ESSENTIAL SERVICES COMMISSION

SMART METER PRIVACY IMPACT ASSESSMENT

DRAFT REPORT

MAY 2012

An appropriate citation for this paper is:

Essential Services Commission, 2012, *Smart Meter Privacy Impact Assessment – Draft Report,* May 2012

Table of Contents

GLOSSARY

AER	Australian Energy Regulator
AEMO	Australian Energy Market Operator
AMI	Advanced Metering Infrastructure
AP	Accredited Person
DB	Distribution Business (Distributor)
DPI	Department of Primary Industries
ENA	Energy Networks Association
ESC	Essential Services Commission
ESI	Energy Saver Initiative scheme
EWOV	Energy and Water Ombudsman of Victoria
HAN	Home Area Network
IHD	In-home Display
OAIC	Office of the Australian Information Commissioner
NER	National Electricity Rules
NPPs	National Privacy Principles
NSMP	National Smart Meter Program
RB	Retail Business (Retailer)
VEET	Victorian Energy Efficiency Target scheme

1. SUMMARY

Smart Meter Program

A major upgrade of Victoria's electricity infrastructure (the Advanced Metering Infrastructure AMI program) means all households and small businesses are scheduled to have their existing accumulation meter upgraded with a new digital Smart Meter by the end of 2013. Digital Smart Meters are being rolled out by Victoria's five electricity distributors – CitiPower/ Powercor, Jemena, United Energy and SP AusNet.

Unlike the old metering technology they replace, Smart Meters are two-way, digital communication systems that record electricity usage every 30 minutes. Using a web portal or an in-home display connected to their Smart Meter, householders and businesses (or their agents) will be able to access more detailed information about their electricity use.

As with any new system, it is important that privacy issues have been addressed as far as possible at the outset.

Lockstep Report

In 2011, Lockstep Consulting was engaged by the Department of Primary Industries (DPI) to undertake a Privacy Impact Assessment of Victoria's smart metering program. The scope of the Lockstep PIA Report is *the smart metering program in general, with the objective of establishing whether the program as overseen by DPI properly anticipated the privacy impacts of introducing interval metering, remote communication and control capabilities to domestic consumers, and whether the management and design of the new metering system provides for adequate controls over Personal Information*[1].

Lockstep has taken the view that smart metering data should be treated as "Personal Information"[2] in privacy terms because of the capacity to identify a consumer from their data. Defining metering data as such means that this information belongs to the customer (as opposed to the Distributor or Retailer) and must be treated in accordance with the National Privacy Principles (NPPs).

This view reinforces the consumer's entitlement to receive their own information. It means that consumers must also be given the opportunity to choose how or indeed whether, their metering data may be used for secondary purposes. It means that consumers may agree to pass on their metering data to third parties to provide some other service arising from the data such as analysis of their power usage. Lockstep's view, if endorsed by

[1] The Lockstep Consulting Privacy Impact Assessment Report, Version 1.2, August 2011.

[2] Personal information is information that identifies you or could identify you. There are some obvious examples of personal information, such as your name or address. Personal information can also include medical records, bank account details, photos, videos, and even information about what you like, your opinions and where you work - basically, any information where you are reasonably identifiable.
Information does not have to include your name to be personal information. For example, in some cases, your date of birth and post code may be enough to identify you.
To be precise, the Privacy Act definition of personal information is:
"... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." From the website of the Office of the Australian Information Commissioner.

policymakers, potentially opens the industry to a broad spectrum of new players and, unless appropriately regulated, could increase the likelihood of inappropriate use of customers' Personal Information.

While Lockstep concluded that there was no need for operational changes to the way electricity Retailers, Distributors and the Australian Energy Market Operator (AEMO) handle information flows and that data security was generally good, it noted that the means of resolving broader concerns related to privacy – most notably openness about use and disclosure of information and the choices that consumers will have to control secondary usage under a future smart meter environment – are not well ingrained across the electricity industry.

Lockstep's Report included nine critical recommendations and fifteen other recommendations intended to address the shortcomings it identified. The full Lockstep PIA Report is available on DPI's website[3].

Ministerial referral

The Minister for Energy and Resources wrote requesting that the Commission:

- Consider the relevant findings and recommendations of the Lockstep report and review, accordingly, the regulatory requirements on Retailers and Distributors;
- Require electricity Retailers and Distributors to ensure that they comply with privacy standards and procedures in relation to smart meter data in accordance with their licence requirements; and
- Publish a fact sheet on the YourChoice website advising consumers how personal information is handled securely by Retailers and Distributors;
- Liaise with the Department of Primary Industries on the development of a framework within which third parties may provide smart meter enabled products and services while protecting the rights and interests of consumers.

The Commission's approach to this Review

After discussions with DPI, the Commission released an Information request seeking industry submissions in relation to sixteen of the recommendations. The remaining eight recommendations are to be considered by other regulatory agencies. The Commission has used the Industry responses, and its own experiences and analysis to prepare this draft report.

A summary of responses from Industry can be found on the Commission's website, www.esc.vic.gov.au.

The draft report is released for public consultation. Submissions close on 15 June 2012.

A final report will be provided to the Minister by 29 June 2012.

Risk Assessment

The current regulatory framework in Victoria obligates retailers and distributors, via their licences, to comply with all applicable laws, Codes and Guidelines. Relevant industry Codes and Guidelines, issued by the Commission, do not explicitly address privacy concerns and therefore compliance with privacy obligations is not specifically monitored by the Commission.

[3] See http://www.dpi.vic.gov.au/smart-meters/privacy

We note that there is currently insufficient granularity within reported complaint numbers published by the Energy and Water Ombudsman Victoria (EWOV) or the Office of the Australian Information Commissioner (OAIC) to draw any definitive conclusions that the electricity sector is currently not meeting their licence obligations as they relate to privacy.

The Lockstep Report also noted that they found little evidence of regular internal auditing by businesses of the way customer databases are used.

To date, as reported through the media, consumer privacy concern seems to be mainly about whether the operation of smart meters (e.g. the flashing light and the collection of meter data) might reveal to others the activity of a household. We note that the smart meter rollout is not due to conclude until December 2013 and that consumer concerns about privacy in relation to smart meters may increase, particularly as the rollout proceeds and third party businesses offering services to enable more diverse uses of metering data become prevalent.

Given community sensitivity to issues of privacy and confidentiality the Commission recommends that Government pursue a moderately strong level of regulation and self-regulation at the outset to ensure the AMI programme commences with a secure beginning with respect to privacy issues while not unnecessarily constraining the opportunity for diversity and competition within the sector to emerge.

Regulatory Approach

In undertaking this Review, the Commission has been mindful of the broader Government policies to reduce regulatory burden and the resultant costs to business, and to provide greater choice to consumers as a means of encouraging competition and greater efficiency.

The Commission's light handed regulation of the retail energy sector reduced the frequency of regulatory audits, to allow the retail industry to self-report its non-compliances as they occur and to annually attest to the robustness of its compliance monitoring systems. Faced with increasing complaint numbers the Commission required regulatory audits in 2011 and those independent audits have concluded that the retailers' faith in the robustness of their compliance monitoring systems has often been overstated.

The Commission is also conscious that a significant change to the industry is likely to occur with the introduction of third party services providing advice to consumers based on analysis of customers' smart metering data. It is expected that such businesses could be small, start-up businesses that would not be necessarily subject to an existing regulatory regime in respect of privacy as many may fall outside the parameters set by the Privacy Act 1988[4].

The Commission would expect that as the smart meter roll out is completed and the industry implements a number of protocols (some still under consideration, others yet to be considered) that the degree of regulatory oversight could be progressively reviewed. Better information based on the actual operation of the AMI programme would also be available to inform any future regulatory approach.

[4] Businesses with an annual turnover of $3 million dollars or less are exempt from coverage under the Privacy Act 1988.

We also note that other comparable industries, such as telecommunications, have stringent industry specific legislative provisions governing the handling and release of Personal Information, which are far in excess of the regulatory approach recommended in this case[5].

The Commission is mindful that the regulation of the energy industry is changing from 1 July and that most of the Commission's regulatory recommendations will fall to the Australian Energy Regulator (AER) to implement in a context where the use of smart meters is presently limited to Victoria.

Industry Submissions

Retailers and Distributors provided a great deal of information regarding their current practices, policies and procedures. They believe that no substantive changes are necessary to these internal systems as a result of the smart meter rollout. Retailers, in particular, noted that the pending transition of state based retail regulation to the Australian Energy Regulator (AER) was such a fundamental change to the regulatory framework that further incremental amendments to existing State based regulations at this time were undesirable.

Retailers' responses seem to address future secondary usage based on the current industry model rather than envisaging a future model involving a diversity of roles for Retailers and Distributors, third parties, greater opportunities to access customer data and a greater number of secondary purposes. This is reflected in their responses to questions about data retention and storage and obtaining customer consent to the use of their data for secondary purposes.

Distributors have pilot programs to trial In-Home Displays and Home Area Networks, taking on new roles and relationships with customers and Retailers as they do so.

Neither Retailers nor Distributors suggested means to address the emergence of unregulated third party providers to the market other than to note this possibility and leave it to the consumer to manage.

.

[5] Under Part 13 of The *Telecommunications Act 1997*

- Carriers, carriage service providers, number-database operators, emergency call persons and their respective associates must protect the confidentiality of information that relates to:
  - (a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and
  - (b) carriage services supplied by carriers and carriage service providers; and
  - (c) the affairs or personal particulars of other persons.
- The disclosure or use of protected information is authorised in limited circumstances (for example, disclosure or use for purposes relating to the enforcement of the criminal law).
- An authorised recipient of protected information may only disclose or use the information for an authorised purpose.
- Certain record-keeping requirements are imposed in relation to authorised disclosures or uses of information.

1.1 Key Themes

In summary, the Commission's recommendations, outlined in Chapters 2 & 3, are based on:

a) The introduction of independent privacy audits of business systems, data bases and processes for Retailers, Distributors and third parties (subject to an appropriate regulatory framework)

b) The development of a commonly worded Privacy Notice and/or a Privacy Policy, including a common statement of secondary uses of metering data, to enhance customers' understanding of how their smart meter data will be used and protected.

c) Providing consumers who request it access to their smart metering data information

d) The development of a process for customers to expressly Opt-In to the use of their data for each of the different secondary ways it may be used

e) The encouragement of unregulated third party service providers to opt-in to the National Privacy Principles (NPPs)

f) The provision of consumer information on:

- Standard privacy protection wording to look for when entering into a contract with an unregulated third party provider
- Standard formats and parameters available for provision of interval meter data information to customers
- A list of third party providers that have agreed to abide by the NPPs in handling customers' information
- How to unbind an In-Home Display (IHD) from a Home Area Network (HAN) and how to remove historical data from an IHD
- The roles and responsibilities of Retailers', Distributors and other third party providers for smart meter data and IHDs (who installs these, what happens if I move or change Retailer, who can help me interpret the data, what if I have a question or complaint?)

g) The improved collection and analysis of information from consumers about privacy issues through Industry, regulatory agencies and EWOV complaint recording processes.

2 ESC consideration of Lockstep Report Recommendations

The following table outlines in more detail the Commission's response to each of the Lockstep recommendations and the Commission's [Draft] recommendations. Chapter 3 provides a more detailed discussion of the Commission's analysis and the rationale for each recommendation.

Lockstep Recommendation	ESC Recommendation
Recommendation 1 All metering data from or about residential meters should be handled throughout the Advance Metering Infrastructure (AMI) system in accordance with the National Privacy Principles (NPPs), in order to safeguard it against potential abuse, better control future secondary usage by unregistered third party participants, and to more clearly demonstrate to customers and the public that the industry is committed to privacy.	**Recommendation1** 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. Audit results should be published in their annual report/on the company website and provided to the Australian Energy Regulator through regulatory performance or compliance reporting,

Lockstep Recommendation	ESC Recommendation
	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 and react to systemic non-compliance. **See also ESC Recommendation 7 below**
Recommendation 2 Privacy Policies of Distribution Businesses (DBs) and Retail Businesses (RBs) should be reviewed and updated to describe each organisation's commitment to the NPPs, including explanations 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	**Recommendation 2** Industry should 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 (within the meaning of section 2.1 of the NPPs) 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.

Lockstep Recommendation	ESC Recommendation
	• 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. Third Party providers that voluntarily opt in to the NPPs would be subject to the requirements of the Privacy Act.
Recommendation 3 Even though details of how third party services and Home Area Networks (HANs) will operate remain sketchy, it would be appropriate at this stage for RBs' and DBs' Privacy Policies to anticipate the sharing of data beyond their businesses and circumscribe access to metering data. Note that this action should satisfy the ESC's call for "privacy principles" to be developed before In-Home Displays (IHDs) are deployed.	**Recommendation 3** The Commission recommends that consumers who seek it be given access to their smart metering data to the extent this is possible under existing National Electricity Rules.
Recommendation 4 The industry should adopt and promote an Opt-In policy of not putting metering data to any secondary purposes without express customer consent. For the avoidance of doubt, and to maximise consumers' sense of control, such secondary uses should include even those that seem reasonably related to the primary purpose for collection, such as the	**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.

Lockstep Recommendation	ESC Recommendation
provision of efficiency advice. The industry should ensure that consent to secondary uses is always freely given, is not conditional, and is never bundled into acceptance of an electricity supply contract. The AMI Policy Committee should review any suggested exceptions to the Opt-In that might be put forward by Registered Participants, and if agreed, officially specify them.	Further, we consider that 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.
Recommendation 6 As and when DBs and RBs implement new databases as part of the AMI adoption, they should take care to keep raw metering data (keyed by National Meter Identifier alone) separate from all other identifiable customer records in order to mitigate against ready re-identification. In general it is essential that teams implementing, configuring and maintaining databases are fully aware of the NPPs and the broad legal definition of Personal Information, to help them avoid inadvertent privacy problems.	**Recommendation 5** This aspect of data security should be subject to internal and external audit processes as outlined in ESC Recommendation 1 above.
Recommendation 8 Consideration should be given to clarifying what meter data may be (or should be) disposed of after seven years. From a privacy perspective, unless there is a clear reason to retain fine grain interval data at each Participant, it should be destroyed, or aggregated to the greatest	**Recommendation 6** We recommend that 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

Lockstep Recommendation	ESC Recommendation
reasonable extent.	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.
Recommendation 14 Review “Privacy Notices” provided to smart meter customers— whether they be explicit or implicit (as is often the case where passages of legal text are incorporated into other customer communications) — and ensure that the notices properly anticipate the potential secondary uses of metering information (such as providing energy efficiency advice direct to consumers, supporting third party services on an opt-in basis and so on).	**See ESC Recommendation 2 above.**
Recommendation 15 Consider developing a common skeletal layered Privacy Notice that all organisations involved in AMI can use as a basis for their own notices, setting out the industry’s regulatory protections, the reasons and uses for smart meter data collection, and the controls that consumers have over how meter data is used.	**See ESC Recommendation 2 above**

Lockstep Recommendation	ESC Recommendation
Recommendation 16 Require that small Retail Businesses that might otherwise fall below the Small or Medium Enterprise (SME) criterion for the Privacy Act expressly opt in to the NPPs with the Office of the Privacy Commissioner.	**Recommendation 7** All unregulated 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 as a form of 'tick' or approval of such action. The ESC should monitor compliance of Accredited Persons (VEET accredited installers of IHDs) 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.

Lockstep Recommendation	ESC Recommendation
Recommendation 17 Consider industry-wide minimum security policy settings for protecting interval data against misuse, including the following possibilities: • DBs should quarantine all data containing customer names from raw interval data • DBs and RBs should audit log all access by users to interval data Retained interval data aged between two and seven years should be subject to more limited access rights than more recent data that might be needed to resolve billing issues.	**See ESC Recommendations 1 and 6 above**. Staff access to retained interval data is the responsibility of business to manage according to the NPPs. We see this aspect of data management as also subject to our audit recommendations.
Recommendation 19 In order to give consumers access to their interval data (as required by the Access & Correction Principle NPP 6), protocols should be developed for providing data in standard formats such as Excel spread sheets.	**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.

Lockstep Recommendation	ESC Recommendation
Recommendation 20 In order to boost consumer confidence in the security of the system, DPI should consider commissioning an independent Threat & Risk Assessment (TRA) of any new online portals	**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 also be included as part of an independent audit of data security systems and processes. Sites not applying recognised industry best practice standards 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. Further, the Government should clarify what powers would be required to rectify/remedy deficient websites and which agency would be responsible for undertaking this assessment.
Recommendation 21 Protocols will need to be developed for preventing old occupants from still having access to and/or control over the HAN after they vacate premises. Ideally, when a smart meter's customer changes, there should be an automatic unbinding of devices from the HAN, and the access code for establishing a HAN on that meter should be changed. It may be prudent	**Recommendation 10** We support Lockstep's recommendation and consider that a Protocol will be essential 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

Lockstep Recommendation	ESC Recommendation
to amend the NECF or NER to legislate these measures.	Accredited Person) in accessing data via the HAN in future, • The requirement to give customers the opportunity to explicitly Opt-In to use of their data for secondary purposes. 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.
Recommendation 22 When the BPPWG comes to develop business processes and protocols for HAN activation, it should enact the Opt-In policy of Recommendation 4 above (to be confirmed) that all secondary uses of metering data shall be subject to express consent. Further, the BPPWG should consider enforceable requirements that data is handled across all HANs in	**Recommendation 11** We recommend 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

Lockstep Recommendation	ESC Recommendation
accordance with the NPPs.	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).
Recommendation 23 If in future individuals within a household enter into third party contracts (with Retailers or Third Parties) relating to use of smart meter data, such contracts should be signed by both the individual and the main electricity account holder.	**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.
Recommendation 24 The ESC should amend the wording of its decision to refer to Privacy Policies or Codes, rather than "Privacy Principles" because the latter term has a technical meaning in legislation.	**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 scheduled transfer of retail regulatory functions to the Australian Energy Regulator in July 2012.

2.1 Other Recommendations

The following three recommendations do not correspond with specific Lockstep recommendations but arise from the Commission's considered view that there is not a regulatory option available or recommended at present for each identified issue.

In particular these recommendations seek to increase knowledge of actual consumer concerns about privacy and to provide consumer information and education as an alternative to regulation of certain third party providers that may emerge in the electricity market.

Recommendation 14 - EWOV

We recommend that the Energy and Water Ombudsman of Victoria review its current Privacy complaint classifications to maintain relevant statistics and to report specifically on complaints related to Smart meters and breach of privacy. Further, we recommend that the AER review its key performance indicator definitions to ensure that Smart Meters and Privacy concerns will be sufficiently identified and captured by relevant licensed entities.

Further consideration of privacy issues should be undertaken by the AER in future when more detailed complaint and industry audit information becomes available.

Recommendation 15 - Consumer Information

We recommend the following consumer information be developed as to assist customers contracting with unregulated third party providers of services where this involves access to and storage of customers' metering data:

- Publish a list of third party providers who agree to opt in to the NPPs[6]; and
- Develop a standard contract (or standard contract terms) dealing with information privacy protection for the use of consumers entering into arrangements with a third party provider not already subject to any compliance regime.
- Advice regarding complaints and the relevant complaint resolution agency.

Recommendation 16 - Further Privacy Impact Assessment

The Commission recommends that the Department of Primary Industries commissions another privacy impact assessment of the Industry after smart meters have been fully rolled out and operating for five years or sooner if evidence emerges of unresolved privacy concerns.

[6] This could be in the form of a link to the website of the office of the Australian Information Commissioner which maintains a list of organisations (including individuals) that fall outside the legislative requirement of the Privacy Act but have voluntarily nominated themselves as being subject to the Act.

3 Discussion of Lockstep PIA Report Recommendations

This chapter outlines in greater detail the Commission's consideration of the Lockstep Report and industry responses to our Information request.

As previously discussed, the Commission sought industry submissions in relation to the nine critical and 15 other recommendations outlined in the Lockstep Report. Our analysis of the submissions received and our subsequent recommendations are outlined below. A detailed summary of Industry submissions can be found on the Commission's website.

Lockstep PIA Report Recommendation 1

All metering data from or about residential meters should be handled throughout the Advance Metering Infrastructure (AMI) system in accordance with the National Privacy Principles (NPPs), in order to safeguard it against potential abuse, better control future secondary usage by unregistered third party participants, and to more clearly demonstrate to customers and the public that the industry is committed to privacy.

Audits

In keeping with the requirement under NPP4 to keep information secure, the OAIC recommends that businesses undertake regular internal audits to detect system weaknesses and or breaches. In the Commission's view Retailers and Distributors should conduct regular internal audits of their systems, policies and procedures, including as they relate to the handling of Personal Information. Retailers and Distributors that use third party providers that access and store customers' metering data should satisfy themselves as to the scope, completeness and regularity of the training provided by third party providers to their staff.

As with Lockstep, we could not establish whether such audits are regularly conducted and where information about these audits is published, if at all.

While Retailers and Distributors may have adequate internal security systems, staff training and internal audit processes in place, it could be beneficial to ensuring high standards are maintained and enhancing the public's confidence if an independent audit of these matters was also conducted using the methodology outlined by the OAIC. Each company could be required, through regulatory performance or compliance reporting, to publish their audit results in their annual report, on the company website and provide it to the AER. This could be especially important during the period that smart meters are being introduced to allay public concern about inappropriate access to customer data.

The proposed independent audit of Retailer and Distributor security systems, staff training and staff access to their systems and information, as recommended by the Commission, should wherever possible extend to the systems and processes of contracted third party providers, if and where customer data is accessed and/or stored by these.

All industry participants should be audited initially in the period of roll out of smart meters or as soon after, and then as compliance is assured, audits could be limited to those participants who generate a disproportionate number of complaints.

Information Collection

As noted earlier, the Commission could not conclusively determine the level of public concern about the handling of their Personal Information from a privacy perspective. We think it prudent that agencies responsible for handling customer complaints should place a greater focus in their data collection and analysis on privacy issues so that the industry regulators and Government can be better informed about how well Retailers, Distributors and other third party providers are protecting their customers' privacy.

The need for further tightening (or a relaxation) of the initial regulatory approach can be reconsidered if more detailed complaints and audit data reveals an increase in, or absence of, significant consumer concerns after the AMI roll out is completed.

The Department of Primary Industries may wish to commission another privacy impact assessment of the Industry after the smart meter rollout has concluded and has been operating for five years, or when there is more evidence of any actual privacy concerns.

Third Party providers

While licensed electricity Retailers and Distributors can require compliance with NPPs by their contractors through service level agreements or similar contractual arrangements, this framework would not currently apply where the electricity customer chooses directly to contract with an unregulated third party for additional services. The question arises whether unregulated third party providers that access and/or store Personal Information of electricity customers via customers directly should be required to register their business or obtain some form of accreditation[7] so as to be subject to a monitoring and compliance regime.

To obtain this level of surety represents a significant challenge for Government and it could require a substantial allocation of resources to implement a form of regulation and maintain compliance. There could be some tension between a proposal for third party regulation and Government policy to reduce regulatory burden on business and promote competition in the energy sector.

It is difficult to justify the imposition of a regulatory scheme, which in itself would be costly and difficult to effectively implement, without having a clearer idea of the degree of risk to privacy that third party providers may represent.

However, we think that in the interests of consistent treatment of customers 'Personal Information' all third party providers that access and store customers' metering data should be, at a minimum, encouraged to opt-in to

[7] The Energy Network Association discussion paper [March 2012] titled 'ENA Smart Meter Operating Model', notes that the challenges of the current energy market environment can result in increased complexity and/or costs for distributors in maintaining compliance to network functionality, integrity, reliability and security requirements [p2]. Its analysis of emerging products and services under a smart meter model refers to 'accredited parties', including distributors, retailers, customers and third party providers- the latter presumably includes VEET accredited persons but it is not clear whether it is meant to be wider than this [p4]. Clause 3.2 of the related 'Communications and Data Security Protocol Principles', indicates that a consumer or a market participant [a licensed Retailer or Distributor] could authorise a third party to access data [clause 3.2, p11]. The Protocol is designed to cover perceived gaps in communication and data security relating to smart meters.

NPPs and the scrutiny of the OAIC. As Lockstep notes there is provision for small businesses to voluntarily opt-in to the NPPs and jurisdiction of the Privacy Act. We also recommend that the AER considering publishing the names of third party providers who agree to abide by NPPs[8] as a form of 'tick' or approval of such action.

This may still leave those unwilling to take this path outside the scope of the NPPs.

In addition DPI could develop and publicise a standard contract (or standard contract terms) dealing with information privacy protection for the use of consumers entering into arrangements with a third party provider not subject to any privacy compliance regime.

Better collection of data regarding smart meters and privacy complaints would help to inform any future need to move beyond encouragement to some form of accreditation.

We note that the Victorian Energy Efficiency Target (VEET) Scheme, administered by the Commission, requires accreditation of persons used to install In-Home Displays (IHDs). This accreditation process requires Accredited Persons (APs) to attest that they have the means of complying with all relevant laws and guidelines. There may be value in explicitly stating for applicants the particular laws that apply to them. VEET will act as a point of contact for any consumer complaints that may arise from the conduct of APs and so will be in a position to see if further specification or tightening of accreditation processes becomes necessary in the light of experience. We consider that the VEET scheme should also be required to include privacy issues as part of its performance monitoring audit programme. This could become more important if APs in future diversify their business model to provide services beyond mere installation of IHDs.

We also understand that a core service agreement between Distributors and APs includes standard clauses covering privacy among other issues. We envisage that these provisions would clarify privacy expectations placed on APs and provide a means of exercising accountability and compliance over APs for conducting their business within the NPPs.

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.

[8] This could be in the form of a link to the OAIC website, where those who have opted to be covered by the Privacy Act and the NPPs are listed.

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.

Lockstep PIA Report Recommendation 2

Privacy Policies of Distribution Businesses (DBs) and Retail Businesses (RBs) should be reviewed and updated to describe each organisation's commitment to the NPPs, including explanations 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.

There is already a degree of community concern about the introduction of smart meters, and to date little consumer knowledge or experience of the enormous data potential of smart meters. For example, as Lockstep states, ".. *the richness of data can yield information about behavioural patterns within each household* …" and "*smart metering also introduces the theoretical potential for collection of a new instance of Personal Information concerning specific appliances used in the home*".[9]

In view of both of these factors, it would seem advisable to anticipate an increase in consumer concern as knowledge becomes more widespread. Further, it is important to be explicit about these matters in Privacy Policies and Notices so that customers are clear about what they can expect from their Retailer and Distributor and are reassured as to the protection of their information.

Privacy Policies and Privacy Notices could benefit from standardisation in the wording of their provisions at least as they relate to smart meter data (so consumers see it as an industry wide protection) and so that it uses easy to understand wording.

We recommend the development of a commonly worded Privacy Policy (which could be in the form of an Industry Code approved by the OAIC) with standard, plain-English wording and an agreed definition and explanation of secondary uses of personal information. Examples of secondary uses could be listed, according to the current practice of each business, and could include provision to expand as new uses are introduced.

The Privacy Policy should explain 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. In addition, the Privacy Policy should contain contact details for the business, the OAIC and EWOV or its equivalent, to facilitate complaint handling.

An Industry Code could be approved by the OAIC for the whole electricity industry as a means of providing consistent privacy information, to an approved standard across the sector.

As an overarching principle, all Privacy Policies should be made easy to find on websites, be expressed in simple terms and make provision for customers of non-English speaking background.

Third Party providers that voluntarily opt in to the NPPs would be subject to the requirements of the Privacy Act

[9] Lockstep Report, p28

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.

Lockstep PIA Report Recommendation 3

Even though details of how third party services and Home Area Networks (HANs) will operate remain sketchy, it would be appropriate at this stage for RBs' and DBs' Privacy Policies to anticipate the sharing of data beyond their businesses and circumscribe access to metering data. Note that this action should satisfy the ESC's call for "privacy principles" to be developed before In-Home Displays (IHDs) are deployed.

It is evident from submissions that not all industry participants are ready to discuss operational aspects of Home Area Networks and releasing data to third party providers. Generally, we note there is a view that sharing meter data will work within existing privacy considerations provided the customer gives their consent and that third party providers are required to abide by NPPs. As we have already discussed the latter is still problematic in some cases and the former requires some protections or information to assist consumers.

In our view, the possible logistical and privacy difficulties for Retailers, Distributors and customers of sharing interval metering data with third party providers could include:

- Dealing with a large number of third party providers,
- If there is high turnover of this type of business,
- The capacity of small start-up businesses to provide systemic protection of personal information,
- The monitoring of consumer consent arrangements for particular contracts,
- The need for specialist customer service knowledge/staff to handle complex queries or complaints arising from the operation of IHDs and HANs
- The risk to consumers of dealing directly with unregulated third party providers

We agree with Lockstep that smart meter data sharing is qualitatively different from the kind of secondary uses of personal information currently covered by Privacy Policies and Notices. As the technology is highly innovative and lends itself to multiple new uses, and as there is already consumer concern about the new smart meters, we think it advisable to explicitly refer to them in Privacy material and to set common principles for sharing this data such as obtaining explicit customer consent and adherence to NPPs by third party providers wherever possible.

Distributors are anticipating the sharing of data beyond their businesses and are trialling some such arrangements. These arrangements are based on the current roles of Distributors and Retailers and the current rights of customers to access their own consumption data (i.e. customers cannot provide data directly to third parties). Distributors will need to prepare themselves to take on a new customer service role with respect to such

contracts. A further possible complexity could arise after 1 January 2014 if Distributors do not retain an exclusive role for smart meter provision.

The “traditional” model of Retailers dealing directly with customers, (and on behalf of Distributors) will likely have to change to reflect new business opportunities, which may not be embraced willingly by existing industry participants. Retailers and Distributors are especially keen to avoid any potential liability to them should third party providers not abide by Privacy legislation and the appropriate means to manage and indemnify industry participants should be the subject of further consultation.

Jemena noted what it believes is a regulatory constraint requiring approval by the Customer’s Retailer before a customer can access or be provided their meter data (National Electricity Rule 7.7(a)(7)). The Commission understands that DPI has sought legal advice on this issue and is investigating whether there is a need to further clarify the operation of the clause for the purposes of installation of IHDs in Victoria under the Energy Saver Initiative (ESI) scheme.

We note that under privacy guidelines it is recommended that appropriate contract management for contracted functions include conducting due diligence on those companies to who functions are contracted and monitoring compliance with security policies and practices through periodic audits.[10]

Clarity is required as to what extent Retailers and Distributors currently conduct (or should conduct) due diligence and ongoing compliance monitoring on third party providers with whom they currently contract to provide services. We think this is an aspect of privacy management that could be audited independently as per the Commission's view expressed in relation to Lockstep Recommendation 1 above.

The Commission sees no reason from a privacy perspective to continue to circumscribe access to metering data. Diversification of services in the energy sector depends on the capacity of consumers to access their own data and/or provide it to third parties for analysis. Although the Lockstep recommendations identify areas for improvement in the management of Personal Information by Retailers and Distributors, we consider that there is sufficient protection exercised by them and little scope to regulate third party providers with whom consumers may choose to deal. The need for further regulation in this regard may become evident as more experience is gained.

Nonetheless, at present, there is little justification for limiting customer access to their metering data, should they seek it.

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.

[10] Australian Privacy Commissioner, Guidelines section 5.3

Lockstep PIA Report Recommendation 4

The industry should adopt and promote an Opt-In policy of not putting metering data to any secondary purposes without express customer consent.

For the avoidance of doubt, and to maximise consumers' sense of control, such secondary uses should include even those that seem reasonably related to the primary purpose for collection, such as the provision of efficiency advice. The industry should ensure that consent to secondary uses is always freely given, is not conditional, and is never bundled into acceptance of an electricity supply contract.

The AMI Policy Committee should review any suggested exceptions to the Opt-In that might be put forward by Registered Participants, and if agreed, officially specify them.

This recommendation reflects the Lockstep Report's view of the:

> *"generally poor communication to consumers of the privacy realities of smart metering and that a spectrum of privacy anxieties has been allowed to build up in the community, many of which prove to be not substantive, but all of which need to be treated seriously and respectfully".*

In a similar vein, Lockstep notes the Victorian Privacy Commissioner highlighted "*that people are concerned about smart metering representing a sort of intrusion into their homes*"[11]

The responses we received to the Lockstep Report recommendations demonstrate that there is a tension evident between the need to have customer consent to the release of their information, and Industry's desire to make the obtaining of consent as streamlined, inexpensive and unobtrusive as possible.

To mitigate consumers' concerns we think that Retailers and Distributors need to treat the secondary usage of smart meter data as qualitatively different from their use of metering data to date; in other words, as a new product and a new contract with their customers.

The commencement of this new relationship could be at the point customers install or switch on an In-House device and /or bind to a HAN. This would be subject to a final view on whether some current secondary uses of data also require further express consent from customers after they have entered an energy supply contract with the Retailer.

We observe that many (non-energy) purchases now require consumers to give consent in the form of agreement to specific terms and conditions at the point of sale, particularly in the case of use of personal information for secondary purposes. This can be as simple as a check box on a form (such as in the online purchase of an airline ticket). Retailers and Distributors would be able to identify appropriate times within the business

[11] Lockstep Report, p 14

relationship with a customer to obtain explicit consent to the use of the customer's smart meter data for a secondary purpose or purposes.

To comprehensively implement an Opt-In policy would require a clear and common understanding (and listing) of what constitutes a secondary purpose when it comes to the 'Personal Information' collected by Retailers, Distributors and other third party providers. Current Privacy Policies/Statements generally do not refer to metering data at all (although some refer to energy consumption) or subsequently define it as 'Personal Information'.

There may also need to be exceptions arising from other legislative obligations that are explicitly excluded, such as the requirement to monitor consumption data to assist customers experiencing hardship, to ensure supply to customers with medical dependence on life support equipment and to provide energy efficiency advice on customers' bills, and where data is aggregated so that individual customers cannot be identified.

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.

Lockstep PIA Report Recommendation 6

As and when DBs and RBs implement new databases as part of the AMI adoption, they should take care to keep raw metering data (keyed by National Meter Identifier alone) separate from all other identifiable customer records in order to mitigate against ready re-identification. In general it is essential that teams implementing, configuring and maintaining databases are fully aware of the NPPs and the broad legal definition of Personal Information, to help them avoid inadvertent privacy problems.

Industry responses seem to indicate the continuing need to be able to link customer data and relevant personal identifiers to ensure accurate billing. Protection of data relies then on separate but linkable databases, appropriate staff access and appropriately trained staff.

We have not assessed whether record keeping systems of smaller Retailers are sufficiently sophisticated to protect data. We envisage that smaller operators with less sophisticated systems would need to be more diligent about controls and audit trails to minimise any customer detriment.

As part of this review, the Commission has not assessed the records and systems maintained by meter data agents who are contracted to Distributors to read customers' meters but who do not have a direct billing function. If the function of meter data agents is to continue under the Smart Meter Programme, further consideration to determine whether existing accreditation process or audit program in relation to meter data agents are sufficient to manage these concerns is warranted. In the absence of such processes or programs, we recommend that the Government consider the creation of one and determine the most appropriate regulatory framework for that scheme to operate within.

Distributor's submissions have not detailed the regularity of training provided to their own staff or sub-contractors. Nor do they indicate whether regular audits of staff access of customer data are conducted.

Responsibility to ensure AMI data bases are adequate to the purpose of protecting privacy should be exercised by the relevant regulator (for Retailers and Distributors and Accredited Persons), and Retailers and Distributors themselves in the first instance for contracted parties such as meter data agents.

We have previously recommended that audit programs of Retailers and Distributors be examined to establish their regularity and reliability as well as being strengthened by the requirement for an independent audit. Where possible, we also recommend that this incorporate an examination of the systems and processes of related or contracted bodies.

Scrutiny of unregulated third party providers would depend on them becoming subject to some form of accreditation or regulatory oversight. Opting in to the NPPs might provide this framework.

ESC Recommendation 5

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

Lockstep PIA Report Recommendation 8

Consideration should be given to clarifying what meter data may be (or should be) disposed of after seven years. From a privacy perspective, unless there is a clear reason to retain fine grain interval data at each Participant, it should be destroyed, or aggregated to the greatest reasonable extent.

Current standards and practice generally relate to meter data that has historically been collected on a 3 monthly basis. Retailers noted that they are obliged to retain data records for specified periods to settle long standing individual billing disputes and to provide historical billing information to customers. Distributors highlighted the need to retain this data, not only for market settlement purposes but also to enable long term network planning to be undertaken.

There are likely to be significant costs incurred by industry as they augment their existing databases and data retention systems to manage the increase in AMI data.

Retailers may be looking for ways to remove a very large volume of data from their databases rather than store it.

Presumably, the vastly increased volume of data (interval data is collected every 30 minutes) could be aggregated and made anonymous after a reasonable period of time.

We note that network planning purposes can likely be addressed by data that does not identify customers, so provided industry anonymises the data, as suggested by Lockstep, the risks of customer detriment would seem minimal.

Data retained in In-Home Devices will need to be separately regulated. This is discussed further in Lockstep PIA Report Recommendation 21.

Although we see the retention of data as largely the business of industry (subject to regulatory constraints), the Commission thinks there could be capacity to aggregate fine grain interval data to protect privacy and that it may not strictly be necessary for all Participants to store data long term for network planning purposes.

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.

.

Lockstep PIA Report Recommendation 14

Review “Privacy Notices” provided to smart meter customers— whether they be explicit or implicit (as is often the case where passages of legal text are incorporated into other customer communications) — and ensure that the notices properly anticipate the potential secondary uses of metering information (such as providing energy efficiency advice direct to consumers, supporting third party services on an opt-in basis and so on).

As previously noted, we recognise that Privacy Policies would benefit from standardisation of wording and many Retailers’ Policies need to be made much easier to locate online. Presumably this would also apply to specific Privacy ‘Notices’ provided to smart meter customers.

To enable easy updating of Policies to reflect new and changing secondary data uses, we recommend that Retailers consider making their Privacy Policy primarily available in electronic form, with print versions provided on request. In addition, welcome pack information, Customer Charters and Terms and Conditions documentation could also refer customers to the retailer’s website. We note that potential AGL customers can already view the Privacy Policy as part of its online sign up process.

See also comments and recommendation in relation to Lockstep PIA Report Recommendation 2 above.

Lockstep PIA Report Recommendation 15

Consider developing a common skeletal layered Privacy Notice[12] that all organisations involved in AMI can use as a basis for their own notices, setting out the industry's regulatory protections, the reasons and uses for smart meter data collection, and the controls that consumers have over how meter data is used.

We agree that the introduction of smart meter technology and the related information uses provides an opportunity to improve this aspect of industry information. Consideration of an industry wide standard to reassure customers and show industry's responsiveness to customer concerns is warranted. Such a response by industry may be vital to ensuring the smooth and enthusiastic uptake of the new technology.

There is substantial support amongst Retailers, and less support from Distributors, for a standardised approach to informing customers of their privacy rights and obligations. Industry is concerned to be involved in the development of any such 'Privacy Notice' and to ensure its consistent use across all jurisdictions. The Commission recommends that any such approach is undertaken as part of the National Smart Metering Program.

We recommend that industry develops a common layered privacy notice that can be used as the basis for all organisations involved in AMI. Further, there is the scope for industry to consider developing an Industry Code to be approved by the Privacy Commissioner.

See also comments and recommendation in relation to Lockstep PIA Report Recommendation 2 above.

[12] A layered format offers layers of greater or lesser detail so people can read as much as they wish and find what they need fast.

Lockstep PIA Report Recommendation 16

Require that small Retail Businesses that might otherwise fall below the Small or Medium Enterprise (SME) criterion for the Privacy Act expressly opt in to the NPPs with the Office of the Privacy Commissioner.

Under certain circumstances, a business with an annual turnover of less than $3 million is exempt from compliance with the Privacy Act. However, they may elect to opt in to the NPPs. Lockstep Report has recommended that energy retailers with the exemption be required to "expressly opt in" to the NPPs.

We agree that small electricity retailers should be under the same obligation as larger Retailers to protect customer data.

The Commission would also prefer that the same privacy requirements apply to all parties that offer services whereby they access customer meter data, irrespective of any existing exemptions based on turnover or other considerations. As we have discussed earlier, we do not see this being achieved for currently unregulated third parties by the introduction of an accreditation scheme.

Whether coverage under the NPPs can be achieved for small retail businesses or third party providers depends on how it can be enforced and by whom. It may not be possible to 'require' otherwise unregulated businesses to opt-in to what is essentially a voluntary commitment to adopting the NPPs made possible by the OAIC.

To make coverage of small businesses mandatory under Privacy legislation would require amendment to the National Privacy Principles, or the Privacy Act, which would need to be undertaken at a State and Federal Government level. This would surely bring unintended consequences for other small business and is most unlikely to be acceptable as a regulatory solution to the matter of making third party providers in the energy industry accountable. However, we accept that it could be made a condition of authorisation for small electricity Retailers that they opt into the OAIC voluntary scheme.

Third Parties that voluntarily opt in to the NPPs become subject to the jurisdiction of the Privacy Commissioner, and would be required to conduct their business in accord with the NPPs and able to have privacy complaints heard against them by the OAIC. They also receive the benefit of being listed on the OAIC website as a business concerned to protect their customers' privacy. The AER could make reference to these third party businesses on its website with a link to the list of names on the OAIC website. However, in the absence of any obligation to opt in, this would remain a potentially high risk area that should be monitored, and if necessary reviewed in the light of experience. See ESC Recommendation 13.

It would also seem reasonable that should this Lockstep recommendation be implemented, that parties contracted to Retailers and Distributors should have those contracts terminated for systemic and unresolved breaches of privacy contract terms.

We note that the broad existing obligation for Retailers and Distributors to ensure that they operate within the law will be retained as part of the transition to the National Energy Customer Framework. This obligation puts some onus on them to ensure their contractors operate within the law. As we have noted previously, the adequacy of existing industry compliance monitoring systems and processes to adequately monitor performance of their

contractors in this regard should be reviewed to provide a higher level of assurance to consumers and Government.

In the absence of any specific regulatory framework that applies to contractors or third parties, we recommend that the relevant industry regulator (either the AER or OAIC) be empowered to take enforcement action should Retailers and Distributors not monitor their contractors' compliance. If not already explicit, this obligation should be incorporated into industry licensing or authorisation processes.

See also comments and recommendation in response to Lockstep PIA Report Recommendation 1 above.

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.

Lockstep PIA Report Recommendation 17

Consider industry-wide minimum security policy settings for protecting interval data against misuse, including the following possibilities:

- DBs should quarantine all data containing customer names from raw interval data
- DBs and RBs should audit log all access by users to interval data
- Retained interval data aged between two and seven years should be subject to more limited access rights than more recent data that might be needed to resolve billing issues.

Given the fine detail and tremendously increased volume of smart meter interval data (collected every 30 minutes as distinct from the current 3 monthly collection), some aggregation and ring-fencing after a reasonable period of time would seem desirable provided it didn't interfere with billing requirements. It would also seem warranted to protect data that may reveal individual household consumption patterns, which may be perceived as intrusion into household privacy.

It is unclear to us whether Retailers and Distributors have anticipated the greatly increased volume of interval data as posing any significant challenges for their data access audit systems in the future, and whether their systems are sufficiently adaptable enough to cope with future demands. We agree with Lockstep that the " *presence of detailed interval data will provide new opportunities for criminal abuse by a rogue insider and even ad hoc access to records out of curiosity by the odd unscrupulous staff member*".

Care is needed to restrict access to interval data on a need to know basis and it becomes more important to be able to audit for potential misuses of customer information.

We cannot determine whether Industry anticipates their current data access audit methods will be adequate for the greatly increased volume of interval meter data. In our experience, such assurance could be obtained through audits or through analysis of complaints data, both recorded by industry or by the relevant customer dispute resolution agency.

We envisage that the volume of data and safe retention will be an issue for all parties.

Staff access to retained interval data is the responsibility of business to manage according to the NPPs. We see this aspect of data management as also being subject to our audit recommendations.

We recommend that any current regulatory obligation to retain and provide data to the market should be clarified by the AER in terms of time frame and detail having regard to the new circumstances presented by smart meters.

See also comment on Lockstep PIA Report recommendations1 and 8 above.

Lockstep PIA Report Recommendation 19

In order to give consumers access to their interval data (as required by the Access & Correction Principle NPP 6), protocols should be developed for providing data in standard formats such as Excel spread sheets.

In our view, Retailers and Distributors currently seem to be well able to service current customer information needs, although we note that at present this is on a much smaller scale than could be anticipated when the smart meter roll out and related devices is completed. Additionally, it is expected that, based on historical relationships between customers and retailers, the bulk of customer queries would be handled by Retailers in the foreseeable future.

There is more work to be done to develop and improve forms of assistance to customers to understand interval data. Some Distributors will need to consider the extent to which they wish to provide assistance directly or leave this work to Retailers or other third party providers. This type of assistance could be a distinct selling point for smart meters from the customer's viewpoint. Clearly this is a point of potential difference for consumers, i.e. consumers will actively seek out the most concise, logical, simple displays of AMI data and technical assistance.

The Commission expects that provision of data will need a variety of standardised formats as the demand for it increases with widespread roll out of smart meters and related devices.

There is value in the development of a minimum industry standard for data provision with respect to smart meter interval data, while permitting quality and variety of customer service to flourish as a commercial point of difference between participants in the electricity industry.

In consultation with industry stakeholders, Government or the relevant regulatory agency should undertake the development of standard information and explanatory materials to assist consumers in deciphering AMI data. This could be drafted by an Industry body and reviewed by Government to ensure it is does not conflict with its broader competitive market goals and then published on relevant State and Federal Government websites.

Customer detriment arising from the potential mishandling of information requests will to some extent be addressed through the jurisdictional Ombudsman schemes. Retailers and Distributors will therefore have some financial and reputational incentive to ensure that requests for information are handled well and that their customers are satisfied.

Affording customers access to their own data also opens up the possibility of them dealing directly with Distributors, Retailers or third parties as they choose. Information flows and processes should reflect this and not restrict or inhibit customers' capacity to obtain their data.

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.

Lockstep PIA Report Recommendation 20

In order to boost consumer confidence in the security of the system, DPI should consider commissioning an independent Threat & Risk Assessment (TRA) of any new online portals.

We consider that website portals should apply industry best practice standards and that these portals are demonstrably adequate to support a new range of uses that flow from accessing smart meter data online and to protect the data so accessed.

We note that the Energy Networks Association (ENA) has developed draft guidelines for portals delivered over public networks like the internet[13]. It sees security testing [for example: penetration testing, vulnerability scanning, source code review or equivalent] on the web server and its related infrastructure as highly critical prior to release with ongoing security testing on an annual basis and/or after any significant code or web infrastructure change.

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.

.

[13] Clause 4.7 of Draft SMI Communications and Data Security Protocol Principles, March 2012

Lockstep PIA Report Recommendation 21

Protocols will need to be developed for preventing old occupants from still having access to and/or control over the HAN after they vacate premises.
Ideally, when a smart meter's customer changes, there should be an automatic unbinding of devices from the HAN, and the access code for establishing a HAN on that meter should be changed. It may be prudent to amend the NECF or NER to legislate these measures.

The Commission considers that it will be essential to clarify the respective roles of Retailers, Distributors and third party providers to protect customer meter data at the time of unbinding or disconnecting an In-Home Display from a Home Area Network (HAN).

We note the work done in March 2012 by the Department of Primary Industries in anticipation of regulations coming into effect 1 March 2012 – the provision of IHDs to consumers as prescribed activity in the ESI scheme.

For the purposes of this review the main aspects of the DPI work are:

- The development of core service agreements between Distributors and Accredited Persons. The latter will install IHDs and provide some information to customers about their operation. These service agreements will contain common terms including terms relating to privacy.
- The proposed short term and long term processes for unbinding from the HAN.

We note that DPI has received advice on the issue of potential wrongful access of a previous customer's meter data stored in an IHD or smart meter when a former occupant vacates their premises[14]. In the short term this advice is that customers should have responsibility to erase the IHD of all historical information if they wish to leave behind their IHD. Longer term Industry controlled solutions to unbinding IHDs from the HAN when a customer vacates are referred to the National Smart Metering Program (NMSP) to determine. Similarly, unauthorised access to historical meter data held in a smart meter is referred to the NSMP to resolve.

The Victorian Energy and Efficiency Targets(VEET) Scheme has also placed obligations on Accredited Persons when installing IHDs to tell customers that their meter information is Personal Information (in terms of the Privacy Act), to inform them about how data is stored in their meter and how it can be managed. Customers will need to acknowledge at the point of installation that they have received and understood this information

The extent for potential consumer detriment arising from unauthorised access to meter data via an IHD is not clear. We think it may be unreasonable to expect some customers to be able to, or to remember to, purge their data, or to take their IHD with them.

Therefore, we recommend that a mechanism for unbinding from the HAN that does not solely rely on customers purging their own data or remembering to remove their IHD before vacating be developed.

[14] This advice is contained in a report prepared by Accenture Management Consulting for the Department of Primary Industries, 14 March 2012

As an alternative, steps should be taken to remind customers of the need to unbind/purge information from their IHD at a number of points during the life of the contract. This could include when customers move in and move out, and when an IHD is installed, serviced or relocated.

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.

Lockstep PIA Report Recommendation 22

When the BPPWG comes to develop business processes and protocols for HAN activation, it should enact the Opt-In policy of Recommendation 4 above (to be confirmed) that all secondary uses of metering data shall be subject to express consent. Further, the BPPWG should consider enforceable requirements that data is handled across all HANs in accordance with the NPPs.

In our view the sensitivity in the community toward smart meters warrants a cautious approach to assuming that customers have adequately consented to the myriad possible uses of their data on a one time basis. This is particularly the case where new uses of data may arise over time.

We also note the VEET accreditation process for Accredited Persons and the core service agreements between Distributors and Accredited Persons. Although Distributors could end an agreement with an Accredited Person found to be in breach of their contract, we think it would be useful if there was provision to suspend and ultimately cancel accreditation for repeated breaches of privacy laws by Accredited Persons.

We recommend that 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. This work should be undertaken as part of the National Smart Metering Program.

Enforcement will also depend on the nature of the regulator's relationship with the person using the customer's data. This is presently clear in the case of regulated participants and service providers with whom they may contract, nonetheless, there may be some further regulatory audit required to confirm compliance by regulated entities.

The Commission's previous recommendations in response to PIA Recommendations 1, 2, 14 & 15 are relevant in this regard.

The capacity to enforce an Opt-In provision is much less clear in the case of completely unregulated third party providers. As discussed previously, we recommend that unregulated third party providers be encouraged to opt-in to coverage by the NPPs. The need for further regulation could be reviewed in light of experience with the smart meter programme.

We also see value in the provision of some other structured form of information or support for customers.

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**).

Lockstep PIA Report Recommendation 23

If in future individuals within a household enter into third party contracts relating to use of smart meter data, such contracts should be signed by both the individual and the main electricity account holder.

We can see that this proposal would currently be difficult to implement while protecting the Personal Information of the account holder/customer and without significant amendment to existing contractual relationships and documentation. Indeed it would require disclosure of that information to a third party. Nonetheless, we can see that the information about consumption would likely belong to other persons in a household who contribute to that consumption (and possibly also toward payment of the account). It is not contemplated that an account holder's/ customer's information would be given without their consent. Other potential uses of detailed consumption data in the future could be possible and viewed as desirable by account holders and other individuals within a household. In our view, Lockstep's recommendation seeks to respond to innovation without compromising customer privacy.

This is an emerging issue, the implications of which may not become apparent for some time. Pressure could come on a Retailer to act (beyond the mere giving of agreed metering data information) at the request of someone other than the account holder. It could add a layer of complexity to Retailer's record keeping which in turn could lead to mistaken disclosure of some kinds of information. Retailers would be reluctant to expose themselves to the potential consequences of wrongful disclosure of information.

Government and the relevant regulatory agencies would need to consider whether a completely new form of contract is required given the type of service envisaged and what the complexities and risks of taking the proposed approach could be. There are likely to be significant costs associated with any change and we would recommend that a detailed cost benefit analysis be undertaken.

Ongoing discussions are required to develop a framework to ensure that contractual arrangements remain relevant, viable and enforceable as new products are developed.

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.

Lockstep PIA Report Recommendation 24

The ESC should amend the wording of its decision to refer to Privacy Policies or Codes, rather than "Privacy Principles" because the latter term has a technical meaning in legislation.

The responses from Retailers are noted and the matter will be further considered by the Commission.

While this may have been preferable wording, we would note that any amendment to previous Commission decisions may have unintended outcomes particularly given the transfer of retail regulatory functions to the Australian Energy Regulator in July 2012.

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