safeguards to businesses

Although we would support the consumer data right being extended to any businesses, we question the need to extend the proposed privacy safeguards to small businesses in the context of energy data, which is unlikely to constitute or involve personal information.

Please see our comments at paragraph 5.1 with respect to these safeguards. To subject disclosure of business energy data to the same requirements, and the same strict penalty regime, as for residential consumers appears to be a disproportionate measure.

2.4. Application of consumer data right to households

We are concerned that the proposed CDR regime does not adequately address the complexities associated with circumstances where a household consists of multiple individuals who may not be account holders.

In our view, it is unclear how the consumer data rights will apply in the energy sector where one or more occupants of a household are not named as account holders by the data holder. In the energy sector it is common for only a single individual to be registered account holder for a household. As a result, energy data will only be recordable at the household level and verified in reference to the account holder.

If, in the context of the energy sector, the term "CDR consumer" is intended to capture every member of a household, we are concerned that this will, at best, create significant compliance issues and, at worst, be impossible to implement. For example, a data holder that is an energy retailer may not be able to comply with a request to disclose CDR data because:

(a) the retailer is unable to obtain consent from all of the possible CDR consumers prior to disclosing any CDR data; or

(b) the retailer cannot verify that the CDR data relates to the particular individual (either because the retailer does not know what energy data relates to that individual, or because the retailer cannot verify that the individual lives or lived at that address).

In our view, the CDR consumer for the energy sector must be an account holder. The consumer data right should not extend to any other member of a household, as data holders (such as energy retailers) do not have a formal customer relationship with individuals who are not account holders and therefore cannot properly provide access to the consumer data right for these individuals. Granting a CDR consumer with the ability to request data if that consumer is not an account holder would be near impossible to manage and may cut across existing regimes with respect to consent and identity management.

We are particularly concerned that data holders may be required to disclose consumer data to former household members in circumstances where disclosure would be inappropriate and potentially dangerous (for example, where there is domestic abuse or other potential safety risks to a CDR consumer).

We strongly believe that the data holder should not be obliged to disclose information that may put any individual at risk, or should be relieved of liability for any such disclosure in circumstances where the data holder is required to disclose the data under that framework. In our view, it is essential that the CDR framework allows a data holder to assess these issues on a case by case basis and to exercise discretion where there is a reasonable belief that disclosure may put any individual at risk. This may be framed as an exception to the access right, similar to the exceptions described under paragraph 5.2 below.

3. Nature of CDR data

3.1. Scope of CDR data

We are concerned that the potential scope of CDR data is too broad and could lead to a CDR regime that is overly burdensome for data holders.

As currently drafted, CDR data will include any data specified by the Minister, without any defined limits. We believe that the Bill should specify pre-defined limits on the types of data that can be specified by the Minister, to ensure that CDR data only extends to datasets that are necessary to enhance competition in the sector. To achieve this, we suggest that the consultation requirements for designation under section 56AD, as well as the framework for the preparation of the consumer data rules, include robust processes to clarify the precise

scope of CDR data for each sector. In our view, broad-based designations of CDR data will lead to considerable uncertainty and possible unintended operation of the regime.

For the energy sector, thought will also need to be given as to whether CDR data would include information relating to solar and gas, and not just electricity. We note that the National Electricity Rules and related laws and procedures put in place a detailed system for the measurement, collection and disclosure of metering data and other data related to a customer's electricity usage. However, solar and gas data are currently subject to different rules and processes to electricity, which may pose significant practical issues and cost to data holders and consumers. For example, gas meters still require manual reads.

If CDR data is expanded to these areas, broader collection rights would be required for bodies than under the current regime and data standards may have to be more flexible.

3.2. Derived and value-added data

We are also concerned with the broad inclusion of derived data in the definition of CDR data. For the energy sector, we do not believe that there is a strong rationale for the inclusion of a right to access derived data.

In our view, the scope of derived data in the energy sector would predominantly include value-added data that has been created by data holders to better understand their customer and to adapt services to target a customer's particular needs. The development of this data often involves investment and innovation on the part of the data holder and, as such, may include the data holder's intellectual property, confidential information and other commercially sensitive information.

While there may be some cases where it would be appropriate to include derived data within the scope of CDR data, we expect these to be the exception rather than the norm. Where the inclusion of certain types of derived data is necessary to achieve the aims of the CDR regime, this could be achieved by the Minister designating the specific category of derived data as "CDR data" for the sector. As such, we do not believe that the broad inclusion of derived data within the scope of the Bill's definition of CDR data is warranted or necessary to achieve the intentions of the Bill.

We are particularly concerned that there may be unintended consequences by including derived data in the definition of CDR data. We are concerned that it will remove an important incentive to businesses to invest in innovation which may in turn decrease opportunities for data holders to improve services and enhance the consumer experience. It can be difficult for energy retailers to differentiate themselves in the market. Value-added data is one area in which energy retailers are able to distinguish themselves by providing consumers with improved services and information. By requiring all derived data to be disclosed to consumers and competitors, this area of distinction is removed and the incentive to innovate to compete for customers by enhancing the customer experience is curtailed. In our view, this is inconsistent with the intent of the Bill.

3.3. Fees for access to data

Where data holders are required to disclose CDR data, we believe that data holders should be entitled to charge a reasonable fee for access to particular information (consistent with the right granted under the Privacy Act).

The value of this fee should reflect where there is additional effort required to access, create or provide the information and any value that has been added to the data by a business, including a return on the business's investment. Otherwise, it is likely to stifle innovation.

In our view, the ACCC should only be responsible for setting the amount of the access fee where the CDR data is raw, unedited and collected through standard processes. To the extent that derived data is included in the proposed regime, in our view the ACCC should not have the power to set the amount that can be charged for access to derived or value-added data.

Where the information contained in CDR data is commercially sensitive, we believe that data holders should be entitled to set an access fee for that data which fairly reflects the value of the data to the data holder (which may include a return on the business's investment). We would be concerned if there was a legislated right to access value-added data in circumstances where the access fee is fixed or capped.

Depending on the proposed data sharing mechanism, in the energy sector a third party such as the Australian Energy Market Operator may be better placed to collect the applicable fees, as opposed to a data holder, such as an energy retailer. With that possibility in mind, in our view, further consideration should be given to which CDR participant should be required to pay any applicable fees (that is, whether these are paid by the CDR consumer or the accredited data recipient) and, if a party other than a data holder has the role of collecting the fee, how that fee will be collected and distributed to the data holder.

4. Relationship between data holder and authorised data recipients

4.1. Right of data holder to be notified where consent is revoked

In our view, the Bill should include a right for data holders to be notified when a consumer's consent to disclose CDR data to an accredited data recipient has been revoked. To effect this, we suggest that the Bill (or the relevant consumer data rules) contains a process by which the data holder can be notified of the revocation of consent to ensure that:

(a) no additional CDR data is transferred to the accredited data recipient, in accordance with the CDR consumer's wishes; and

(b) the accredited data recipient complies with its obligations under privacy safeguard 11 to destroy or de-identify the data.

We note that customer identity verification and management will be a significant issue to address in the context of the energy sector. Currently, the Bill does not differentiate between what we view as "once-off" consents (for a single disclosure) and "ongoing" consents (for continuous disclosures in relation to a period in the future). This "ongoing" consent concept would be required for the operation of services such as *Flipper*, an automated energy provider switching service available in the United Kingdom.

While we understand that some of this detail may be set out in the consumer data rules, we suggest that the Bill set out clearer obligations in respect to maintaining consent and further guidelines regarding when consents are no longer considered current and valid.

4.2. Accreditation of data holder's third party suppliers

As with most large organisations, EnergyAustralia relies on services from within its group and from external third party suppliers to provide its services. With that in mind, we note that the Bill appears to be somewhat unclear as to how the consumer data right is intended to apply to a data holder's related bodies corporate and third party suppliers.

While we do not assume it is intended that related bodies corporate or third party suppliers of the data holder should be required to obtain accreditation if they are receiving data under the consumer data right, in our view clarification of this point may be useful.

5. Interaction between APPs and privacy safeguards

5.1. Crossover between the APPs and the privacy safeguards

We query whether a clear enough delineation between the APPs and the privacy safeguards has been set out in the Bill. As currently drafted, the possibility of dual application of the

privacy safeguards and the Australian Privacy Principles (**APPs**) could lead to somewhat confusing and inconsistent outcomes.

Additionally, as indicated at paragraph 2.3, we note the proposal that the privacy safeguards will apply to CDR data of businesses as well as individuals. In our view, this is a significant new obligation that requires further consideration and cost-benefit analysis before being implemented. While we understand the policy justification for applying expanded protections under the privacy safeguards to CDR data of individuals, it seems less apparent why heightened "privacy" protections should apply to CDR data businesses – effectively granting an extraordinary new right of privacy to those entities.

While maintaining the confidentiality of CDR data of a business is clearly a justifiable requirement, consistent with other regulatory regimes (such as obligations of confidentiality under the National Electricity Rules), the expansion of a broader privacy right to businesses is unprecedented, not costed and particularly onerous. We note that the expansion of a privacy right to businesses was not expressly contemplated in either the Review into Open Banking or the Productivity Commission's Report into Data Availability and Use. Both of these documents reference rights of confidentiality with respect to business data, but not a broad right to privacy.

In addition, there will also be an ongoing need to assess the complex relationship between CDR data and personal information in relation to requests for access, correction of information, security requirements and data breaches. This is likely to require data holders to incur significant costs and establish new processes for dealing with that information. Accordingly, in our view, the obligations under the privacy safeguards should be as consistent as possible with the corresponding obligations under the APPs to ensure that compliance with these obligations can be appropriately and effectively managed.

5.2. Specific privacy safeguards

There appear to be some inconsistencies between the privacy safeguards and the APPs. In particular, the privacy safeguards do not include the same rules and exceptions regarding use and disclosure, collection and other acts or practices.

For example, privacy safeguard 6 (use or disclosure of CDR data) does not include exceptions for a "permitted general situation" or "permitted health situation" (as described in sections 16A and 16B of the Privacy Act) or enforcement related activities, which appear in the APP equivalent (APP 6 (use or disclosure of personal information)). These exceptions deal with threats to life, health or safety of individuals, public safety, taking action in relation to unlawful activity and similar matters.

Additionally, we also note that there are various justifications for a refusal of access under APP 12 (access to personal information). We believe equivalent justifications for refusal should apply, including those suggested in paragraph 2.4 above.

Although section 56EI(1)(a) of the Bill implies that exceptions may be set out in the consumer data rules, it is not clear that equivalent exceptions will apply. In our view, consistent standards should apply across all categories – rather than multiple standards across multiple instruments. We believe that it would be more appropriate to set out exceptions in the privacy safeguards, as opposed to being drafted in the consumer data rules.

5.3. Cross-border disclosure of CDR data

Privacy safeguard 8 (cross border disclosure of CDR data) allows the disclosure of CDR data outside Australia where the recipient holds an accreditation under section 56CE(1) or certain conditions in the consumer data rules have been met.

This appears to allow cross-border disclosure of CDR data to persons that are not accredited data recipients. However, there are no corresponding obligations on the recipient to protect or treat CDR data in accordance with the privacy safeguards.

In our view, this is inconsistent with the equivalent obligations under APP 8 (cross-border disclosure of personal information), which sets out a "reasonable steps" obligation to ensure that the overseas recipient continues to treat that information in accordance with the APPs, unless certain exceptions have been met.

6. Data breach notification

6.1. Application of the eligible data breach requirements to CDR data

The data security breach reporting obligations set out in section 56ER of the Bill are drafted in a way that directly imports the eligible data breach requirements under the Privacy Act, instead of creating an equivalent regime for accredited data recipients.

However, the application of the eligible data breach requirements to all CDR data may have unintended consequences that may require further review. In particular:

(a) it is not clear how the concept of "serious harm" (as used under Part IIIC of the Privacy Act) is intended to apply to CDR consumers that are not individuals; and

(b) given that it appears the Privacy Act obligations will continue to apply to any personal information forming part of the CDR data, dual obligations to notify may arise.

Additionally, we note that the eligible data breach scheme under the Privacy Act is still relatively new. While it will have matured somewhat by the time that the consumer data right is implemented, industry and regulatory approaches to some aspects, such as applying the threshold for serious harm, remain unclear and require further consideration.

6.2. Obligations to notify data holder

As the Bill is currently drafted, an accredited data recipient would be required to provide notice of an eligible data breach to affected CDR consumers and the Office of the Australian Information Commissioner.

Given that the data holder maintains the primary relationship with a CDR customer and given the importance of maintaining the security of CDR data, we suggest that an additional obligation to notify the data holder should be included. This is particularly important in the energy sector, where the retailer is the primary point of contact for consumers in a market that includes a large number of participants in the supply of services for that customer.

7. Remedies

7.1. Misleading or deceptive conduct

We are concerned with how the prohibition against misleading or deceptive conduct might apply to EnergyAustralia's contact centre agents, given that there are instances of human error and there is the possibility of triggering this prohibition in relatively benign circumstances.

While the criminal offence for certain misleading or deceptive conduct set out in section 56BM(1) requires knowledge, this is not the case for the civil penalty under section 56BM(2).

For example, the absence of a knowledge requirement makes it possible that the prohibition could apply to circumstances where a contact centre agent informs a CDR consumer that they have right to access particular information, because the agent is mistaken in the belief that it is "CDR data". We suggest that the civil penalty should only apply where there is an intent to mislead or deceive to avoid it from being overly punitive.

In addition, in our view, a fine of 1000 penalty units for mistaken behaviour that does not result in any harm to the consumers would be unnecessarily punitive and not achieve any meaningful enforcement objective.

We also believe that the application of a criminal penalty, particularly with a potential of 5 years imprisonment, is too harsh in relation to the relevant offence. This penalty is out of step with similar obligations under the Australian Consumer Law. By way of comparison, the criminal offence provisions for false representations do not impose any term of imprisonment, and there are no pecuniary or other penalties for a breach of the general prohibition against misleading or deceptive conduct under the Australian Consumer Law.

If the objective of the rule is to prevent hacking or phishing, then the rule should be crafted in a way that makes clear, with a greater focus on the mental element of the offence (for example, by framing it as false or deceptive conduct to obtain a personal advantage).

7.2. Penalties for breach of Privacy safeguards

We do not believe that the strict application of penalties for breaches of the privacy safeguards set out in the Bill is proportionate to the relevant breach, nor does this mechanism drive the correct behaviour.

Penalties for breaches of privacy are not limited to penalties handed out by regulators, but also include severe reputational harm. Given the strong competition in the energy retail sector, the ability to demonstrate strong privacy credentials is already driven by consumer demands.

Our concern is that minor, accidental, and remediable breaches of the privacy safeguards could, under the current form of the Bill, be subject to significant penalties. This may result in trivial breaches of the privacy safeguards being subject to the same penalty as a serious or repeated breach under the Privacy Act (including in circumstances where the breach could result in serious harm to a consumer).

We consider that this is a disproportionate application of the penalty regime. It may also have the unintended consequence of causing businesses to focus on compliance with the CDR regime over the Privacy Act regime, instead of a holistic approach to protecting individuals against serious breaches of their privacy. Having a regime that is more punitive than the Privacy Act regime is unlikely to remove human error, which is behind many breaches. The penalties for breach of privacy under the Privacy Act have been established with a range of factors in mind, including ensuring that the compliance regime drives correct behaviours. This established position should not be circumvented by the application of the consumer data right, which could effectively override the Privacy Act regime given that the CDR data will, in many cases, also be considered personal information under the Privacy Act.

Further, in our view a civil penalty regime linked to serious or repeated infringements (as is the case under the Privacy Act) is a suitable and appropriate position to adopt for breaches of the privacy safeguards, as it recognises that there is a hierarchy of compliance mechanisms and of the seriousness of privacy breaches. Instead, we suggest adopting the Privacy Act model for the quantum and scope of penalties – including the use of a "serious or repeated" requirement (similar to section 13G of the Privacy Act). We believe that it is more likely that this approach will promote a consistent compliance regime for consumers' privacy.

7.3. Direct right of action for compensation; class actions

We are also concerned with the proposed introduction of a right for consumers to bring action for any civil penalty provision under the consumer data rules, including in relation to a class of persons, through amendments to section 87(1A) of the *Competition and Consumer Act 2010* (Cth).

As we are unaware of what will be covered by the consumer data rules and the civil penalty provisions of the consumer data rules, we cannot provide adequate comment on whether this would be appropriate. However, where non-compliance with the consumer data right could attract a right of action for consumers in a wide range of cases (even for minor or technical breaches), this may increase compliance costs significantly. We suggest that the right of action should only be permitted where expressly specified under the consumer data rules, rather than

by default. Each of these elements should be considered in detail, to ensure that the rights of action granted to an individual are proportionate to the loss that might be suffered under the relevant aspect of the consumer data right.

7.4. Penalties under the Privacy Act and the privacy safeguards

Although section 56ET(5) prevents a person from being penalised under the privacy safeguards and the consumer data rules, we note that it does not prevent a person from also being penalised under the Privacy Act for the same behaviour. As these regimes are likely to overlap, the same conduct should only be liable to penalties under one regime.

8. Role of the ACCC

8.1. ACCC and OAIC oversight

The dual regulator model proposed in the Bill is a novel proposal, which will require significant management to ensure that both the ACCC and the OAIC manage complaint handling, enforcement and their respective powers in a co-ordinated and consistent sense.

The worst-case outcome would be for the ACCC and OAIC to take an inconsistent approach to the interpretation and application of the rules, as it would make compliance difficult if not impossible. We are also concerned that, in the interest of avoiding that situation, the dual-regulator model could also lead to a situation where each body is reluctant to provide compliance guidance for fear of the other body taking a different view.

In a novel area of regulation such as this (and arguably more generally), clear guidance from the regulator about how it will interpret and apply the law is fundamentally important to achieving the policy objectives that underpin the law. We therefore submit that it will be very important for:

(a) the ACCC to prepare and publish clear guidelines about the delineation of functions between it and the OAIC;

(b) the ACCC to ensure that the scope of delegations to OAIC are transparent; and

(c) the regulatory bodies to provide clear, and consistent, guidance about how they will interpret and apply the law.

8.2. ACCC enforcement powers

The ACCC is a powerful regulator, with a formidable arsenal of investigative and enforcement tools available to it. In this new area, it will be in a position where it is the author, administrator and enforcer of the substantive rules that underpin the regime.

Given this, we consider it very important for the ACCC to clarify its compliance and enforcement policy in this area by issuing detailed guidance about complying with the rules.

Our view is that, in such a novel area, the ACCC should adopt a collaborative and consultative approach (similar to the way it approaches authorisations), rather than a more traditional enforcement approach, except in cases of serious or systemic misconduct. This is more likely to achieve the policy objectives by working with industry to ensure that the rules are applied in a way that is clear and makes sense, and to avoid a situation where regulatory uncertainty leads to conservative compliance practices that create inefficiencies, stymying competition and investment in this very important area of the economy.