



Contact: Verity Watson  
Manager Regulatory Strategy  
United Energy  
Phone: (03) 8846 9856

# UE Response to ESC, Smart Meter Privacy Impact Assessment, Draft Report

15 June 2012



*This page intentionally left blank*



---

## Table of Contents

1. Introduction and purpose .....	4
2. Audit Requirements .....	4
3. Privacy Policies .....	6
4. Customer Access to metering data.....	6
5. Secondary use of metering data.....	7
6. Audit of data security .....	7
7. Access controls to on line and archived metering data.....	8
8. Opt in arrangements to NPP.....	8
9. Provision of data in industry standard format.....	9
10. Industry best practice management for portals.....	9
11. Binding and unbinding processes.....	10
12. National business processes for HAN activation .....	11
13. Shared household management.....	12
14. Earlier ESC decision wording .....	12

## 1. Introduction and purpose

This document sets out United Energy's (UE) response to the ESC Draft Report titled Smart Meter Privacy Impact Assessment.

UE recognises that privacy of metering and energy data is a significant concern for consumers and that data access provisions will need to change with the introduction of energy portals, in home displays, third party information service providers and possibly centralised energy hubs.

Due to the sensitive nature of personal data, Lockstep and the ESC have taken the view that metering data is in itself confidential information about a single individual. However, UE note that smart metering data or metering data, without a personal identifier of the customer, is not of itself private information. UE is supportive of appropriate business processes relating to data security and privacy to manage personal information. Audit processes need to be cost effective and risk based.

A number of issues relating to third party providers need to be clarified by policy makers and systems and processes put in place by the appropriate regulatory agency to manage the registration and compliance/enforcement arrangements.

UE considers that as In Home Displays (IHDs) and other Home Area networks (HAN) devices are consumer products and not in the control domain of the distributor, or retailer. The consumer is ultimately responsible for the management of these devices including the stored data within those devices and is best placed to effectively purge any data.

## 2. Audit Requirements

### ESC Recommendation 1

Retailers and Distributors should be required to conduct an independent audit of their compliance with NPPs before the roll out of smart meters is completed or as soon as possible thereafter. The audit should follow principles laid down by the Office of the Australian Privacy Commissioner and should include:

- Security systems (including data storage and quarantining, online portals)
- Staff training
- Staff access to systems and information
- The systems and processes of third party providers contracted by Retailers and Distributors, where customer metering data is accessed or stored by these.

In the short term all industry participants should be audited, and then as compliance is assured, audits should be limited to those participants who generate complaints.

Audits should be published in their annual report/on the company website and provided to the Australian Energy Regulator through regulatory performance or compliance reporting.

To promote industry readiness and consumer confidence, Retailers and Distributors should also:

- Conduct induction and on-going training for their staff in Privacy principles, and

- Satisfy themselves as to the scope, completeness and regularity of the training provided by third party providers to their staff, as part of initial and ongoing contractual arrangements with third party providers engaged by them
- Ensure that they can identify, react to and resolve systemic non-compliance

UE agree that businesses should include privacy and confidentiality within normal audit programmes.

Internal audit findings should be primarily aimed at ensuring that effective controls are in place to ensure compliance, ensure that systems and processes are continually reviewed for improvement and identify actual or potential breaches. Internal audit findings should be reviewed by the relevant management and provided to an overarching audit committee.

Whilst UE includes privacy within its internal audit programme, UE does not support the publication of audit findings on external websites. Internal audit reports are for management purposes and it is not necessary or appropriate to publish such information on a public website.

UE is supportive of an independent audit in this area as part of the AER compliance framework. The Draft Report states that these independent audits would review security systems, staff training and staff access to the systems and information and would extended to contracted third parties if customer data is stored or access by these parties. UE is supportive of an approach that after an initial audit assuring compliance that further audits be limited to those participants who generate complaints. This ensures that audit costs are minimised resulting in lower costs for smart metering services such as portals or binding services. UE also supports the AER publishing a summary of audit findings across industry in a similar manner to current compliance arrangements in order to promote consumer confidence.

AEMO accreditation requirements consider data confidentiality, audit, security management and access controls, physical security and security controls. AEMO audit metering providers and metering data providers on these aspects on a regular basis. UE query the need for any additional level of audit review.

UE note that the Draft Report proposes significant obligations on licenced entities or authorised retailers. The Draft Report notes that it is difficult to justify the imposition of a regulatory scheme, which would be costly and difficult to implement without having a degree of risk to privacy that third party providers might present. If the ESC view is that metering data is in itself private information of an individual then it may be appropriate that at a minimum third party providers who are not subject to the National Privacy Principles (NPP) are encouraged to opt in to the NPP. Ideally, these third party providers should be registered and accredited so that compliance can be monitored.

The Victorian Energy Efficiency Target (VEET) Scheme, administered by the ESC requires accreditation of persons used to install in home displays (IHD). This accreditation process requires the Accredited Persons (APs) to attest that they have the means of complying with all relevant laws and guidelines. UE support the ESC view that the VEET Scheme should include privacy issues as part of the ESC's performance monitoring programme. Whilst UE's core service agreement will clarify privacy expectations placed on APs, it is not the distributor's role to exercise accountability and compliance of the AP, this is a matter for the ESC. The VEET scheme has created the AP role, the enforcement agency for this policy should deal with any compliance matters created by the APs.

### 3. Privacy Policies

#### ESC Recommendation 2

We recommend that Industry develop a common layered Privacy Notice that can be used as the basis for all organisations involved in AMI; and consider developing an industry-wide Privacy Policy (perhaps as an Industry Code to be approved by the Privacy Commissioner). The Notice, and the Policy or Code should include:

- Plain English wording and provision for customers of non-English speaking background.
- An agreed definition and explanation of secondary uses of personal information developed by the National Smart Meter Program in conjunction with Industry.
- A list of examples of secondary uses according to the current practice of each business, and provision to expand as new uses are introduced.
- An explanation of why smart metering data is collected, how it is used, under what circumstances is it disclosed, and the range of regulatory and operational safeguards that protect it.
- Contact details for the business, the OAIC and EWOV or its equivalent, to facilitate complaint handling.

All Privacy Codes should be easy to locate on Industry websites.

UE broadly support the ESC Draft Report in relation to the contents and ease of access to a Privacy Policy. UE suggest that the Privacy Commissioner may be a better contact point for privacy issues as opposed to the proposed contacts above.

There are a number of data access issues in relation to various sets of rules, third party access and the future role of information service providers which will need to be resolved before embarking on an industry wide privacy policy or code.

Further, UE sees limited value in developing an industry wide Privacy Policy. The National Privacy Principles (NPP) apply across the industry and as a result ensures a degree of consistency across Privacy Policies in Victoria.

### 4. Customer Access to metering data

#### ESC Recommendation 3

The Commission recommends that consumers who seek access to their smart metering data be given it to the extent this is possible under existing National Electricity Rules.

UE note that, with respect to customer access to energy and metering data, the interaction between rule 7.7 (a) (7) of the National Electricity Rules, rule 86 of the National Energy Retail Rules and rule 38 of the draft National Energy Retail Law (Victoria) Act 2012 – Victorian Energy Rules needs to be clarified. The AER has indicated that it may use a Compliance Bulletin to provide some clarification regarding the interaction between these clauses.

UE concur with the ESC view that customers should be provided access to their energy data or metering data should they seek it.

## 5. Secondary use of metering data

### ESC Recommendation 4

We support the Opt-In process for customers consenting to the secondary use of metering data.

We recommend that the process used by Industry for obtaining customers' consent to the use of their 'Personal Information', including metering data from smart meters, should be structured to permit consent to separate secondary data uses over time as new products and capabilities are developed for the market.

A customer's express consent should not be required for secondary purposes exempted by the AMI Policy Committee and uses stipulated and required by legislation.

UE support broad consistency across the industry regarding secondary use of metering data to provide a level of reassurance to customers. The ESC has recommended that this be undertaken as part of the National Smart Meter Program (NSMP), however this program is currently waiting on a number of policy issues to be clarified by the Standing Council on Energy and Resources (SCER).

## 6. Audit of data security

### ESC Recommendation 5

This aspect of data security should be subject to internal and external audit processes as outlined in ESC Recommendation 1.

UE support a cost/risk based approach to audit programs including data security and access controls. UE note that such matters are currently part of an overall audit program conducted to ensure compliance with regulatory obligations.

## 7. Access controls to on line and archived metering data

### ESC Recommendation 6

Any regulatory obligation to provide data to the market should be clarified by the AER in terms of who bears this responsibility, time frame and detail having regard to the new paradigm presented by smart meters.

Staff access to retained interval data should be monitored and audited (as per the Commission's Recommendation 1 above) to ensure it remains appropriate and required for defined business purposes.

External access to aged interval data should only be permitted with a customer's consent if it is their data, and otherwise, only where it is aggregated or otherwise unable to identify individual customer's usage.

Data access provisions are in accordance with the arrangements under the NER and relevant laws/rules/regulations.

## 8. Opt in arrangements to NPP

### ESC Recommendation 7

We recommend that all third party providers that access or store 'Personal Information', including metering data of electricity customers from customers themselves via their HAN should be encouraged to abide by the NPPs in their business.

This could be in the form of encouragement to Opt-In to coverage under the Privacy Act 1988 as allowed for by the Office of the Australian Information Commissioner. We also recommend that the AER consider publicising the names of third party providers who agree to abide by NPPs.

The ESC should monitor compliance of Accredited Persons with privacy obligations. In the event any APs expand their business model to provide other services involving accessing and storing data from IHDs (such as for energy efficiency analysis) the ESC should:

- Further specify Privacy obligations as part of the process for seeking accreditation
- Amend or develop regulation to be able to suspend or remove accreditation for breaches of privacy.

Small electricity retailers should be under the same obligation to protect customer data as other Retailers. Accordingly they should be made subject to the NPPs as a condition of their authorisation by the AER.

If the ESC view is that metering data is in itself private information of an individual then it may be appropriate that at a minimum third party providers who are not subject to the NPP are encouraged to opt in to the NPP. Ideally, these third party providers should be registered and accredited so that compliance can be monitored.



## 9. Provision of data in industry standard format

### ESC Recommendation 8

We recommend the development of a minimum industry standard for data provision with respect to smart meter interval data; and separate information materials to inform consumers of the value of metering data information and to clarify industry terms.

UE considers that there is limited value in the development of a minimum industry standard for information and explanatory materials to assist customers in deciphering AMI data. UE has already undertaken such an initiative in its smart metering material for customers and also in the presentation of metering data in the UE Energy Easy portal.

## 10. Industry best practice management for portals

### ESC Recommendation 9

Retailers' and Distributors' online portals should comply with industry best practice standards, including when operational, the conduct of regular security audits. This should be included as part of an independent audit of data security systems and processes (see ESC Recommendation 1).

Websites not applying a recognised industry best practice standard should be subject to an independent threat and risk assessment.

We recommend that DPI work with industry to identify acceptable standards for online portals, monitor online portals and keep industry informed of changes in industry best practice standards.

Government will need to consider what is the appropriate standard/benchmark for these types of websites, what powers would be required to rectify/remedy deficient websites and which agency would be responsible for enforcing this.

UE notes its responses to ESC recommendations 1 and 5 above, but is otherwise supportive of ESC recommendation 9.

## 11. Binding and unbinding processes

### Recommendation 10

We recommend that a Protocol be developed to clarify the respective roles of customers, Retailers, Distributors and third party providers to protect customer data (by purging it from an IHD) at the time of unbinding from a HAN. This protocol should consider:

- The present primary communication role of Retailers with customers,
- The possible involvement of other third party providers (other than meter readers and Accredited Person) in accessing data via the HAN in future,
- The requirement to give customers the opportunity to explicitly Opt-In to the use of their data for secondary purposes ( as expressed in NPP 2.1)

We recommend that the unbinding process be an industry managed solution that does not rely on customer knowledge or memory to prevent wrongful access to another customer's data.

The Lockstep Report recommends that a customer's HAN devices be unbound upon the customer vacating the premise. UE supports this Lockstep recommendation, however notes that the Lockstep report does not suggest purging of energy data from HAN devices.

Smart Meter connected HAN devices as deployed in Victoria are at minimum compliant to ZigBee Smart Energy Profile 1.0 (SEP). The Smart meter includes an Energy Service Interface (the ESI is an implementation of ZigBee SEP). A HAN device like an IHD is a consumer appliance and outside the control domain of the LNSP. The ESI is the last domain of control for the LNSP and the ESI cannot manage downstream devices as prescribed by the ESC recommendation 10.

Presently, Smart Meters in Victoria must have the capability of storing interval energy data for a period of 200 days (pursuant to clause 2.4.23 of Metrology Procedure part A, for a type 5 metering installation). Consequently the energy data in the meter cannot be erased and any HAN device can retrospectively collect 200 plus days of energy data once connected.

None of the present or forthcoming ZigBee SEP standards (SEP 1.0, SEP 1.1, SEP 1.2 or SEP 2.0) has provision for a command/control to purge data from a HAN device. Even if a future implementation of SEP supported such a command it may not be adopted by device vendors as it is not compulsory to implement all features of the ZigBee stack. Therefore there will be no certainty that issuing a purge to HAN devices from the Smart Meter ESI will have the desired outcome. The only way a HAN device can be purged of historical data with any certainty is individually and at the device.

UE notes that once energy data enters the consumer domain the customer does have a role in taking responsibility for their own energy data and how it is stored, transmitted, analysed and utilised by the customer, or other parties.

Accordingly, UE considers that consumer education and participation is key to addressing privacy concerns in relation to HAN devices. Consumers should be educated so that they are aware of the types of information stored in a HAN device, and how care should be exercised in authorising a HAN device to pass this data to other parties or services. Importantly, consumers need to be aware that moving out and

leaving a HAN device may result in the new property owner accessing their historical energy data. If this is of concern to the consumer they can choose to erase the historical data.

UE considers that as IHDs and other HAN devices are consumer products and not in the control domain of the LNSP, or retailer, the consumer is ultimately responsible for the management of these devices including the stored data within those devices.

## 12. National business processes for HAN activation

### ESC Recommendation 11

The Commission recommends that the National Smart Metering Program take into account the following considerations in developing business processes and protocols for HAN activation:

- The need for a clear and common understanding of secondary uses of metering data and a clear delineation of the responsibilities of Retailers, Distributors and/or others for obtaining customer consent are minimum requirements for effective enforcement of customer Opt-In provisions.
- The development of a specific regulatory relationship with unregulated third party businesses, beyond encouraging the adoption of the NPPs, may impose potentially excessive regulatory burden, and that this issue be revisited in the light of future experience with smart meters.
- At this stage the Commission sees value in the provision of some structured form of information or support for customers (**see also Consumer Information Recommendation 14 below**)

The NSMP recommended to policy makers that a gateway review be conducted to determine how best to transition a number of arrangements beyond a mandated smart meter roll out. The provision of third party data access and roles and responsibilities generally needs to be reviewed.

UE note that DRET are already considering third party information service providers and centralised portals under the Clean Energy Package.

Once the SCER has consulted and made these policy positions clear, the AEMO reference groups will be better positioned to develop industry processes and protocols. Whether third parties are regulated or accredited under the Rules framework is a matter for policy makers.

---

## 13. Shared household management

### ESC Recommendation 12

We don't see an immediate need to introduce regulations in relation to Lockstep's recommendation.

Government and the relevant regulatory agencies would need to consider whether a completely new form of contract would be required given the type of service envisaged and what the complexities, risks and cost benefit of taking the proposed approach could be.

UE support the ESC view that there is no need for further regulation in this area.

## 14. Earlier ESC decision wording

### ESC Recommendation 13

While we agree the recommended wording may have been preferable, we consider that any amendment to previous Commission decisions may be unnecessary and undesirable at this point particularly given the transfer of retail regulatory functions to the Australian Energy Regulator in July 2012.

UE has no comment.