



Dept of Primary Industries

PIA Report

Advanced Metering Infrastructure (AMI)

Version 1.2

Lockstep Consulting
August 2011

Consulting report
PIA Report
Version 1.2
For Dept of Primary Industries
[Lockstep DPI AMI PIA Report (1.2.1).docx]

PUBLIC

*Lockstep Consulting (est. 2004) provides independent research, analysis and advice on digital identity, privacy, cyber security policy and strategy, and e-business risk management.
Contact swilson@lockstep.com.au.*

Table of Contents

EXECUTIVE SUMMARY	4
GLOSSARY	6
TECHNICAL TERMS.....	6
ABBREVIATIONS.....	6
INTRODUCTION	9
SCOPE & DELIVERABLES	9
METHODOLOGY	10
STAKEHOLDER MEETINGS	10
TERMS OF REFERENCE.....	13
PART 1: DESCRIPTION OF THE PROJECT	15
OVERVIEW.....	15
PART 2: INFORMATION FLOW MAPPING	19
INFORMATION FLOWS	19
COLLECTION OF PERSONAL INFORMATION AND METERING DATA	21
USE OF METERING DATA	22
DISCLOSURE OF METERING DATA.....	23
PART 3: PRIVACY ANALYSIS	24
ON <i>PERSONAL INFORMATION</i>	24
ON “OWNERSHIP” OF INFORMATION.....	25
PERCEIVED PRIVACY PROBLEMS.....	25
PRIVACY POSITIVES OF THE PROGRAM	26
PRIVACY CHALLENGES	28
OTHER HIGH LEVEL PRIVACY ISSUES	30
PART 4: PRIVACY MANAGEMENT	34
PART 5: RECOMMENDATIONS	51
A SUMMARY OF FINDINGS	51
SUGGESTED PRIVACY CONSIDERATIONS FOR DPI AND THE INDUSTRY.....	52
SUGGESTED PRIVACY CONSIDERATIONS FOR DISTRIBUTION BUSINESSES	53
SUGGESTED PRIVACY CONSIDERATIONS FOR RETAIL BUSINESSES	53
SUGGESTED PRIVACY CONSIDERATIONS FOR FUTURE THIRD PARTIES	53
THE CRITICAL RECOMMENDATIONS	54
OTHER RECOMMENDATIONS	55
REFERENCES	58
A.1 PROJECT DOCUMENTS	58
A.2 EXTERNAL DOCUMENTS.....	58
A.3 OTHER SOURCES.....	60
APPENDIX: NATIONAL PRIVACY PRINCIPLES	61
NPP 1 COLLECTION.....	61
NPP 2 USE AND DISCLOSURE	61
NPP 3 DATA QUALITY	62
NPP 4 DATA SECURITY	62
NPP 5 OPENNESS	63
NPP 6 ACCESS AND CORRECTION	63
NPP 7 IDENTIFIERS.....	64
NPP 8 ANONYMITY	65
NPP 9 TRANSBORDER DATA FLOWS	65
NPP 10 SENSITIVE INFORMATION.....	65

Executive Summary

Lockstep Consulting was engaged by the Department of Primary Industries to undertake a Privacy Impact Assessment (PIA) of Victoria's Advanced Metering Infrastructure (AMI) or "smart metering" program.

The scope of this PIA is the smart metering program in general, with the objective of establishing whether the program as overseen by DPI has 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, including the governance of new controls yet to be developed for potential broader usage of power consumption data.

This PIA is not an assessment of the privacy compliance of any particular organisation involved in the AMI program.

The PIA uncovered no collections, disclosures or other flows of Personal Information concerning consumers that would go beyond the AMI's legitimate purposes. We see no need for any operational changes to the way electricity retailers, distributors and AEMO handle information flows. Security is generally very good, as required by Essential Services Commission licensing, the National Electricity Rules and the Minimum AMI Functionality Specification, and there are high expectations of confidentiality imposed by industry codes. Technical security standards and conservative default settings mean that inadvertent privacy risks with Home Area Networks (HANs) such as exposure to drive-by snooping are unlikely. Business processes are not yet in place for the widespread establishment of HANs from smart meters, and it will be some time before they are, but these will have to recognise and address potential privacy concerns.

Yet the broader concerns of privacy—most notably openness about use and disclosure, and the choices that consumers will have to control secondary usage under a future AMI environment—are not well ingrained across the electricity industry. Relatively little public information has been made available about smart meters. A range of community concerns abound and some of them are warranted. While many of the public's anxieties exceed the actual risks of privacy invasion, a much improved program of communications aimed at consumers and the general public is recommended. Communications to date have been limited to the mechanics of the meter rollout, and have done little to allay concerns relating to the broader sharing of metering data that will be made possible in the medium term. We recommend a fresh set of messages be designed by a reenergised AMI Communications Working Group, covering the reality of smart metering information flows, the limited extent to which they reveal behavioural patterns within households, and the choices that consumers have to control them. The sheer volume of meter data being

retained now for many years should be reviewed, with consideration given to de-identification, aggregation and/or earlier deletion if there is not a compelling business need to retain all raw data well beyond two years.

We recommend that all metering data should be handled in accordance with the National Privacy Principles (NPPs). Regardless of any fine arguments about whether metering data technically counts as *Personal Information*, committing to and applying the NPPs will set a uniformly high standard of care, commensurate with the community's broad anxieties about smart metering, and with the future potential value of the data.

All Retail Businesses and Distribution Businesses should review and update their privacy policies in this light, to articulate how they understand their obligations under the National Privacy Principles. Distribution Business especially should note that the legal definition of *Personal Information* is broader than customer records and the like. It appears that materials given to consumers to date have not included much information about the primary purpose of collecting smart meter data and the potential for secondary usage of the data. Nor has the industry clearly communicated the many safeguards that are already in place to protect consumer privacy, such as the National Electricity Rules, the ESC licence conditions and the ESC's codes. All organisations handling metering data should therefore review and update their "Privacy Notices" or any other explanations provided in customer information about how their data is handled. The complexity and depth of metering information means that *layered* privacy notices are advisable.

The electricity industry anticipates a great deal of innovation to be enabled by smart metering, with many new services to help consumers better manage their energy efficiency, and the emergence of new third party services. Such rapid changes coming on the heels of the physical meter rollout may create further anxieties. Looking ahead, we believe the industry needs to do more than improve the way it explains these developments. To demonstrate good faith to consumers and the public, we recommend that the industry commit to an Opt-In model, such that secondary usage of smart meter data, to the greatest practical extent, is only made with express consent of the customer.

In summary, the present privacy shortcomings of the AMI program may be addressed by updating Privacy Policies, refreshing and extending customer communications, committing to the National Privacy Principles, and committing to an Opt-In model for managing secondary use of metering data. None of these recommendations should mean immediate operational changes, and no privacy response will change the license conditions of any Registered Participants. In the medium term, an Opt-In model will influence the design of business processes for HAN activation and for other sharing of metering data with third parties.

Glossary

See also <http://share.aemo.com.au/smartmetering/Pages/Glossary.aspx>.

Technical terms

Personal Information According to the Privacy Act 1988 (Cth) personal information means “*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*” [13].

ZigBee A special purpose wireless communication protocol developed for the secure networking of devices such as medical equipment and “smart” home appliances. ZigBee is the protocol of choice for Home Area Networking. It is separate from and not interoperable with the better known “wifi” wireless protocol for computer networking, and is generally rather more secure.

Abbreviations

AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AMI	Advanced Metering Infrastructure <i>That is, the Victorian smart metering program.</i>
BPPWG	Business Process & Procedures Working Group <i>of the national smart metering program.</i>
COTA	Council on the Ageing
CUAC	Consumer Utilities Advocacy Centre
DB	(Electricity) Distribution Business
ENA	Energy Networks Association <i>Peak national body for gas and electricity distribution businesses.</i>
ERAA	Electricity Retailers Association of Australia <i>Independent association lobbying in the interests of national RBs.</i>
ESP	Energy Services Portal <i>A data structure and interface contained in the smart meter, and specified by the ZigBee standards, which controls what information can be exchanged over the HAN.</i>

ESC	Essential Services Commission <i>Licenses Victorian electricity market participants and develops/administers industry codes.</i>
FAQ	Frequently Asked Questions
HAN	Home Area Network <i>A special type of local area network where a smart meter is connected over the wireless "ZigBee" protocol with other devices such as an In Home Display and "smart" appliances.</i>
IHD	In Home Display <i>A domestic device connected to a smart meter (typically by the special purpose wireless ZigBee protocol) for showing electricity consumption data in various formats.</i>
IPPs	Information Privacy Principles <i>As laid down for example by the Victorian Information Privacy Act or separately by the federal Privacy Act for government bodies. Not applicable to Victoria's privately owned DBs and RBs.</i>
LAN	Local Area Network
MDA	Meter Data Agent
MDM	Meter Data Management system
MDP	Meter Data Provider
NBN	National Broadband Network
NECF	National Electricity Consumer Framework
NEM	National Electricity Market.
NMI	National Meter Identifier
NSMP	National Smart Metering Program
OPC	Office of the Privacy Commissioner (federal)
OVPC	Office of the Victorian Privacy Commissioner
NER	National Electricity Rules
NPPs	National Privacy Principles <i>As laid down by the private sector provisions of the federal Privacy Act [XXX REF] and applicable to privately owned large businesses such as Victoria's DBs and RBs.</i>
PAN ID	Personal Area Network Identifier <i>The ZigBee network identifier for a HAN hub (such as a smart meter) akin to a wifi network SSID.</i>
PI	Personal Information
PIA	Privacy Impact Assessment
PSM	Protective Security Manual <i>The Commonwealth's 'bible' for securing information, personnel and physical assets.</i>
RB	(Electricity) Retail Business
RoLR	Retailer of Last Resort

SEP	Smart Energy Profile
SME	Small or Medium Enterprise <i>Businesses turning over less than \$3M p.a. are generally not required to comply with the NPPs.</i>
SMI	Smart Metering Infrastructure <i>Technically equivalent to “AMI” and used more in the National Smart Metering Program.</i>
SSID	Service Set Identifier <i>The public name for a wifi network, visible to devices trying to connect to the network.</i>
TOU	Time Of Use [pricing]
TRA	Threat & Risk Assessment <i>A formalised methodology for analysing the potential security threats to a system, and gauging their seriousness as a function of expected likelihood and severity of all foreseeable adverse events.</i>
WAN	Wide Area Network

Introduction

Scope & Deliverables

This PIA was conducted on behalf of DPI in order to ascertain the overall state of consumer privacy protection within the AMI program, in parallel with the broader program reviews being undertaken by the new state government. The contracted PIA was required to deliver the following:

1. *Project description: Broadly describe the project, including the aims and whether any personal information will be handled.*
2. *Mapping the information flows and privacy framework: Describe and map the project's personal information flows and document all relevant legislative and organisational rules.*
3. *Privacy impact analysis: Identify and analyse the project's privacy impact.*
4. *Privacy management: Consider how to manage any privacy impact, particularly options that will improve privacy outcomes and still achieve the project's goals.*
5. *Recommendations: Produce a final PIA report covering the above stages and including recommendations.*

This report is structured accordingly.

This PIA is not a detailed assessment of the privacy compliance of any particular organisation involved in smart metering. It may be the case that electricity distributors and retailers will undertake separate PIAs of their respective businesses, in the same way as they undertake their own security evaluations. Moreover, our investigation of privacy and security practices at various participants was limited to relatively short interviews, to attain a general understanding of how RBs and DBs work with customer data across the board. We have had to generalise to a significant extent about security and customer service practices. We have tried to make clear in this report where we make assumptions and where such assumptions should be substantiated by further investigation.

The PIA was focused on the *difference* to privacy made by introducing smart metering. We do not seek to pass judgement on the privacy arrangements for customer data collected from older "accumulation" ("spinning disk") meters, nor to any other data handled by businesses.

The PIA does attempt to anticipate (as best we can at this stage) privacy issues arising in the medium term, when Home Area Networks (HANs) come to be activated, and when power consumption data may start to be shared with third parties which are not currently Licensed Participants.

Methodology

This PIA was conducted primarily by means of desk top review of business analysis and technical documents and in-person interviews with selected stakeholders.

In summary, the desk top review covered:

- AMI project documentation
- NSMP project documentation
- Customer communications of the DBs and RBs
- ZigBee technical specifications
- ESC regulations and codes
- the National Electricity Rules (particularly chapter 7)
- selected stakeholder submissions to AMI program reviews.

The full list of documents in the desk-top review appears in the References section.

Stakeholder meetings

We conducted two waves of focused stakeholder meetings as detailed in the table below, in order to understand the AMI program from all angles, and to collaboratively explore and uncover privacy issues. The first wave of meetings (June 21-22) was with individuals for the most part selected by DPI to give us a fast start to the investigation stage, including consumer groups and advocates. We met informally¹ with members of the Energy Networks Association (ENA) and the Electricity Retailers Association of Australia (ERAA) to discuss broad industry issues. During the first visit we were also able to make a few additional ad hoc appointments. The second wave (July 11-12) was an attempt to engage with a fuller and more representative set of industry stakeholders.

Date	Interviews
9 June	PIA engagement kickoff (tele conference) <ul style="list-style-type: none"> — Eleanor McCracken-Hewson — Graham Dawson — Peter Clements — Stephen Wilson, Anna Johnston

¹ These meetings were “informal” in the sense that they were not conducted on the basis of anyone claiming to represent the official views of the respective associations. Rather, individuals were senior players in the industry and could be relied upon as authoritative insofar as they are deeply informed by the perspectives of retail and distribution business.

21 June	Orientation meeting (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Eleanor McCracken-Hewson — Graham Dawson — Peter Clements — Stephen Wilson, Anna Johnston
21 June	Technical briefing (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Stephen Thompson — Eleanor McCracken-Hewson — Stephen Wilson, Anna Johnston
21 June	Consumer group briefing (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Janine Raynor – Consumer Action Law Centre — Eleanor McCracken-Hewson — Stephen Wilson, Anna Johnston
22 June	Informal ENA briefing (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Patrick Murphy – SP AusNet — Kevin Webster – United Energy Distribution — Verity Watson – United Energy Distribution — Eleanor McCracken-Hewson — Stephen Wilson, Anna Johnston
22 June	Informal ERAA briefing (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Martin Excelby – Red Energy — Eleanor McCracken-Hewson — Stephen Wilson, Anna Johnston
22 June	Marketplace briefing (AEMO, 530 Collins St.) <ul style="list-style-type: none"> — John Wiskin – AEMO — Eleanor McCracken-Hewson — Stephen Wilson, Anna Johnston
22 June	Consumer group briefing (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Craig Memery – Alternative Technology Association — Eleanor McCracken-Hewson — Stephen Wilson
23 June	Retailer meeting (Lumo, 575 BourkeSt.) <ul style="list-style-type: none"> — Ross Evans – Lumo Energy — Stephen Wilson
11 July	Consumer group briefing (98 Elizabeth St.) <ul style="list-style-type: none"> — Debra Parnell – Council of the Ageing — Stephen Wilson, Anna Johnston
11 July	AMI management briefing (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Peter Clements — Stephen Wilson, Anna Johnston
11 July	Retailer meeting (DPI, 1 Spring St.) <ul style="list-style-type: none"> — Alex Cruikshank – AGL — Stephen Wilson, Anna Johnston

11 July	Retailer meeting (DPI, 1 Spring St.) — Fiona Simon – Origin — David Calder – Origin — Stephen Wilson, Anna Johnston
11 July	BPPWG briefing (AEMO, 530 Collins St.) — Shaun Dennison – BPPWG — Stephen Wilson, Anna Johnston
12 July	Retailer meeting (tele conference) — Stuart Pearce - TRUenergy — Stephen Wilson, Anna Johnston
12 July	Consumer group briefing (172-190 Flinders St.) — Jo Benvenuti – CUAC — Deanna Foong – CUAC — Stephen Wilson, Anna Johnston
12 July	Follow-up technical questions(DPI, 1 Spring St.) — Stephen Thompson — Stephen Wilson, Anna Johnston
12 July	Regulatory meeting (ESC, 35 Spring St.) — Jeff Cefai – Essential Services Commission — Phil Warren – Essential Services Commission — Peter Clements — Stephen Wilson, Anna Johnston
20 July	Regulatory meeting (OPC, Sydney) — Timothy Pilgrim – Privacy Commissioner — Alison Nesbit – Office of the Privacy Commissioner — Stephen Wilson

On July 27 we convened a three hour workshop in Melbourne with a wide range of stakeholders, to present interim findings and to discuss the ramifications of our initial recommendations. Attendees were as follows:

Eleanor McCracken Hewson	Department of Primary Industries
Graham Dawson	Department of Primary Industries
Peter Clements	Department of Primary Industries
Michael Stoyanoff	Department of Primary Industries
Paula Cosgrove	Department of Primary Industries
Stephen Wilson	Lockstep Consulting
Peter Wallace	Citipower /Powercor
Bob Bosler	AEMO
Jason Forte	Privacy Victoria
Tim McCoy	GE Energy
Miguel Brando	GE Energy
Sallie Proctor	AGL Energy Limited
Judy Anderson	Smart Grid Australia
Simon Vardy	Smart Grid Australia
Pia Herbert	Department of Business and Innovation

Alan Love	Simply Energy
Neil Bryden,	DiUS
Clency Coutet	DiUS
Louizanne Diaz	Neighbourhood Energy Pty Ltd
Stephen Major	United Energy and Multinet Gas
David Calder	Origin Energy
Jo Benvenuti	Consumer Utilities Advocacy Centre
Stephen Grant	Red Energy
Chris Logie	Energy and Water Ombudsman of Vic
Susan Streeter	Energy Networks Association
Shane Fairlie	Jemena
Caroline McGeechan	Australian Power & Gas
Yann Burden	Billcap
Nabil Chemali	Jemena
Janine Rayner	Consumer Action Law Centre
Phil Waren	Essential Services Commission
Craig Memery	Alternative Technology Association
Dean Lombard	Victorian Council of Social Service
James Harris	SMS Management & Technology
Gary Campanella	AMI Program Office

Terms of reference

The primary terms of reference for this PIA are the National Privacy Principles (NPPs), based on the fact that in Victoria all DBs and nearly all RBs are large privately owned enterprises. There are two types of exception to this rule.

Firstly, it is possible that the very smallest electricity retailers fall below the annual revenue limit that defines small-to-medium enterprises (namely \$3M p.a.) which are exempt from the Privacy Act. While it is expected that any viable RB would generate revenues in excess of \$3M eventually, it may be prudent during the early stages of such a business to clarify that it is expected to comply with the NPPs. One way to ensure this is for small retailers to expressly opt in to be bound by the NPPs, as can be done at <http://www.privacy.gov.au/business/small/opting>.

Secondly, the ownership of one RB—namely Red Energy—may be traced back to state governments via Snowy Hydro Limited. This means that Red Energy is neither a private business nor a federal government agency, and thus it falls outside the jurisdiction of federal privacy legislation. Nevertheless, we note that both Red Energy and Snowy Hydro have committed themselves to the NPPs:

Red Energy is committed to compliance with the laws that protect your personal information, including the Privacy Act 1988 and the National Privacy Principles
<http://www.redenergy.com.au/page.html?privacy> accessed 6 July 2011)

Snowy Hydro Limited is committed to complying with the National Privacy Principles set out in the Privacy Act 1988 (Cth)

<http://www.snowyhydro.com.au/utility.asp?pageID=7> accessed 6 July 2011.

We occasionally make additional reference to the Victorian Charter of Human Rights & Responsibilities, for it includes obligations with respect to individual privacy. Technically, the Charter only applies to the government of Victoria and not to private industry, yet because smart meters are mandated by government, there is an argument that the Charter may be relevant. We also note that the Victorian Privacy Commissioner made mention of the Charter in her submission to the ESC review [8] when she highlighted that people are concerned about smart metering representing a sort of intrusion into their homes. If the Charter does not hold sway formally, it still acts as a useful benchmark.

The Victorian Human Rights Commission notes that:

The Charter ... requires that the Victorian Government, public servants, local councils, Victoria Police and other public authorities consider human rights when they make laws, develop policies and provide their day-to-day services.

http://www.humanrightscommission.vic.gov.au/index.php?option=com_k2&view=item&layout=item&id=764&Itemid=515

That is, as an arm of government, DPI may need to refer to the Charter when developing policies in the AMI program, even though electricity market participants themselves are not themselves bound by it.

DPI should take heed also of the statement that “the Victorian Ombudsman can receive and investigate complaints about whether administrative actions taken by the Government, local councils and public authorities are in breach of, or have not properly considered human rights”.

Part 1: Description of the project

Overview

Victoria's smart metering program

The move to AMI is driven by several different factors, which may be expressed in different ways by each of the many stakeholders.

One of the most fundamental drivers is the desire for better management of electricity distribution infrastructure so that current investments can be made to last significantly longer, allowing new expenditure to be spread out. The cost of distribution infrastructure is dictated by its peak load carrying capacity. At present, peak consumption in the state is triggered on only a few days annually when extreme heat leads to high demand for air conditioning; otherwise the bulk of the distribution system operates at significantly beneath its peak capacity. This means that if the rare peak loads can be spread out, the current system on average will be able to meet medium term future demands without significant enhancement, thus reducing or delaying additional network costs.

Smart metering is key to better management of peak power consumption. It allows more effective flexible pricing, including sophisticated time-of-use (TOU) tariffs, with real time price signals able to be relayed to consumers in a variety of ways. Smart metering also provides greatly enhanced data for DBs to monitor their networks, manage instantaneous distribution, and plan for the future. It will allow direct load control of power hungry appliances such as air conditioners, in-floor heating and swimming pool pumps, so that in times of crisis, electricity companies can ration supply to such appliances items, without noticeably affecting their amenity. Meter Data Services will in future let power consumption and efficiency data to be relayed to consumers to help them positively modify their power-related behaviours.

Finally for the purposes of this brief recounting of AMI's drivers, we note that it is expected to deliver a further set of direct consumer benefits. It will lower the cost of meter reading, and eliminate estimated reads, thus providing consumers with more accurate electricity bills. And it allows remote disconnect/reconnect of power to premises, significantly improving customer service and cost when occupancy changes.

Project environment

The AMI project is not without controversy.² The cost-benefit from the consumer perspective worries some, especially when charges for smart meters appear on electricity bills even before they are installed. In the wake of the accelerated rollout, some consumer groups have been left feeling that many of their concerns have not yet been addressed. Above all, relatively little information has been made available (for reasons we discuss later) and in this void, a great deal of supposition has been allowed to build up and propagate.

The environment has bred a remarkably wide spectrum of consumer concerns. It is unclear to many householders what smart meters are doing. Some feel that the flashing lights, being visible at a distance from the property may compromise home security by indicating when people are in and out. The electronic nature of smart metering is suspected by some of allowing potential surveillance of what householders are up to, and increasing their exposure to unwelcome direct marketing. And the possibility of sharing electricity consumption data with third parties brings additional privacy fears, especially given the unfortunate occasional excesses of various large Internet companies.

Victoria's AMI rollout is proceeding in parallel with the National Smart Meter Program (NSMP), with the expectation that Victoria will transition over time to national arrangements once they are sufficiently developed. AMI stakeholders are using their experience to actively contribute to NSMP deliberations on governance and technological issues, while attempting to safeguard their strategic and business interests by keeping the NSMP aligned with AMI's established features.

Smart metering provides a powerful platform for significant innovation in retail electricity products and services, and this has created major excitement in some circles.³ Some industry players would prefer that more experience with this new technology be garnered before regulating 'pre-emptively'. Lockstep notes that tension between privacy and innovation often arises in online businesses, and this is not always satisfactorily resolved. It is important to maintain a good faith dialogue amongst diverse stakeholders to head-off unhelpful perceptions that innovation and consumer protection are at odds.

² See for example <http://www.ceda.com.au/news-articles/2011/06/10/smart-metering-towards-an-efficient-electricity-future>. Similar concerns have dogged smart meter programs overseas as well; see for example <http://www.computerweekly.com/Articles/2011/06/21/247050/Smart-meter-project-lacks-public-support-due-to-concerns-about-rising-energy.htm>.

³ See for example <http://www.emeter.com/smart-grid-watch/2010/uk-smart-meter-prospectus-groundwork-for-energy-industry-innovation>.

Project details

Bearing in mind that this PIA is concerned only with changes to information flows and thence privacy brought about by smart metering, here is a diagram of the major AMI components and a list of the important high level features of the program.

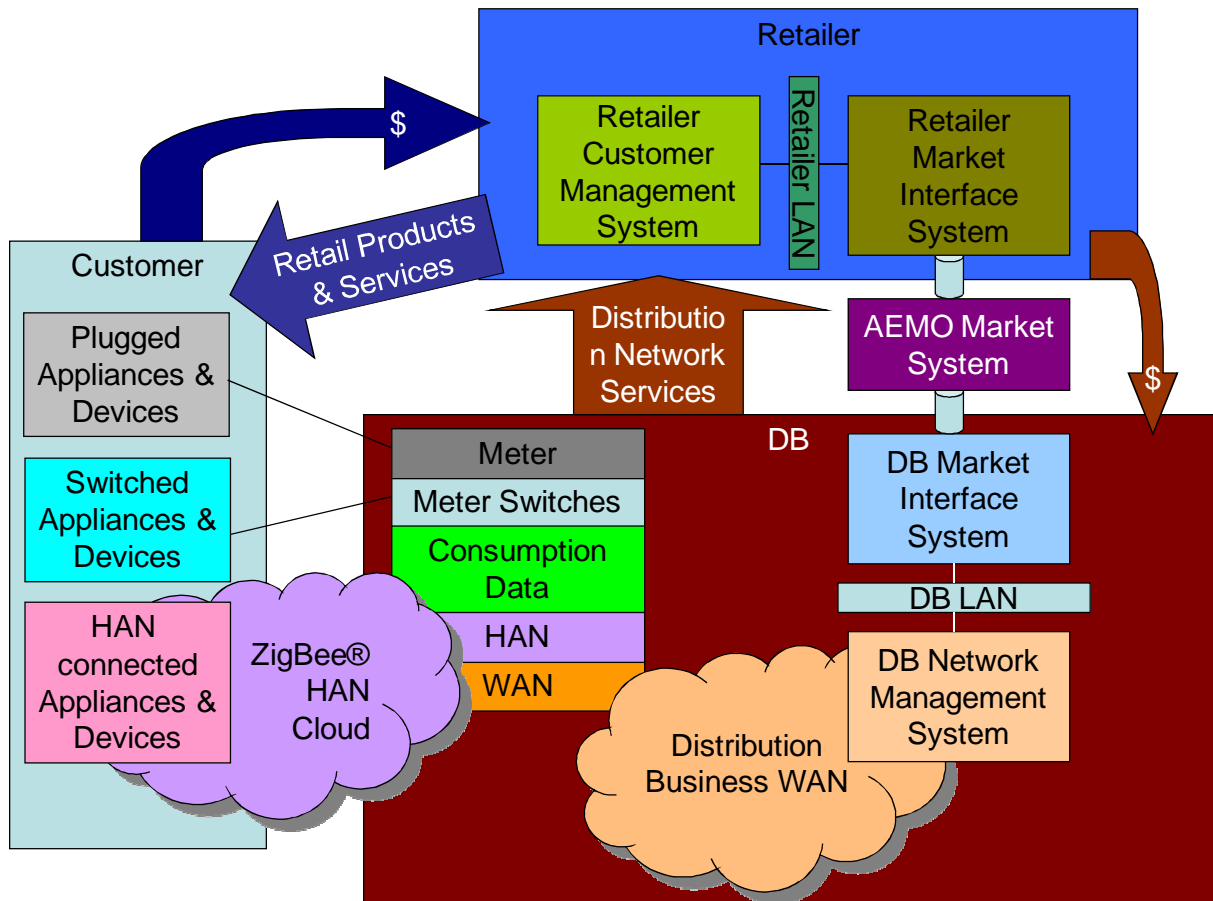


Figure 1: Electricity Industry Structure and Relationships Today⁴

Smart meters measure power consumption continuously, and records it every half-hour, to provide data needed for settling the national electricity market. The meters buffer the measurements and upload them periodically to the Distribution Business that controls the meter, for input to the market system. Uploads should occur at least once a day, in line with National Electricity Rules. To cope with network outages, the meters retain interval data over a much longer period (200 days).

Smart meters communicate interval data back to DBs over special secure private radio networks. Most use a “mesh radio” service provided by Silverspring; one uses the different technology of “wimax”. In future some of these private network connections may be superseded by NBN.

⁴ Diagram courtesy of Stephen Thomson, *Industry Structure and Relationships.ppt*, 21 June 2011.

Smart meters feature a second type of wireless connectivity known as *ZigBee*, which is available for establishing optional Home Areas Networks (HANs). ZigBee is technically similar to the familiar “wifi” protocol which underpins all domestic wireless computer networks (but as we shall discuss later, crucially ZigBee is more secure by default than most commodity wifi devices).

The main intention of a HAN is to connect In-Home Displays (IHDs) and “smart” appliances directly to the meter for real time monitoring and control of electricity consumption. The ZigBee protocol is supported by an increasing range of “smart” appliances. There is very little experience of these devices as yet in Australia, and almost no consumer awareness.

Finally of note to this PIA, smart metering is intended to support a range of advanced services to assist consumers better manage their electricity consumption. These can be as simple as providing a secure personal webpage on which fine grained electricity statistics are displayed. Over time, more sophisticated services are anticipated. DPI has commissioned a preliminary survey of these; see [1]. There appears to be many ways for high resolution consumption data to be value-added to allow householders to monitor their power consumption, understand how it varies, and what they can do to better manage it.

Importantly, some of these advanced services will likely be provided by third parties who are not themselves registered market participants. In principle, third party services can obtain information by one of two routes:

1. From the backend interval data collected by a DB or RB; this data will be aged by up to 24 hours but is more readily available through backend information systems rather than direct connection to the HAN.
2. Direct from the meter via ZigBee; this data will be instantaneous, and available at a resolution of much less than 30 minutes, but it requires another device to be bound to the ZigBee network.

Third party meter data services occupy new ground in the electricity marketplace. Practical and attractive services are still in a state of flux; there appear to be no clear business models as yet. Significantly, Google recently withdrew its *PowerMeter* service.⁵ This may indicate difficulties for pure-play third party information services. Indeed, more than one RB told us they believe a ‘conversation’ about power consumption can only be meaningfully conducted with a consumer by their electricity retailer. The beneficial implication for privacy is that there is little prospect of an explosion of third party services, and the attendant privacy risks, while certainly potentially significant, will not be pressing concerns for the time being.

⁵ See *An update on Google Health and Google PowerMeter* 24 June 2011; <http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html> (accessed 22 July 2011).

Part 2: Information Flow Mapping

Information flows

Summary of existing information flows

Historically, metering data has been collected from accumulation (“spinning disk”) meters by or on behalf of DBs, usually no more frequently than once a quarter. Metering data provided by the DB to AEMO and RBs is tagged only by a National Meter Identifier (NMI). It is not accompanied by name or address information.

Metering information is transferred by the DB to AEMO and to the RB.

In a distributor’s backend systems, the NMI is associated with a physical address for the meter. The DBs also maintain contact names for each address, for the purposes of making contact in case of a problem accessing the meter; these names may be different from those used by RBs for billing purposes. There is also the necessity to keep track of households with medical equipment that cannot be routinely disconnected from the supply without special checks. For retailers, the NMI is associated with a location (typically a residential street address) and a customer name for billing purposes. In order to provide for RoLR events, RBs are obligated to inform DBs when there is a change to the customer name associated with a NMI (for example, when a customer moves out of residential premises). Therefore DBs collectively hold name and address details for essentially all electricity customers. In general these details are kept separate from the NMI-keyed meter data.

The use of NMIs (rather than actual addresses or names) to identify metering information when in transmission provides a measure of privacy protection, yet both DBs and RBs can and do associate each NMI with both an address and a named individual, in other parts of their businesses. Therefore in some cases metering data will constitute *Personal Information*. To put it another way, given the complexity of databases, and the fact that staff within the businesses have diverse roles that necessitate access to multiple systems, there are certainly various means for metering data to be rendered identifiable. Therefore it would be difficult to prove that *no* metering data was *Personal Information*.

To avoid tortuous and technical arguments about identifiability, and to exhibit instead a precautionary approach, later in this report we will make the case for handling all metering data in accordance with the NPPs, as if it was in fact potentially *Personal Information*. For the rest of this analysis, we will examine metering data ‘through the lens’ of the NPPs, whether or not the data is technically *Personal Information*.

New smart meter related flows

The following diagrams illustrate the primary flows of smart metering data today from premises to the DB and through to the RB and AEMO, and the additional secondary flows expected in future with the introduction of third party services and HANs.

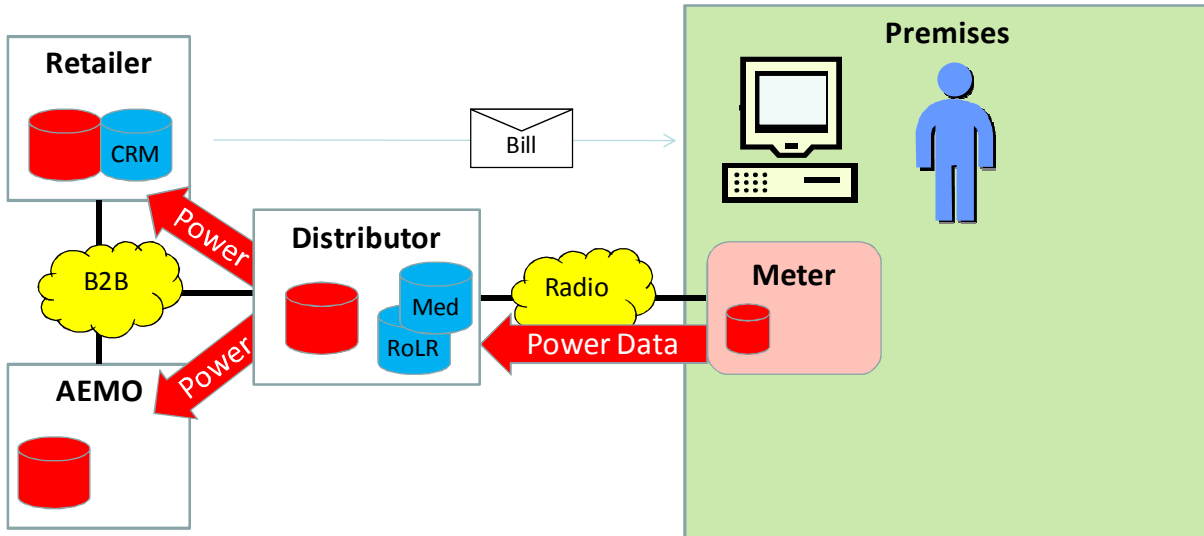


Figure 2: Primary flows of metering data

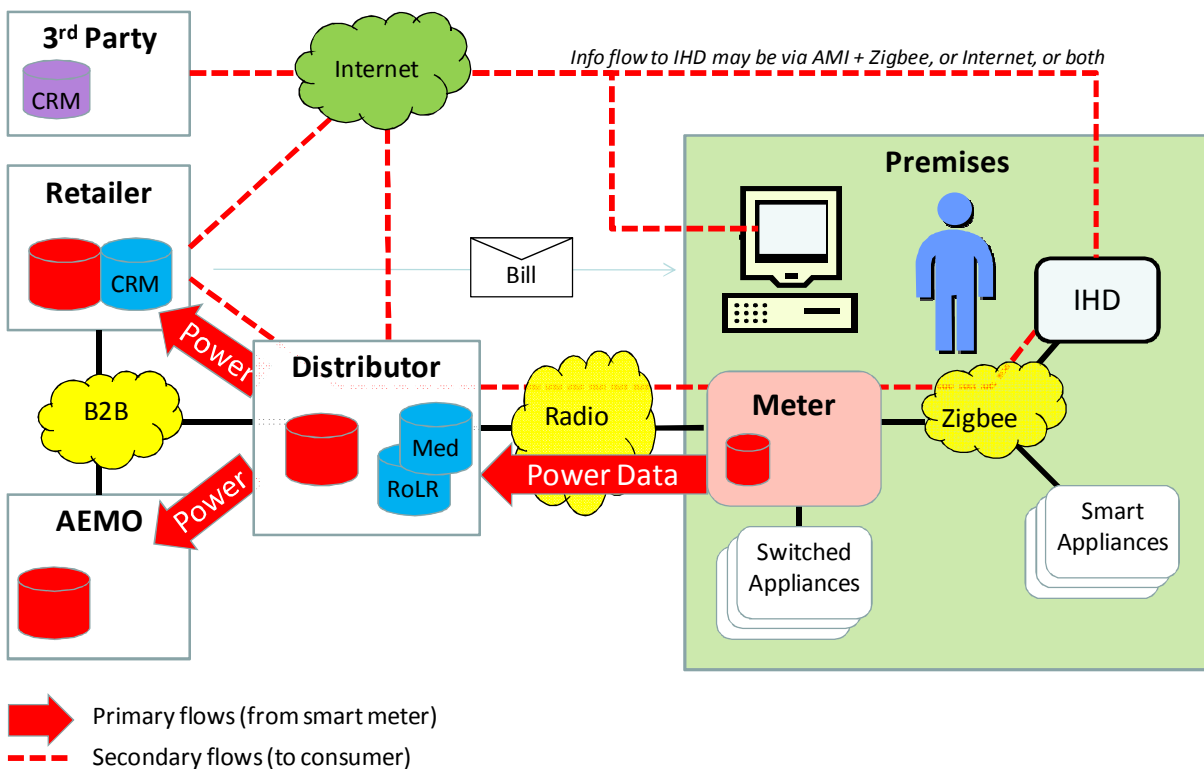


Figure 3: Secondary flows of metering data

- Interval power consumption is sampled every 30 minutes and sent from the meter to the DB, typically in blocks over the course of the day; 24 hours worth of interval data thence sent daily to the RB and to AEMO.
- Power quality (a function of voltage) is sampled less often, on an exception basis.
- Commands may be sent from the DB to the meter, for example to disconnect supply, to re-energise the supply, and to bind a new HAN device.
- Log information is sent from the meter to the DB concerning defined events such as power disruptions and tampering (not shown in the diagrams).
- Instantaneous power consumption (that is, power consumption at any instant in time, without the 30 min sampling constraint) can be sent from the meter to a qualified HAN-connected device.
- The ZigBee protocol supports the exchange of other brief messages amongst devices sharing the meter-controlled HAN. We understand there is some flexibility here to set constraints on HAN device messaging via the Smart Energy Profile (SEP), and that these matters will be covered by BPPWG in near future.

Collection of Personal Information and metering data

Overt collection

Our review of the installation process indicates that customers are not generally required to furnish any details themselves at the time of installation (indeed, they are not even required to be present). Instead, details are taken from existing records at the backend. Therefore, no Personal Information is generally collected *directly* from individuals in AMI.

Automated collections

Metering data is collected and stored automatically in the meter.

Metering data is transmitted in batches from the meter to the DB in blocks that are usually no more than 24 hours long. National rules dictate that daily meter data be uploaded to AEMO by 6:00AM the following day. To help manage data network capacity, DBs increasingly tend to upload in shorter blocks from the meters several times a day.

Data collected in the meter is retained there for 200 days to help ensure business continuity should the normal meter reading process be interrupted. Data older than 200 days is automatically overwritten.

Raw interval is retained at AMEO for seven years.⁶

Use of metering data

The *primary* purpose for half hourly interval meter data collection in AMI may be considered to be two-fold:

1. Provide frequent high quality interval consumption data to support the national electricity market which settles on a half-hourly basis.
2. Monitor consumption with greater resolution so as to improve network infrastructure management.

Note that the collection of power consumption data *in general* (and in common across old accumulation meters and new smart meters) is primarily related to the billing of electricity consumers. The AMI program does not change the fundamentals of billing, nor the relationships between DBs and RBs that enable sharing of meter data for billing. Because this PIA is focused on the changes to privacy brought about by smart metering (see *Scope & Deliverables*, page 9), we do not discuss billing, and we ignore billing in analysing primary vs. secondary uses for *interval* meter data.⁷

There is a spectrum of current and potential *secondary* uses of interval data, including:

- a. supporting direct load control
- b. the creation of energy efficiency advice (for 'free')
- c. direct marketing of advice and/or energy management services by the contracted retailer
- d. direct marketing of and/or energy management services by third parties
- e. direct marketing of specific appliances.

In privacy, a central issue is the degree to which any secondary use of information is related to the primary purpose for collection, and the likelihood that individuals would perceive secondary use to be reasonable.

The further along the spectrum we venture, the harder it becomes to argue that the secondary usage is directly related to the primary collection purpose. Given the need for judgement, and the inevitability that such judgments would be made differently by different consumers, we urge caution with regards to presuming that *any* secondary usage of metering data is directly related to half-hourly settlement of the market.

⁶ We note that AEMO believes its mass storage system to be the biggest in the Southern Hemisphere.

⁷ Note also that enhanced Time Of Use (TOU) as enabled by smart metering is regarded as directly related to billing. TOU tariffs have been in use for many years, and have been enhanced by the advent of interval data. The use of interval data in TOU pricing is not a secondary use of that data.

We recommend that the AMI program not take for granted that *any* customer will regard secondary use as reasonable. In other words, we believe that an express Opt-In model be adopted for managing consumers' acceptance of secondary usage, by which consumers would always be given a free choice to take any of these options, and that by default, no secondary reuse would be made until the consumer freely chooses same.

Disclosure of metering data

We regard the daily transfer of interval data from Distribution Businesses to AEMO to relate to the primary purpose for information collected by smart metering. However, other exchanges of information with Retail Businesses—with the exception of billing—are secondary and need to be examined in terms of compliance with the Disclosure principle. With respect to billing, as noted on the previous page, we assume in this PIA that a typical consumer, if they appreciate the role of Distribution Business and Retail Businesses, would find it reasonable for DBs to disclose meter data to RBs for the purposes of billing. The fact that RBs and DBs are separate legal entities, with no control over how each other operates, means that any transfer of metering data between them for purposes other than billing should be regarded as a *Disclosure*, and not a *Use*.

Part 3: Privacy analysis

On Personal Information

Data privacy is often framed in the commercial world in terms of explicit customer details and especially valuable information such as credit card numbers. Yet the legal definition of “Personal Information” under information privacy law is broad. According to the Privacy Act 1988 (Cth):

personal information means 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 (emphasis added) [13].

That is, any data that can feasibly be related to a customer counts as *Personal Information* and becomes subject to the NPPs. This includes data that is internally generated within an organisation, or which is indirectly collected from an entity other than the individual concerned.

Further, while the word “collection” tends to connote an interaction between a person and the collector of Personal Information, it is important to understand that information privacy law is largely blind to the manner in which PI comes to be present in a business. The automatic electronic transmission of data into a business by whatever means, where the data could be associated with an individual, generally counts as an act of collection under the Privacy Act.

We note there is a view that power consumption data generally relates to the aggregate behaviours of multiple members of a household rather than any one individual (excepting sole occupants of course). To some extent this aggregation serves to protect privacy, because even if the name of the electricity account holder was to be associated with the interval meter data, it wouldn't necessarily reflect that person's power usage compared with other members of their household. Lockstep on the other hand cautions that this might be an overly technical treatment, and may appear self-serving. We urge a precautionary approach (especially since DBs and RBs do not know for sure which of their customers are sole occupants) in which metering data from all residential premises would be handled in compliance with the National Privacy Principles.

The Australian Privacy Commissioner has also urged the development of privacy protections in relation to smart metering,⁸ notwithstanding the

⁸ See *Energy meters could make burglars smarter*, The Australian, 22 Nov 2010 <http://www.theaustralian.com.au/news/nation/energy-meters-could-make-burglars-smarter/story-e6frg6nf-1225958013268> (accessed 22 July 2011).

technical argument about data being associated with a small group of individuals (a household) rather than with one individual (the known customer).

On “ownership” of information

A number of consumer groups we interviewed suggested that there was uncertainty over who *owns* data generated by smart meters, and that this uncertainty should be resolved. There may well be other reasons to clarify this matter, but Lockstep advises that *ownership* is not actually a practical tool for managing privacy. No clear legal principles exist as yet for property rights over data (and some mooted mechanisms such as intellectual property protection are somewhat controversial and unattractive in online consumer affairs).

Moreover, in the Australian privacy regime, businesses are obligated to safeguard Personal Information regardless of who “owns” it. The concept of information ownership does not figure in the Privacy Act [13]. We hope that the recommendations of this PIA, framed within existing regulations, prove satisfactory to consumer organisations without needing to appeal to the concept of ownership.

Perceived privacy problems

Smart metering here and overseas has attracted significant community concerns. It is worthwhile recapping what the major concerns are, ahead of making an objective analysis of the information privacy issues.

In general, Lockstep recommends that community concerns be taken seriously, and that they be fully investigated. Where the concerns are found to have substance, obviously the implications should be managed, via tools like this PIA. Where community concerns are not substantiated, it is nevertheless important that the AMI program undertake an awareness program to seek to put the majority of peoples’ minds at rest.

Over the course of our investigation, we compiled the following catalogue of privacy concerns and related objections:

- smart metering may reveal householders’ behaviour patterns
- smart metering may reveal times of absence from the house, either directly by observing the flashing lights from afar or by surreptitiously accessing back end data, and therefore create personal security risks (see e.g. [8] paragraph 7)
- smart metering may reveal whether home alarm systems exist, and are switched on or off, therefore presenting personal security risks
- smart metering may provide means for extra and unwanted direct marketing from electricity businesses; as the Victorian Privacy Commissioner put it, “if the usage data is shared beyond the electricity provider, this type of information could be used by other electricity companies, for research purposes or even by third parties for direct, targeted marketing based on usage” [8]

- smart metering may reveal other information to third parties such as the types of appliances in the home
- some find the flashing lights emotionally confronting, suggestive of “Big Brother” operating at a new level across neighbourhoods;⁹ some consumers feel anxious in the absence of clear education about what exactly the flashing lights are for.

Lockstep also sees parallels between the use of wireless communications in the Home Area Network and community sensitivities raised when it came to light that Google and other businesses were routinely surveying the presence of wifi installations detectable from the street, and inadvertently collecting network payload data at the same time. There is a significant political risk to consumer public acceptance of AMI should its use of wireless technology in the HAN be misunderstood by consumers as having the same vulnerabilities as regular wifi, or worse, if people thought HAN communications crossed-over with other wireless networks.

Privacy positives of the program

Several aspects of the AMI program and smart metering technology provide distinct privacy benefits. We identify and commend the following as privacy enhancing features:

- The working groups of AMI and the National Smart Metering Program provide a pre-existing governance skeleton and decision making forum in which to resolve many of our recommendations. In particular, the refreshed AMI Communications Working Group¹⁰ in principle should be able to “own”, review and implement any of our findings.
- As a result of the ESC’s review, ESC Registered Participants have already been tasked to develop “privacy principles”¹¹ specific to the dissemination of consumption information from smart metering through IHDs, before IHDs are utilised [5].
- Smart metering should result in an improvement in the quality of customers’ consumption data held by RBs (thanks mainly to the elimination of estimated reads). Enhancing the accuracy and quality of Personal Information is intrinsically good for privacy (as per the *Quality Principle* NPP 3; see Appendix).

⁹ One consumer advocate related the unusual and off-putting sight of lights blinking all the way down a street of terrace houses, “like Christmas lights”. We appreciate the impression that may be given of houses being networked together in surreptitious ways without householders’ consent.

¹⁰ This group, made up of industry, consumer advocates and other relevant organisations, was established by the AMI Policy Committee to provide advice to government on communications aspects of the program.

¹¹ We actually understand this to mean what are better called privacy *policies*.

- In the longer term, the ability for customers to access their own metering data (via IHDs and/or third parties) is intrinsically good for privacy (as per the *Openness Principle* NPP 5; see Appendix).
- There is evidently a strong information security culture at Registered Participants, and security obligations also bind Participants pursuant to the Minimum AMI Functionality Specification [3] and Chapter 7 of the NER [11]. The international information security standard ISO 27001 has been adopted across the sector. At least one DB appears to routinely do security TRAs.
- Use of NMIs means that some degree of de-identification is built in to raw power consumption data (although we hasten to add that in itself this protection is not at all absolute and should only be viewed as being a privacy ‘aid’).
- Smart meters’ HAN connectivity is turned off by default, and can only be turned on by active intervention from the DB on request from a customer (potentially via their retailer). Procedures for same have been identified by the BPPWG but not yet written; inadvertent activation is highly unlikely until procedures are put in place.
- When networking is activated, all HAN traffic is always encrypted. Unlike regular wifi networks, it is not possible to de-activate HAN encryption. “Drive-by” snooping on HAN network information or power consumption is not practicable.
- As and when the new HAN binding procedures are developed, there is an opportunity to ensure that connection to third party services is made on an opt-in basis, with consumers needing to take express steps with their meter provider to consent to and services devices joining the HAN.
- Smart metering does not provide DBs and RBs with real time visibility into a customer’s behaviour. Data is uploaded from smart meters with a delay of several hours, up to 24 hours. This ameliorates to some extent the concern that smart meters expose householders to increased security concerns, although the fact remains that behaviour patterns might be inferred. Instantaneous real time data will be available only to devices connected directly to the meter over the ZigBee network.

We also identified the following positive features of the Victorian electricity industry in general, which serve to improve the prospects of implementing the recommendations of this PIA:

- Smart metering is being implemented in a highly regulated industry, with a rich management controls environment. Registered Participants are strictly licensed. No entity can gain access to power consumption data without going to substantial efforts.

- There are several existing binding codes of practice overseen by the ESC, including electricity metering in general, and the marketing of retail energy. These codes help to protect privacy. Furthermore, the existence of such elaborate codes points to a culture and a governance framework in which additional privacy measures can be implemented as need be.
- All electricity metering data is already specifically classified as “Confidential” under the Electricity Customer Metering Code (see [9] section 7.2) which brings obligations to protect its privacy.
- The ESC’s licence conditions for Participants entail information security standards compliance.
- All Participants are also bound by the National Electricity Rules [11] which (in chapter 7 particularly) set down detailed rules around the collection of metering data, entitlement to handle and access that data, security and confidentiality provisions .

Privacy challenges

- There needs to be an appreciation that even though the fact of electricity consumption data collection has not changed, the dramatically increased frequency of collection—from once every three months to once every 30 minutes—significantly changes the value and meaning of the data. The richness of the data can yield information about behavioural patterns within each household. It is this richness which creates the most important new privacy risks for householders.
- Smart metering also introduces the theoretical potential for collection of a new instance of Personal Information concerning specific appliances used in the home. Widespread activation of HANs is contingent on the development of business processes and technical protocols for the exchange of security codes between the meter and the DB; this development is identified in the BPPWG work plan but has yet to commence. In the absence of activation processes, some small scale HAN pilots have been conducted and may continue. Ideally such pilots would provide useful information on potential new PI flows and issues, for consideration by the BPPWG when formalising HAN arrangements.

More work may need to be done (within the BPPWG) to delineate and if necessary control the possibility of DBs compiling registers of appliances bound to each HAN. It is important that the community’s anxieties about HANs not be exacerbated by any sudden increase in HAN activations, and that it is made clear that consumers will be in control of their home networks.

- While some of the more common privacy concerns (such as worries about hacking or eavesdropping on the wireless transmissions from the meter) are not substantiated, the program has not yet

systematically dealt with these concerns. In an environment where overall the AMI program receives significant attention in the media, the program needs to carefully separate and deal with privacy concerns and other issues, to avoid conflation.

- In the industry there seems to be an under-appreciation of what constitutes *Personal Information*. In particular, some DBs appear to believe that “Personal Information” is confined to customer-furnished data such as credit card details, or that metering data intrinsically doesn’t qualify as PI as it is associated with a NMI only (and not a name or address) at time of collection and transmission. It is not uncommon for private sector businesses to develop a narrow view of privacy, informed by such topical issues as identity theft and credit card fraud, yet the legal definition of PI is actually much broader, as discussed above. It seems likely that some subsets of metering data held at DBs would constitute *Personal Information* because that data may be linked to identifiable persons; if so, businesses may be unaware of the full range of obligations that go with holding PI.
- Furthermore, it would be difficult for a DB to show that metering data it holds *cannot* be linked to a named individual, given the proximity in the same organisation of RoLR and other data which links names and addresses to NMIs. Therefore trying to make a case that metering data is definitely *not* Personal Information would be challenging.
- Privacy Policies of DBs seem mainly concerned with PI collected on the websites of the Participants. It is less obvious what policies that have around metering data and the potential for authorised disclosure to third parties.
- DBs’ interests in smart metering are not totally aligned with RBs’, and communications to date have not proactively covered consumers’ privacy concerns; instead they have tended to describe essentially mechanical issues to do with the installation of the meters. Yet it is RBs that hold the main customer relationship and some tend to find themselves fielding consumer questions and concerns, despite not owning the meters, and not having been responsible for the limited information provided to consumers to date. The broader implications of meter data sharing—though largely to do with perception at this stage than substantive privacy risks—are nevertheless of great concern to consumers, and more attention needs to be paid by DBs and RBs jointly to allay public anxieties.
- There is some tension between “innovation” and privacy (though this hasn’t yet taken shape as a explicit conflict as it has in certain sectors of the digital economy). On the one hand, the industry is leaning towards getting some experience with HANs and developing procedures as they go, whereas consumer groups

would prefer to see firm privacy protections put in place beforehand. HANs are inherently more privacy protective than consumers may realise (because all HAN traffic is encrypted, the network is inactive by default, no devices can automatically join, there is no realistic possibility of drive-by snooping, and the limited ZigBee bandwidth will restrict IHDs from becoming advertising screens) and the tension might be eased if people were made more aware of HAN properties.

- A new type of interaction between RB and DB appears necessary in future to manage consent to bind new HAN devices. The security codes that must be presented to the smart meter (as HAN controller) are known by the DB (or potentially in future by a separate Metering Provider) but the customer who is to authorise binding is known definitively by the RB. Some type of authentication must be performed—presumably by the RB—on requests to bind new HAN devices, and the fact of authentication then handed over to the DB. This may require careful design to prevent unnecessary disclosure of customer PI to the DB, but it does not appear to be a major challenge.

Other high level privacy issues

Availability of previous occupants' metering data

We understand there is an unresolved standing issue about how interval data in the meter should be scrubbed when new occupants take over the electricity account. There would appear to be competing interests in this data. On the one hand, previous occupants may feel that it is private. On the other hand, incoming householders may have an interest in the power efficiency of a premises, and real estate agents may feel it important to make relevant information available in some way.

We do not feel that it is in-scope for this PIA to make a clear ruling on this issue. Instead we recommend that the AMI program (and also the BPPWG) work with consumer groups to strike a reasonable balance between these potentially conflicting interests.

RBs' and DBs' customer database security

From interviews we found there to be a historically reasonable security culture at Retail Businesses, in line with their customer focus. There appears to be consistently serious training of customer service personnel, appropriate internal privacy practices, and commensurate database security. However, we did not find much, if any, regular audit being done of the way the customer databases are used. We suspect that customer databases would not be typically configured for detailed auditability of potential misuses of customer information. Yet we believe 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. If so, then more rigorous auditing may need to be instigated.

Distribution Businesses have understandably not had as much customer focus as the RBs. Distributors do however treat all metering data as confidential, as required by the ESC, and appear to follow strong security practices including compliance with ISO 27001 and in at least one case, regular internal Threat & Risk Assessment. It is important to ensure that access to DBs' databases is also tightly controlled and audited.

We understand that the various data stores at DBs that hold RoLR related information and other customer details are separate from the interval data stores, as they should be. It is important that re-identification of NMI-keyed metering data by linking to name-and-address records is deliberately made difficult.

Meter Data Management systems and billing systems are being revamped at various businesses, to cope with the enormous volumes of interval data being collected. During this PIA we could not see how these systems are configured. We simply observe (without knowing whether this is the case or not) that care is needed to restrict access to interval data on a need to know basis.

Privacy Notices

The interviews, our review of the communications provided by DBs (in the main) to consumers, and our sampling of DBs' and RBs' privacy policies indicate that the concept of Privacy Notices is not well ingrained in this industry. In general, any organisation collecting Personal Information should provide appropriate notice to individuals concerned, particularly in order to satisfy NPP 5, the *Openness Principle* (see Appendix). Privacy notices generally set out a summary of why, how and when Personal Information is collected, cite any applicable legislation that authorises collection, and provide contact details so individuals can make inquiries. There have been opportunities for such notice to be given to smart meter customers, but presumably because metering data is not regarded as Personal Information, no details like these have been disseminated in AMI.

Providing understandable and actionable information about information privacy can be challenging in complex settings like electricity metering. As discussed, the reasons for collecting metering data are multi-faceted and quite technical. Such information needs to be presented in different ways, if it is not by turns going to confuse some readers and fail to meet the questions of others.

The UK Information Commissioner's Office has produced excellent advice on layered privacy notices. They describe the challenge as follows:

When collecting personal information you should be realistic about how interested the public is in the way you are going to handle it. Many individuals will be more concerned with receiving the goods, services or benefits that they have applied for. They are unlikely to read a detailed privacy notice, or to make a complaint about the way you handle their personal information, unless they feel their personal information has been handled badly. This is why a 'layered notice' can be useful. [16]

The Australian Privacy Commissioner recommends *layered* privacy notices, and indeed the Privacy Policy of the Office of the Privacy Commissioner is written in a layered manner.

We informally discussed with the Privacy Commissioner¹² a privacy notice for smart metering structured along the following lines:

1. Provide reassurance as to the legislation and codes under which all electricity businesses operate, and other high level mechanisms that help to protect consumer information.
2. Explain what control consumers have over how metering data is used, and what policies [will] apply to protect future uses.
3. Explain why smart metering has been introduced, from all applicable perspectives (including economics, price signalling, infrastructure planning, efficiency, reduction of cost of reading meters, new functions for remote control, and new services for consumers).
4. Set out more detail for interested readers to follow through if desired, and detailed cross references.

Beyond these high level considerations, this PIA was not scoped to develop privacy notices, but we do include below a recommendation that a reasonably consistent industry-wide form of notice be developed and promulgated.

Other individuals contracting for third party services

In the historical domestic metering setting, there has been little if any commercial concern with anyone other than the electricity account holder, who may for all intents and purposes have been regarded as the 'head of the household'. But now with a wealth of information being available about power consumption and efficiency, and many new ways to communicate about appliance usage and energy efficiency, the potential arises for retailers or third parties to wish to engage with more individuals than just the 'head of the household' or electricity account holder. It was suggested to us by DPI during this study that energy efficiency related contracts might in future be struck between individuals in a household and retailers or third parties, involving IHDs or smart appliances.

¹² Reference: interview with Timothy Pilgrim., 20 July 2011.

From a privacy point of view we must remember that the metering data itself aggregates the power drawn by all appliances and does not indicate individual behaviour (where more than one person is in the household). And yet interval meter data does merit more protection than does accumulation meter data. As discussed elsewhere in this report, it may be prudent to safeguard smart meter data in line with the National Privacy Principles (NPPs). If this were the case, then there should be constraints on the way that anyone including others in the household make use of meter data.

Accordingly, when in future the possibility arises that individuals in a household wish to enter into third party contracts relating to energy efficiency or other use of smart meter data, we would recommend that consent of the main electricity account holder be necessary. That is, such third party contracts should be signed by both the individual and the main electricity account holder.

Part 4: Privacy Management

In this section we present a catalogue of privacy management issues, organised according to applicable NPP, and also according to the broad category of type of indicated action, which is one of the following:

- New or improved communications to consumers and/or the general public.
- Policy setting of DPI and/or the industry.
- A change to selected technology.
- New or modified regulation, rules, laws and so on.
- Further investigation needed to refine any recommendation.

For reference, the National Privacy Principles are set out in an appendix.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
Definitions	Definition of <i>Personal Information</i>	Concern re whether the data can be related to an identifiable person.	<ul style="list-style-type: none"> • Need to recognise privacy concerns are real and valid, regardless of legal technicalities about whether interval data may be interpreted differently from the definition of <i>Personal Information</i>. • Recognise and respect that consumption data represents information about behaviour in the home (both real time data from the HAN, and predictive data gleaned from half-hourly patterns), which poses increased privacy risks (safety and other risks). • All parties to agree to handle all metering data from/about residential meters in compliance with the NPPs.
	Scope of what is a 'privacy issue'	Concern re whether consumption data is behavioural data.	

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
At the meter	<p>NPP 8 (Anonymity), NPP 1.3 (Notice) What data is collected</p>	<p>Concern re identifiability and timeliness of data.</p>	<ul style="list-style-type: none"> Consumer communications (e.g. brochure, web based FAQs) to clarify that no name or address data is held in the meter; data is identified only by NMI. Consumer communications to clarify that consumption data is recorded in the meter every 30 minutes.
	<p>NPP 4.1 (Data Security) Security of data in the meter</p>	<p>Risk of breach by direct attack on meter.</p>	<ul style="list-style-type: none"> Consumer communications (FAQs) regarding security measures taken to protect meters, detect tampering at meters etc. Note that the NER part 7.8.2(a) imposes a civil penalty if the “responsible person” fails to use “suitable password and security controls” to protect “energy data held in the metering installation” from “direct local or remote electronic access”.
	<p>NPP 4.1 (Data Security) Access to data in the meter</p>	<p>What can be read with the naked eye.</p>	<ul style="list-style-type: none"> Consumer communications to explain what the flashing lights mean.
In transmission	<p>NPP 4.2 (Data Retention) Retention of data in the meter (200 days)</p>	<p>Excessive data retention increases data security / misuse risks.</p>	<ul style="list-style-type: none"> <i>Consider this issue as part of the as yet undeveloped protocol for granting incoming residents access to previous residents’ meter data.</i>
	<p>NPP 8 (Anonymity), NPP 1.3 (Notice) What data is transmitted</p>	<p>Concern re identifiability and timeliness of data.</p>	<ul style="list-style-type: none"> Consumer communications (e.g. brochure, FAQs) to clarify that no name or address data is transmitted; data is identified only by NMI. Consumer communications to clarify that data is not transmitted in real time, but is sent from meter in batches through the day, and from DB to AEMO and then RBs once per day.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 4.1 (Data Security) Security of data when in transmission from meter to network (DB)</p>	<p>Risk of breach by external attack.</p>	<ul style="list-style-type: none"> • Data is encrypted in transmission. • We assume that WiMax and Mesh Radio security is fit for purpose.
	<p>NPP 4.1 (Data Security) Security of data when in transmission from DB to AEMO</p>	<p>Risk of breach by external attack.</p>	<ul style="list-style-type: none"> • We assume that DB-AEMO communications security is fit for purpose.
	<p>NPP 4.1 (Data Security) Security of data when in transmission from DB to RB</p>	<p>Risk of breach by external attack.</p>	<ul style="list-style-type: none"> • We assume that DB-RB communications security is fit for purpose.
<p>Primary use of data</p>	<p>NPP 1.1 (Collection Necessity), NPP 3 (Data Quality) Necessity of collection of <i>non-consumption data</i> from the meter for the DB</p>	<p>Justified:</p> <ul style="list-style-type: none"> • Remote read saves money and improves accuracy by obviating estimated reads • DB can control supply to premises remotely (turn power on or off) for better change of residency • Capacity & voltage data from smart meters can indicate power outages, power quality problems, so DB can fix these faster. 	<ul style="list-style-type: none"> • Consumer communications need to explain this use of the data. • We note that greater accuracy is a privacy enhancement attributable to smart metering.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 1.1 (Collection Necessity), NPP 3 (Data Quality) Necessity of collection of <i>half-hourly consumption data</i> for DB</p>	<p>Justified:</p> <ul style="list-style-type: none"> Half-hourly consumption data is useful for managing network infrastructure and daily load (can manage infrastructure efficiency by using TOU pricing to influence customers to shift load and thus flatten peaks in use). DB charges to RB depend in part on actual consumption by the household; smart metering allows more accurate data hence more accurate billing. 	<ul style="list-style-type: none"> Consumer communications need to explain this use of the data. We note that greater accuracy is a privacy enhancement attributable to smart metering.
	<p>NPP 4.2 (Data Retention) Data retention period at DB</p>	<p>National Electricity Rules require at least seven years retention in accessible format.</p>	<ul style="list-style-type: none"> NER 7.11.3 re “metering data providers” says data must be kept for 13 months online and archive for seven or more years. Suggest review of NER to consider (a) whether same data really needs to be kept in triplicate at DB / AEMO / RB, and (b) if it is really necessary to keep all the data at the half-hourly granular level; some aggregation after 13 months would be more privacy-protective. Suggest industry may require further prescription re disposal after seven years.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 1.1 (Collection Necessity) Necessity of collection for RB</p>	<p>Justified:</p> <ul style="list-style-type: none"> Wholesale market settles on 30 minute basis. Allows more accurate billing to customer. 	<ul style="list-style-type: none"> Consumer communications need to explain this use of the data. We note that greater accuracy is a privacy enhancement attributable to smart metering.
	<p>NPP 4.2 (Data Retention) Data retention period at RB</p>	<p>Excessive data retention increases data security / misuse risks.</p>	<ul style="list-style-type: none"> RB practice appears to be to also keep for seven or more years. Suggest review of NER to consider (a) whether same data really needs to be kept in triplicate at DB / AEMO / RB, and (b) if it is really necessary to keep all the data at the half-hourly granular level; some aggregation after 13 months would be more privacy-protective
	<p>NPP 1.1 (Collection Necessity) Necessity of collection for AEMO</p>	<p>Justified:</p> <ul style="list-style-type: none"> Wholesale market settles on 30 minute basis. 	<ul style="list-style-type: none"> Consumer communications need to explain this use of the data.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 4.2 (Data Retention) Data retention period at AEMO</p>	<p>National Electricity Rules require at least seven years retention in accessible format.</p>	<ul style="list-style-type: none"> • Clause 27 of the Energy Retail Code requires retailers to provide up to two years of historical meter and billing data upon request.. • Clause 7 of the Electricity Customer Metering Code also requires retailers and DBs to retain historical data for provision to customers upon request. The wording implies the request could relate to data that is more than two years old. • NER part 7.9.1(g) requires AEMO to keep metering data (i) online for 13 months and (ii) archived for <i>at least</i> seven years (no maximum period set). • Suggest review of NER to consider (a) whether same data really needs to be kept in triplicate at DB / AEMO / RB, and (b) if it is really necessary to keep all the data at the half-hourly granular level; some aggregation after 13 months would be more privacy-protective • Suggest industry may require further prescription re disposal after seven years.
<p>Secondary uses of data</p>	<p>NPP 2.1 (Use) Use of metering connection by DB</p>	<p>Could offer customers “direct load control” - i.e. a remote way to switch appliances on or off (e.g. remotely control pool pump according to price signals).</p>	<ul style="list-style-type: none"> • Need policy decision re whether this use <i>should</i> be allowed. The answer is probably ‘yes’ given the systemic benefits, however we would suggest only with express customer consent. • Suggest consultation with consumer groups to inform policy decision and draft industry guidance (including that consent must be freely given, not conditional and not bundled into standard contract).

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 2.1 (Use) Use of consumption data by DB</p>	<p>DBs could use consumption data for marketing energy efficiency advice, products or services.</p>	<ul style="list-style-type: none"> Consumer communications need to explain direct load control options - now and likely future.
	<p>NPP 2.1 (Use) Use of consumption data by RB</p>	<p>Can structure customer billing according to time of use. Could offer more targeted advice to customer re energy efficiency / cost saving measures (e.g. time-shift your appliance use to save \$).</p>	<ul style="list-style-type: none"> Consumer communications need to explain TOU billing options - now and likely future. Need policy decision re whether this secondary use <i>should</i> be allowed - probably 'yes'. Need legal opinion (and consultation with Privacy Commissioner) regarding whether this is a <i>directly related secondary use</i>; if not, will need customer consent or legislative override to allow it. Best privacy practice: (a) assume it is <i>not</i> a <i>directly related secondary use</i>, and (b) get specific customer consent to allow it. Recognise slippery slope from targeted advice to direct marketing. Suggest consultation with Privacy Commissioner and consumer groups to inform policy decision and draft industry guidance (including that consent must be 'free', not conditional or bundled into standard contract).

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
		<p>Could offer targeted products or services (e.g. X brand TV will use less energy than your current TV).</p>	<ul style="list-style-type: none"> Recognise slippery slope from targeted advice to direct marketing. Need policy decision re whether this secondary use would be allowed - probably 'no' except with specific consent from customer. Suggest consultation with Privacy Commissioner and consumer groups to inform policy decision and draft industry guidance. Note ESC Marketing Code only covers activities leading to a contract - we suspect this means just a contract for the sale of energy, so the Code may not cover marketing by incumbent retailer of extra services or products (IHDs, appliances, etc).
	<p>NPP 2.1 (Use) Use of data by AEMO</p>	<p>Risk of secondary use.</p>	<ul style="list-style-type: none"> Review ESC Marketing Code (and incorporate into NECF): extend coverage to DBs; ensure coverage of "exempt" RBs; ensure coverage of marketing activities re extra services or products (IHDs, appliances etc); consider a ban on marketing messages delivered via IHD. AEMO appears unlikely to use the data for secondary purposes - no recommendation.
<p>Misuse of data</p>	<p>NPP 4.1 (Data Security) Security of data when 'at rest' at DB</p>	<p>Risk of breach by external attack. Risk of misuse by rogue insider.</p>	<ul style="list-style-type: none"> At least some RBs store data offshore; many people in each DB and RB business can see consumption data; audit logging their access may not be industry-wide.
	<p>NPP 4.1 (Data Security) Security of data when 'at rest' at RB</p>	<p>Risk of breach by external attack.</p>	<ul style="list-style-type: none"> DPI to review options further for setting industry-wide minimum information security
		<p>Risk of misuse by rogue insider.</p>	

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 4.1 (Data Security) Security of data when 'at rest' at AFMO</p>	<p>Risk of breach by external attack. Risk of misuse by rogue insider.</p>	<p>requirements (e.g. into a new Privacy Charter or Code), such as:</p> <ul style="list-style-type: none"> ○ DBs: should quarantine customer names (used for RoLR events and ensuring physical site access) from interval data ○ DBs and RBs: should audit log all access by users to interval data ○ DBs and RBs: retention of data aged two to seven years to be subject to more limited access rights.
<p>Disclosures of data</p>	<p>NPP 2.1 (Disclosure) To parties partnered with an RB</p> <p>NPP 2.1 (Disclosure) To third party service providers (e.g. financial counsellor, energy analyst, demand aggregator or home automation service)</p>	<p>Disclosures beyond consumer expectations.</p> <p>Disclosures beyond consumer expectations.</p>	<ul style="list-style-type: none"> ● Privacy notices need to mention any routine disclosures. ● Note that current policy / regulatory setting (NER Ch 7) does not allow direct third party involvement. However consumers can request the data for themselves, and then pass it on to their chosen third party service provider.¹³ <ul style="list-style-type: none"> ● When in future consumption and/or appliance data is to be sent from RB to the third party service provider, specific consumer consent should be obtained, and only for the purpose of providing a service back to the consumer (this will require a change to NER Ch 7).

¹³ It would be privacy enhancing for consumers to be given the data themselves and to subsequently pass it on to third parties if desired, as this maximises transparency and control, yet it may not be practical. Experience of third party services [1] shows the attractiveness of automated data handling.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	NPP 2.1 (Disclosure) To researchers, auditors etc.	Poorly handled disclosures create new privacy risks and erode trust.	<ul style="list-style-type: none"> DBs and RBs to develop standard protocols for managing requests for data from researchers, auditors etc.
	NPP 2.1 (Disclosure) To law enforcement	Poorly handled disclosures create new privacy risks and erode trust. Disclosures beyond consumer expectations.	<ul style="list-style-type: none"> DBs and RBs could have standard protocols for managing requests for data from law enforcement agencies. Privacy notices (see below) need to mention potential disclosure for law enforcement purposes.
Customer access via RB	NPP 6.1 (Access) Authentication of the customer online	Risk of illegitimate access by someone other than authorised customer.	<ul style="list-style-type: none"> Protocols will need to be developed to allow appropriate authentication of customer online, when HAN binding processes are formalised.
	NPP 6.1 (Access) Accessibility of the data	Data must be meaningful and useful.	<ul style="list-style-type: none"> Protocols to be developed for RBs to give customers their data on request, in a standard format (e.g. Excel spreadsheet).
	NPP 4.1 (Data Security) Security of the online portal	Risk of breach by external attack.	<ul style="list-style-type: none"> DPI could commission independent TRA of online portals, and communicate results through consumer channels.
The HAN	NPP 4.1 (Data Security) Security of data in transmission to the HAN	Risk of breach by external attack: consumption data.	<ul style="list-style-type: none"> DPI could commission independent TRA of ZigBee system, and communicate results through consumer channels. Consumer communications (e.g. FAQs) to note that smart meters' HAN functionality is off by default, and needs a special signal from the DB to activate.
	NPP 4.1 (Data Security) Security of the HAN	Risk of breach by external attack: register of smart appliances bound to HAN.	<ul style="list-style-type: none"> DPI could commission independent TRA of ZigBee system, and communicate results through consumer channels.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 4.1 (Data Security) Unauthorised access to data in the HAN</p>	<p>Change of occupancy: risk that new customer may access old customer's data.</p>	<ul style="list-style-type: none"> There are arguments for and against making past meter data available to new occupants. On one hand, meter data should be regarded as PI pertaining to old occupant; on other, new occupants have interests in efficiency indicators. There is some precedent in the way past electricity bills are now made available to buyers/renters. The AMI program should work with consumer groups to resolve the balance of interests. Protocols must then be developed by BPPWG to control new customer accessing data (relating to old customer's consumption or appliances) retained in the meter or HAN - e.g. RB must tell DB on move-out; DB should delete data in the meter at some point.
		<p>Change of occupancy: risk that old customer may continue to access or control appliances.</p>	<ul style="list-style-type: none"> Consider amending the NECF or NER to ensure this protocol is legislated. Old customer must not be able to control HAN or appliances after moving out. Protocols to be developed by BPPWG to ideally automatically un-bind devices from the meter when customer changes; e.g. RB must tell DB on vacancy; DB must change the access code for the HAN. Consider amending the NECF or NER to ensure this is legislated.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 4.1 (Data Security) HAN to IHD or other personal device (e.g. smart phone or PC)</p>	<p>Risk of illegitimate access by someone other than authorised customer.</p> <p>Consumer choice.</p>	<ul style="list-style-type: none"> Protocols to be developed to allow binding of devices to the meter with appropriate authentication of customer, NMI and HAN / device, without compromising the security code held by the DB. Consumer communications to explain different options re use of the HAN. Consumer communications to explain if/when a DB or RB could tell if you have a home alarm system (only if you tell them or you bought it from them) or if the alarm is on or off (only if you also give them access to your real time data from the HAN).
	<p>NPP 1.1 (Collection Necessity), NPP 4.1 (Data Security) HAN to RB to customer</p>	<p>Necessity of additional collection of appliance data by the RB.</p> <p>Necessity of additional collection of real time consumption data by the RB.</p>	<ul style="list-style-type: none"> RB might need to know types of other 'smart' appliances connected to the HAN for doing direct load control. Otherwise, the collection or generation of this information should be prohibited under industry protocols. Any solution must recognise that complete customer benefits cannot be realised without a program which combines (i) real time consumption data (from the HAN rather than via the daily transfer from the DB) and (ii) real time tariff info (from the RB). RBs get the consumption data anyway for wholesale and billing purposes, although delayed by a day.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
			<ul style="list-style-type: none"> Further investigation is needed of opportunity to develop software for consumers which retrieves consumption data from the HAN, and retrieves up-to-date tariff and other price/energy messages from the RB, without sending consumption data from the HAN to the RB.
			<ul style="list-style-type: none"> If considered necessary to send consumption data from HAN to RB, specific consumer consent should be obtained, and only for the purpose of providing analytics back to the consumer.
	Risk of illegitimate access by someone other than authorised customer.		<ul style="list-style-type: none"> Protocols to be developed by BPPWG to allow linking of HAN to RB.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 2.1 (Use), NPP 4.1 (Data Security) HAN to third party service provider (analyst or home automation service) to customer</p>	<p>Additional risks (data security, misuse, secondary use, data mining etc) posed by allowing additional organisations (some of which may not be conventionally registered market participants) to see any or real time consumption data.</p> <p>Necessity of additional collection of 'appliance' data by the third party.</p> <p>Risk of illegitimate access by someone other than authorised customer.</p>	<ul style="list-style-type: none"> Further investigation needed of opportunity to develop software for consumers which retrieves consumption data from the HAN, and retrieves up-to-date tariff and other price/energy messages from the RB, without sending consumption data from the HAN to any third party. Note that current policy / regulatory setting does not allow third parties to receive data from industry, but they can get it from customers. If considered necessary to send consumption data from HAN to third party analyst, specific consumer consent should be obtained, and only for the purpose of providing analytics back to the consumer. <ul style="list-style-type: none"> Further investigation needed of which third parties might need to know types of other 'smart' appliances connected to the HAN (e.g. perhaps home automation systems would need to know this, but not competing retailers, energy use analysts or financial counsellors) If not needed, the collection or generation of this information should be prohibited under industry protocols. <ul style="list-style-type: none"> Protocols to be developed to allow linking of HAN to third party analyst.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
Accountability	Coverage of NPPs	Some participants may not be covered by NPPs (e.g. new market entrants with turnover <\$3M pa).	<ul style="list-style-type: none"> Use some regulatory mechanism (e.g. NECF, NER, ESC Regs or Vic AMI Program Specs) to require all RBs to opt-in to NPPs if not already covered. Note the ESC Code of Conduct for Marketing Retail Energy in Victoria (Jan 2009, part 6) already requires RBs to comply with the NPPs in relation to their marketing activities.
	Enforcement of NPPs	Consumer groups not happy with (lack of) enforcement of NPPs in other sectors.	<ul style="list-style-type: none"> Engage consumers further in development of other options; e.g. should complaints instead be dealt with through an industry code, industry ombudsman or the AER?
	NPPs are not prescriptive	Industry and consumers will seek interpretation of the NPPs.	<ul style="list-style-type: none"> Consumer communications to clarify complaint-handling options / processes / contact details.
Transparency	Consumer involvement	Consumers not involved in technological trials.	<ul style="list-style-type: none"> The current ESC Regulation requires each RB to develop its own “Privacy Principles”; this may lead to confusion re terminology (most are already bound by legislated Privacy Principles, the NPPs) and inconsistency in the detail. An industry-wide “Privacy Charter” (policy-based) or “Privacy Code” (an enforceable regulatory document created under the NPPs) may be a better option, or something under the NECF. Involve consumer groups (both tech-savvy and tech-wary) in trials of IHDs.

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
		<p>Consumers not involved in developing communications.</p>	<ul style="list-style-type: none"> • Involve consumer groups (both tech-savvy and tech-wary) in the AMI Communications Working Group. • Ask consumer groups to provide input re consumer needs and concerns. • Use a professional communications firm to develop a draft communication strategy, including a staged approach and outreach via consumer NGOs. • Ask consumer groups to review draft communications strategy, and to review draft consumer messages.
	<p>Program is opaque</p>	<p>Public not clear who does what or why program is necessary.</p> <p>Written messages come from DBs but generate calls to the RBs.</p>	<ul style="list-style-type: none"> • Need uniform consumer/public-facing brochure to clearly explain the technology (the what), the program (the why: benefits to community now, individual benefits later), the rollout (the when/where/who), and the future (the what next) as well as who to contact for more info or with different types of complaints. • Need FAQs on privacy and security. Include diagram on data flows, and clarity that no identifiable data goes to government. • Communications to be Government-branded (rather than DB or RB-branded). • Refresh the smart metering website (http://new.dpi.vic.gov.au/smart-meters).

Broad privacy issue	Sub-issue	Particular issue	Possible responses and solutions
	<p>NPP 1.3 (Notice) Notice</p>	<p>Lack of privacy notices to consumers re interval metering as a new data collection.</p>	<ul style="list-style-type: none"> Develop plain language layered privacy notices for consumers, to be included in ongoing rollout-date messages. Notice to refer to brochure, FAQs etc (see above). Include brochure (see above) in mail-out re rollout-date message. Need a program to send brochure to households where meters already installed (e.g. by RB with next bill).
	<p>NPP 5 (Openness) Publication</p>	<p>Lack of transparency causes mistrust.</p>	<ul style="list-style-type: none"> Consider publishing extracts of TRA reports. Consider publishing PIA report in full, or extracts.
<p>Choice</p>	<p>Consent</p>	<p>Customer choices must be freely made, and able to be changed at any time.</p>	<ul style="list-style-type: none"> Protocols to be developed to allow customers to easily understand their choices (e.g. choice to turn on the HAN, use a third party service provider, etc), and to easily exercise / change those choices.

Part 5: Recommendations

A summary of findings

- Technically, privacy controls are relatively strong in the AMI program. Metering data is suitably protected in transit and at rest, and is subject to confidentiality provisions in the ESC's codes and licensing regime, as well as the NER. The industry has adopted good information security standards and practices. The security of smart meters themselves is well designed; in particular, the wireless communications links between meters and Distribution Businesses, and between meters and Home Area Networks, appear very sound. All wireless links are encrypted, and unlike domestic wifi networks which have proven problematic for drive-by snooping, smart meter encryption cannot be disabled. There are also strong security governance practices; it is not currently possible for third parties to obtain metering data without being licensed participants, or without having commercial arrangements with e.g. a Retail Business. For the time being, these barriers put a brake on metering data function creep.
- Yet there has been generally poor communications to consumers of the privacy realities of smart metering – a state of affairs that is part of a pattern of sparse and narrow communication focused on the mechanics of the rollout rather than the benefits and broader features of the system. A spectrum of privacy anxieties has been allowed to build up in the community, many of which prove not to be substantive, but all of which need to be treated seriously and respectfully.
- Industry participants, especially Distribution Businesses, tend to have a narrow understanding of *Personal Information*, namely believing that PI generally relates to explicit customer records. In reality the legal definition is much broader, covering any information where the identity of an individual is apparent or may be readily determined.
- While most metering data is keyed by NMI and does not contain explicit names and address details, we find that metering data can potentially be re-identified using other, albeit separate, databases which Distribution Businesses have in-house. It is difficult to make a case that metering data *could not be* Personal Information.
- Many retailers and distributors at this time are implementing new customer databases, in response to the need to handle vastly increased volumes of metering data.
- Historically, customer data seems suitably protected at Retail Businesses. All RBs interviewed for this PIA described similar internal regimes of customer service personnel training, privacy policies, and access controls over customer databases.

- In contrast with large government customer databases operated for health & welfare, driver licensing and the like, where the availability of high grade customer records inevitably leads to a finite level of abuse, RBs and DBs reported no known experience of abuse by insiders of Personal Information.
- Detailed interval data must be accessible to customer service personnel at Retail Businesses, in order to assist them to resolve customer billing inquiries and complaints. On the other hand, such access provides new opportunities for corruption because from now on it exposes detailed behavioural information about consumers, which may be useful to criminals.
- With a seemingly negligible incidence of abuse, not surprisingly interviewees were unsure of the auditing that may be conducted of how staff use the customer databases, nor of the inherent auditability of the systems. We infer that auditability of databases (to track which customer records are accessed by which staff at which times) may not be a high priority for RBs and DBs.

Suggested privacy considerations for DPI and the industry

To demonstrate good faith to consumers and the public, the AMI program in general should promote a precautionary approach to privacy.

- If metering data was handled in accordance with the National Privacy Principles, it would provide tangible acknowledgment by the industry of community concerns. Rather than debating technicalities around the precise definition of Personal Information, it may be better to concede that DBs in many cases are able to associate name and address with NMIs, and that metering data therefore merits a stronger duty of care than appears to be the case at present.

The infrastructure implications of adopting this stance should be relatively minor because there are reasonably high levels of security already in place. However, it would be wise for all players to refresh their Privacy Policies to more clearly explain how they treat and manage metering data.

- An Opt-In policy for all secondary usage of metering data would go a long way to improving the community's perceptions of privacy in the AMI program and would lay the foundations for safer sharing of data with the many third party services seeking to participate in smart metering.
- The need for such high volumes of redundant metering information to be retained across RBs and DBs as well as AEMO should be revisited.

- While information security management standards are well practised, the industry might do more to adopt minimum security policy settings for protecting interval data against misuse, such as auditing of customer database access (see also *Other recommendations* below).
- Without harming the competitive nature of the industry and the ability of businesses to differentiate themselves according to service and so on, the industry could consider crafting consistent text for inclusion in layered privacy notices, to help ensure that all consumers have the same basic appreciation of smart metering, especially if the NPPs are adopted, and if secondary use of metering data is agreed to be managed on an Opt-In basis.

Suggested privacy considerations for Distribution Businesses

- DBs should apply the precautionary principle to the way they handle data. While it can be argued that metering data keyed by NMI is not identified as such, it is not difficult for DBs to associate NMIs with consumers. Therefore DBs should strengthen the way they handle all metering data.
- While confidentiality is already required by ESC and is assured via security standards, DBs should take a broader view of privacy, and invest more effort in explaining to customers the purpose of smart metering, the ways in which metering data is used and disclosed, the regulatory and operational measures that protect the data, and the rights than consumers [will] have to control the flow of data.
- DBs should review and update their Privacy Policies accordingly. Such a review would constitute a good response to the ESC’s final decision that requires development of “privacy principles” for HANs.
- Because the potential for abuse by rogue insiders of customer records is likely to rise when they come to include interval data and behavioural indicators, DBs should ensure that customer database use is auditable and is in fact routinely audited.

Suggested privacy considerations for Retail Businesses

- RBs should review their Privacy Policies in response to the ESC’s final decision that requires development of “privacy principles” for HANs.
- Because the potential for abuse by rogue insiders of customer records is likely to rise when they come to include interval data and behavioural indicators, RBs should ensure that customer database use is auditable and is in fact routinely audited.

Suggested privacy considerations for future third parties

- Consider that all secondary use of metering data—regardless of how useful it may arguably be for efficiency advice, load management and so on—should be subject to express customer consent, and use this strict Opt-In model to engender consumer trust.

- Be sensitive to the fact that sections of the community are especially anxious about surreptitious re-use of Personal Information (given unfortunate experiences such as the covert collection of home wifi network data by Google Street View cars) and make an effort to offer explanations of how metering data moves through the system, and why.

The critical recommendations

1. All metering data from or about residential meters should be handled throughout the AMI system in accordance with the 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.
2. Privacy Policies of Distribution Businesses and Retail Businesses 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.
3. Even though details of how third party services and 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 IHDs are deployed.

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 AMP 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.

5. A fresh awareness campaign should be mounted to improve consumers' understanding of smart metering and privacy. The campaign should be centred on a commitment by all organisations involved in AMI to (a) complying with the NPPs in the handling of metering data, and (b) not putting metering data to any secondary use without the consumer expressly opting in.

Specific messages for consideration are provided under “Other recommendations” below.

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 NMI 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.
7. Consideration should be given to a review of the National Electricity Rules to consider (a) whether duplicate interval data really needs to be kept in triplicate at Distribution Businesses, AEMO and Registration Businesses, and (b) if it is really necessary to keep all the data at the half-hourly granular level. From a privacy perspective, some aggregation after two years would be preferable.
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.
9. The ESC should consider reviewing the Electricity Marketing Code with a view to extending it to cover Distribution Businesses and other parties potentially making use of metering data. In particular, the Code may need to clarify a broader meaning of “marketing” beyond the formation of new retail contracts. The review should come before the possible incorporation of the Code into the NECF.

Other recommendations

10. The recommended awareness campaign could be coordinated by a reenergised AMI Communications Working Group. The campaign might include fresh letters to householders, new FAQs and other materials that would best be defined in detail by communications professionals.
11. New messaging about smart metering privacy should probably come from government, to lend it authority and credibility, and because there is not a widespread understanding in the community of the role of electricity distributors and retailers, or even awareness of all the players. Further, the new government’s past undertakings to review the AMI program makes it logical for an appropriate Minister to lead the new messaging.

12. The awareness campaign should consider promoting the following privacy positive features of AMI:
- existing regulations and sanctions under the NERs, ESC and so on that protect consumers against abuse of metering data
 - the purpose of interval data collection
 - how TOU pricing works
 - the meaning of the flashing lights
 - the policy of Recommendation 4 (*to be confirmed*) that all secondary uses of metering data shall be subject to express consent
 - how direct load control works
 - security measures taken to protect meters, detect tampering etc.
 - security measures taken to protect access to consumption data
 - the absence of name and address details in transmitted metering data, which is identified only by NMI
 - the governance measures that control HANs and restrict access
 - the extent to which any party can tell if a home alarm system is present
 - the fact that all meter-to-DB communications and all HAN traffic is encrypted.
13. Processes may need to be developed, with assistance from consumer groups, for granting incoming residents access to defined aspects of past previous residents' meter data. Technical protocols will be needed to inform DBs and to delete old meter data at some point. This action should take into account NPP 4.2 (Security: Data Retention). Some amendment to the NECF or NER may also be needed.
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).
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.
16. Require that small Retail Businesses that might otherwise fall below the SME criterion for the Privacy Act expressly opt in to the NPPs with the Office of the Privacy Commissioner.

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.
18. In order to support future options for sending consumption and/or appliance data from Retail Businesses to third party service providers (with specific consumer consent as recommended above) a change to NER Chapter 7 should be considered.
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 forms such as Excel spreadsheets.
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 note that very recent regulatory developments in California have raised security standards for smart meters, with new requirements coming to conduct regular security audits [19].
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.
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.
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.
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.

References

A.1 Project documents

- [1]. *Customer information frameworks enabled by AMI Rev 1.0*, Impaq Consulting, 4 November 2010
Filename: Attachment 3 DPI-AMI-Customer Information Research Paper.docx
- [2]. *Minimum AMI Service Levels Specification (Victoria)*, DPI, Rel 1.1, 2008
Filename: Attachment 1 Minimum AMI Service Levels Specification Victoria Release 1-1.pdf
- [3]. *Minimum AMI Functionality Specification (Victoria)*, DPI, Rel 1.1, 2008
Filename: Attachment 2 Minimum AMI Functionality Specification Victoria Release 1-1.pdf
- [4]. *Overview of AMI Services*, Graham Dawson, DPI, 27 May 2011
Filename: Attachment 4 Overview of AMI Services.pptx

A.2 External documents

- [5]. *Regulatory Review – Smart Meters Final Decision*, Essential Services Commission, September 2010
<http://www.esc.vic.gov.au/NR/ronlyres/C6055E17-A851-4F2A-8050-EE2B4464203D/0/FDPSSmartMetersRegulatoryReview20100831.pdf>
- [6]. *Review of the advanced metering infrastructure program – Issues paper for public consultation*, Department of Treasury & Finance, May 2011
<http://www.esc.vic.gov.au/NR/ronlyres/C6055E17-A851-4F2A-8050-EE2B4464203D/0/FDPSSmartMetersRegulatoryReview20100831.pdf>
- [7]. *Business Process and Procedures Working Group Education Forum Objective & Scope* 11 April 11 v05 Peter Egger, BPPWG Leader
[http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/AEMOattachment2/\\$File/AEMO%20attachment%202.pdf](http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/AEMOattachment2/$File/AEMO%20attachment%202.pdf) (accessed 27 June 2011)
- [8]. *Submission to the Essential Services Commission on Smart meters*, Office of the Victorian Privacy Commissioner, 17 May 2010
[http://www.privacy.vic.gov.au/privacy/web2.nsf/files/smart-meters-submission-2010/\\$file/submission_05_10_no1.pdf](http://www.privacy.vic.gov.au/privacy/web2.nsf/files/smart-meters-submission-2010/$file/submission_05_10_no1.pdf)
- [9]. *Electricity Customer Metering Code*, Essential Services Commission, April 2011
<http://www.esc.vic.gov.au/NR/ronlyres/ECE60361-2D94-4AAF-807A-B32B7014B0E7/0/RIElectricityCustomerMeteringCodeApril201120101101.pdf>
- [10]. *ZigBee PRO Smart Energy API User Guide* JN-UG-3059, NXP Laboratories, Revision 2.0, 24 November 2010
http://www.jennic.com/files/support_files/JN-UG-3059-ZigBee-PRO-Smart-Energy.pdf

- [11]. *National Electricity Rules* Version 43, Australian Energy Market Commission, April 11 available from <http://www.aemc.gov.au/Electricity/National-Electricity-Rules/Current-Rules.html>, accessed 30 June 2011
- [12]. *Electricity Industry Act 2000* (Vic)
- [13]. *Privacy Act 1988* (Cth)
- [14]. *Privacy Amendment (Private Sector) Act 2000* (Cth)
- [15]. *Charter of Human Rights and Responsibilities* (Vic)
- [16]. *Privacy notices code of practice*, UK Information Commissioner's Office, 2010
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx
- [17]. *Consumer Principles for Home Area Networks and Direct Load Control*, Version 1.0
Filename: BPPWG workshop 30 - Consumer principles for HAN.pdf
- [18]. *Origin announces Australia's first large-scale pilot of a 'smart home' solution* Media Release 20 May 2011
<http://www.originenergy.com.au/news/article/asxmedia-releases/1299>
(accessed 22 July 2011)
- [19]. *Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas & Electric Co., Southern California Edison Co., and San Diego Gas & Electric Co.* Public Utilities Commission of California, 28 July 2011
http://docs.cpuc.ca.gov/WORD_PDF/AGENDA_DECISION/140188.pdf
- [20]. *Information About Your New Electricity Smart Meter*, Citipower Powercor Australia
Filename: AMI Notification Card and Cover DRAFT PowercorCitiPower.pdf
- [21]. *Smart Meter Fact Sheet*, SP AusNet
Filename: FactSheet-SmartMeter_FINAL PDF.pdf
- [22]. *Important information about the installation of your new Smart Meter*, Jemena
Filename: JEN - Smart Meter Introduction II.pdf
- [23]. *Important Information Regarding Your Electricity Supply*, Citipower PowerCor CitiPower Letters FINAL.pdf
- [24]. *Public Notice to Customers (Shire of Nillumbik)*, SP AusNet
Filename: NCASP528_PublicNoticeCustomers_185x130mm_WEBN2.pdf
- [25]. *Important information about the installation of your new Smart Meter*, United Energy Distribution
Filename: UED - Smart Meter Introduction II.pdf
- [26]. *Notice of Personal Information Management Policy*, United Energy Distribution
http://www.ue.com.au/privacy/download/personal_information_management_statement.pdf

A.3 Other sources

- <http://www.esc.vic.gov.au/public/Energy/Regulation+and+Compliance/Decisions+and+Determinations/Smart+meters+regulatory+review/Smart+meters+regulatory+review.htm>
- <http://www.dtf.vic.gov.au/CA25713E0002EF43/pages/dtf-projects-review-of-the-advanced-metering-infrastructure-program>
- <http://www.esc.vic.gov.au/public/Energy/Regulation+and+Compliance>
- <http://www.aemc.gov.au/Electricity/National-Electricity-Rules/Current-Rules.html>
- <http://epic.org/privacy/smartgrid/smartgrid.html>
- <http://share.aemo.com.au/smartmetering/Document%20library/Forms/AllItems.aspx>
- <http://www.zigbee.org>
- http://www.humanrightscommission.vic.gov.au/index.php?option=com_k2&view=item&layout=item&id=764&Itemid=515
- <http://stopsmartmeters.org>

Appendix: National Privacy Principles

NPP 1 Collection

- 1.1 *An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.*
- 1.2 *An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.*
- 1.3 *At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:*
- (a) the identity of the organisation and how to contact it; and*
 - (b) the fact that he or she is able to gain access to the information; and*
 - (c) the purposes for which the information is collected; and*
 - (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and*
 - (e) any law that requires the particular information to be collected; and*
 - (f) the main consequences (if any) for the individual if all or part of the information is not provided.*
- 1.4 *If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.*
- 1.5 *If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.*

NPP 2 Use and disclosure

- 2.1 *An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:*
- (a) both of the following apply:*
 - (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;*
 - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or*
 - (b) the individual has consented to the use or disclosure; or*
 - (c) [sub-clause relates to direct marketing and is not applicable; or*
 - (d) [sub-clause relates to medical research and is not applicable] or*

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(ea) [sub-clause relates to genetic information and is not applicable] or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 [sub-clause relates to bodies corporate and is not applicable].

2.4 [sub-clause relates to health service providers and is not applicable].

2.5 [sub-clause relates to health service providers and is not applicable].

NPP 3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

NPP 4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2.

NPP 5 Openness

- 5.1 *An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.*
- 5.2 *On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.*

NPP 6 Access and correction

- 6.1 *If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:*
- (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or*
 - (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or*
 - (c) providing access would have an unreasonable impact upon the privacy of other individuals; or*
 - (d) the request for access is frivolous or vexatious; or*
 - (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or*
 - (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or*
 - (g) providing access would be unlawful; or*
 - (h) denying access is required or authorised by or under law; or*
 - (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or*
 - (j) providing access would be likely to prejudice:*
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or*
 - (ii) the enforcement of laws relating to the confiscation of proceeds of crime; or*
 - (iii) the protection of the public revenue; or*
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or*
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its order*
- by or on behalf of an enforcement body; or*

- (k) *an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.*
- 6.2 *However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.*
- 6.3 *If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.*
- 6.4 *If an organisation charges for access to personal information, those charges:*
- (a) must not be excessive; and*
 - (b) must not apply to lodging a request for access.*
- 6.5 *If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.*
- 6.6 *If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.*
- 6.7 *An organisation must provide reasons for denial of access or a refusal to correct personal information.*

NPP 7 Identifiers

- 7.1 *An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:*
- (a) an agency; or*
 - (b) an agent of an agency acting in its capacity as agent; or*
 - (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.*
- 7.1A *However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.*
- 7.2 *An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:*
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or*
 - (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or*

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

7.3 *In this clause:*

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN is not an identifier.

NPP 8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

NPP 9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

NPP 10 Sensitive information

10.1 *An organisation must not collect sensitive information about an individual unless:*

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

- (i) is physically or legally incapable of giving consent to the collection; or*
- (ii) physically cannot communicate consent to the collection; or*
- (d) if the information is collected in the course of the activities of a non profit organisation—the following conditions are satisfied:*
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;*
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or*
- (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.*

10.2 *Despite subclause 10.1, an organisation may collect health information about an individual if:*

- (a) the information is necessary to provide a health service; and*
- (b) the information is collected:*
 - (i) as required or authorised by or under law (other than this Act); or*
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.*

10.3 *Despite subclause 10.1, an organisation may collect health information about an individual if:*

- (a) the collection is necessary for any of the following purposes:*
 - (i) research relevant to public health or public safety;*
 - (ii) the compilation or analysis of statistics relevant to public health or safety;*
 - (iii) the management, funding or monitoring of a health service; and*
- (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and*
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and*
- (d) the information is collected:*
 - (i) as required by law (other than this Act); or*
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or*
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.*

10.4 *If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de identify the information before the organisation discloses it.*