Australian Government
Office of the Australian Information Commissioner

Essential Services Commission
Level 2/35 Spring St
MELBOURNE VIC 3000

Dear Commissioner Cavagna and Commissioner Hartley

Draft Report: *Smart Meter Privacy Impact Assessment*

The Office of the Australian Information Commissioner (the OAIC) thanks the Essential Services Commission (the ESC) for the opportunity to comment on the *Smart Meter Privacy Impact Assessment Draft Report* (the Draft Report).

The OAIC considers that ESC has made recommendations that will strengthen the protection of consumers' privacy.

The OAIC would like to take this opportunity to highlight a number of additional better privacy practice opportunities. Our comments are set out below.

Auditing Process

ESC Recommendation 1 states:

> *'In the short term all industry participants should be audited, and then as compliance is assured, audits should be limited to those participants who generate complaints.'*[1]

The OAIC supports the recommendation that retailers and distributors should be required to conduct an independent audit of their compliance with the National Privacy Principles (NPPs), set out in Schedule 3 to the *Privacy Act 1988* (Cth) (the Privacy Act), before the roll out of smart meters is completed or, if that is not practicable, as soon as possible thereafter.

However, the OAIC considers that limiting subsequent audits to those participants that generate complaints may result in several unintended and undesirable outcomes:

- It may create a disincentive to report data breaches, particularly in the absence of mandatory data breach notification requirements.

[1] *Smart Meter Privacy Impact Assessment Draft Report* (2012), Essential Services Commission www.esc.vic.gov.au/Energy/Smart-Meter-Privacy-Impact-Assessment at 30 May 2012, 23.

- It may not adequately protect consumers in circumstances where they may be unaware of breaches.

- It may result in uneven compliance with the NPPs across the sector.

The OAIC takes the view that better privacy outcomes are achieved if all participants, not just those the subject of complaints, are subject to ongoing assurance measures including audits. Further, as smart meter technology develops, the associated data handling practices will likely also evolve. The OAIC considers that there should be scope for the assurance measures to evolve in parallel with the evolution of the technology and its applications. An audit program could form a key component of the assurance measures.

The Draft Report also states that the Victorian Department of Primary Industries may wish to commission another privacy impact assessment after smart meters have been in operation for five years.[2] For large or lengthy projects, conducting a privacy impact assessment may be an iterative process, with a number of privacy impact assessments done at various stages of development or as project design evolves. The OAIC considers that it is particularly desirable that this approach is taken in respect to smart meters because of the large amount of data that will be collected, and the potential for the data to be used for additional purposes over time.

Third Parties and Accredited Persons

The OAIC supports the ESC's recommendation that all third party providers that access and store customers' metering data should be encouraged to opt-in to the NPPs and the jurisdiction of the OAIC.[3]

The ESC also suggests that the Victorian Department of Primary Industries could develop and publicise a standard contract dealing with information privacy protection to be used by third party providers not subject to any privacy compliance regime.[4] The OAIC supports the development of contract terms that would require third party providers to implement privacy protections, including where they have chosen not to opt in to the Privacy Act.

The ESC notes that the Victorian Energy Efficiency Target Scheme accredits people to install In-Home Devices and that there may be value in explicitly stating the particular laws that apply to accredited persons.[5] ESC Recommendation 7 states:

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

---

[2] *Smart Meter Privacy Impact Assessment Draft Report*, 22.
[3] *Smart Meter Privacy Impact Assessment Draft Report*, 23.
[4] *Smart Meter Privacy Impact Assessment Draft Report*, 23.
[5] *Smart Meter Privacy Impact Assessment Draft Report*, 23.

- *Further specify Privacy obligations as part of the process for seeking accreditation*

- *Amend or develop regulation to be able to suspend or remove accreditation for breaches of privacy.'*[6]

The OAIC understands that the ESC anticipates that accredited persons may expand their businesses to include services such as accessing and storing data from In-Home Devices. As such, the OAIC recommends that the accreditation process includes training about privacy laws. Including privacy training from the start may help avoid future complaints, and will promote better privacy practice.

Industry Code and Privacy Policy

Industry-wide Privacy Policy

ESC Recommendation 2 suggests:

> *'... that industry develop a common layered Privacy Notice that can be used as the basis for all organisations involved in AMI; and consider developing an industry-wide Privacy Policy (perhaps as an Industry Code to be approved by the Privacy Commissioner).'*[7]

The OAIC also notes that the Draft Report provides that the policy should be made accessible to consumers, and drafted in plain English.

The OAIC supports, in principle, the establishment of an industry-wide privacy policy. Such a policy could be expected to help ensure consistency between providers and reduce confusion amongst consumers.

We note that the Draft Report provides that the policy should contain *'the contact details for the business, [and] the OAIC...to facilitate complaint handling'*.[8] The OAIC advises that, under the Privacy Act, the Commissioner must not investigate a complaint if the complainant has not first approached the organisation to which the complaint relates, unless it was not appropriate to complain to that organisation.[9] Accordingly, if an industry-wide privacy policy was developed, and the policy included the contact details of the OAIC, the OAIC would suggest that the policy clearly state that complaints should be addressed to the relevant organisation before complainants contact the OAIC.

The OAIC also recommends that the policy note that the OAIC may only investigate organisations that fall within the jurisdiction of the Privacy Act, and that not all industry participants may be within that jurisdiction (for example, small business operators that have not opted into the NPPs and the OAIC's jurisdiction).

---

[6] *Smart Meter Privacy Impact Assessment Draft Report*, 36.
[7] *Smart Meter Privacy Impact Assessment Draft Report*, 26.
[8] *Smart Meter Privacy Impact Assessment Draft Report*, 25.
[9] *Privacy Act 1988* (Cth), s 40(1A).

In response to Lockstep Recommendation 14, the ESC notes:

> *'To enable easy updating of Policies to reflect new and changing secondary data uses, we recommend that Retailers consider making their Privacy Policy primarily available in electronic from, with print versions provided on request.'*[10]

We consider that it would be better privacy practice if the privacy policy was provided on organisations' websites in a prominent position, and also to consumers upon formation of service contracts. Further, consumers should be notified when updates are made to the privacy policy.

Use of an Industry Code as an Industry-wide Privacy Policy

The development of an industry code is a comprehensive and potentially lengthy process. The OAIC has developed specific guidance on Privacy Code Development which discusses the process in detail.[11]

The ESC should also be aware that on 24 May 2012, the Attorney-General, Nicola Roxon, introduced the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Privacy Amendment Bill) into Parliament.[12] If passed, the Bill will, amongst other things, make significant changes to the provisions of the Privacy Act relating to industry codes.

The OAIC is concerned about the proposed use of an industry code as an industry-wide privacy policy. The OAIC considers that industry codes and privacy policies generally have different purposes, and different audiences. Specifically, an industry code is designed to establish operational parameters for code subscribers. An industry code may provide too much detail and complexity for the purposes of consumers seeking information about the handling of their personal information. It may be that consumers would benefit from a simpler, more concise privacy policy.

Consent to Secondary Data Uses

ESC recommendation 2 states that the industry code or privacy policy should include:

> *'A list of examples of secondary uses according to the current practice of each business, and provision to expand as new uses are introduced.'*[13]

ESC recommendation 4 expands on this:

---

[10] *Smart Meter Privacy Impact Assessment Draft Report*, 33.
[11] *Privacy Code Development* (2001), Office of the Australian Information Commissioner www.privacy.gov.au/materials/types/guidelines/view/6482#c6 at 31 May 2011.
[12] Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth).
[13] *Smart Meter Privacy Impact Assessment Draft Report*, 26.

'We support the Opt-In process for customers consenting to the secondary use of metering data. We recommend that the process used by Industry for obtaining customer's consent to the use of their 'Personal Information', including metering data from smart meters, should be structured to permit consent to separate secondary data uses over time as new products and capabilities are developed for the market.'[14]

The OAIC notes that NPP 2.1 relevantly provides that organisations subject to the Privacy Act must not use personal information for a 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

... [emphasis added]'

In the view of the OAIC, individuals could not reasonably expect that their personal information might be used for products and services that have yet to be developed at the time their consent was provided. The OAIC is firmly of the view that a general catch-all provision in the documents seeking initial customer consent does not sufficiently cover future uses. New products and services that would require the use of personal information collected for another (distinct) purpose should be subject to separate, specific consent.[15]

ESC Recommendation 4 continues:

'A customer's express consent should not be required for secondary purposes exempted by the AMI Policy Committee and uses stipulated by required legislation.'[16]

The Draft Report specifies that this may include the requirement to monitor consumption data to assist customers experiencing hardship, ensure supply to customers with medical dependence on life support, and to provide energy advice on a customer's bill.[17]

---

[14] *Smart Meter Privacy Impact Assessment Draft Report*, 30.
[15] *Privacy Act 1988* (Cth) Sch 3, National Privacy Principle 2.
[16] *Smart Meter Privacy Impact Assessment Draft Report*, 30.
[17] *Smart Meter Privacy Impact Assessment Draft Report*, 30.

The OAIC considers that consumption data that discloses the use of medical equipment (including life support devices) could potentially be 'health information' within the meaning of the Privacy Act.

Any secondary use of personal information should comply with NPP 2, which provides that organisations may only use personal information for a secondary purpose in listed circumstances. Specifically, in relation to the collection of health information, NPP 2.1 relevantly provides that an organisation may only use or disclose health information for a secondary purpose where the individual has consented,[18] where the secondary use is directly related to the primary purpose of collection,[19] or where the organisation has a reasonable belief 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 safety; or*
> ...'[20]

Compliance and Enforcement

In response to Lockstep Recommendation 16, the ESC recommends:

> *'... that the relevant industry regulator (whether the AER or OAIC) be empowered to take enforcement action should Retailers and Distributors not monitor their contractor's compliance. If not already explicit, this obligation would be incorporated into industry licensing or authorisation processes.'*[21]

The OAIC notes that the Information Commissioner will not have the power to take enforcement action unless contractors are within the jurisdiction of the Privacy Act (i.e., are 'organisations' within the meaning of the Privacy Act, or have opted-in to the NPPs). Where the Commissioner has jurisdiction, the Commissioner's relevant enforcement powers under the Privacy Act comprise the power to make a determination or, where a determination has been made as a result of a complaint, the ability to seek enforcement of the determination in the Federal Court.[22]

However, the Privacy Amendment Bill relevantly proposes that the Commissioner's powers under the Privacy Act be expanded to include the power to:

- impose a civil penalty for 'serious and repeated interferences with privacy'[23]

---

[18] *Privacy Act 1988* (Cth) Sch 3, National Privacy Principle 2.1(b).
[19] *Privacy Act 1988* (Cth) Sch 3, National Privacy Principle 2.1(a)(i).
[20] *Privacy Act 1988* (Cth) Sch 3, National Privacy Principle 2.1(e)(i).
[21] *Smart Meter Privacy Impact Assessment Draft Report*, 36.
[22] *Privacy Act 1988* (Cth) ss 52, 55A.
[23] Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), cl 13G.

- assess whether personal information held by an entity subject to the Privacy Act is being maintained in accordance with the Australian Privacy Principles (which will replace the NPPs)[24]

- accept written undertakings by entities to take, or refrain from taking, specified actions to ensure compliance with the Privacy Act,[25] and enforce those undertakings in the Federal Court or Federal Magistrates Court,[26] and

- include in a determination any order considered necessary or appropriate.[27]

Deletion of Data

The Draft Report states that the Victorian Department of Primary Industries has received advice that the *'customers should have responsibility to erase the IHD and all historical information if they wish to leave behind their IHD.'*[28]

ESC Recommendation 10 states:

> *'We recommend that a Protocol be developed to clarify the respective roles of customers, Retailers, Distributors and third party providers to protect customer data (by purging it from an IHD) at the time of unbinding from a HAN....We recommend that the unbinding process be an industry managed solution that does not rely on customer knowledge or memory to prevent wrongful access to another customer's data.'*[29]

The OAIC supports this recommendation. The OAIC notes that data stored by an In-Home Device could potentially include sensitive information such as health information, particularly if the In-Home Device had collected data related to the use of health-related equipment.

Individual Contracts within a Household

The OAIC supports ESC Recommendation 12, which recommends that consideration of the regulation of individual contracts within a household be delayed, as the details of the proposed contracts are currently unknown. We consider that continued monitoring of industry development in this area would be useful to inform later iterations of the privacy impact assessment on smart meters.

Aggregation and De-identification of Market Data

ESC Recommendation 6 states:

---

[24] Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), cl 33C.
[25] Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), cl 33E.
[26] Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), cl 33F.
[27] Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), cl 52(3A).
[28] *Smart Meter Privacy Impact Assessment Draft Report*, 40.
[29] *Smart Meter Privacy Impact Assessment Draft Report*, 41.

'Any regulatory obligation to provide data to the market should be clarified by the AER in terms of who bears this responsibility, time frame and detail having regard to the new paradigm presented by smart meters.'[30]

The OAIC recommends that any review or clarification consider organisations' responsibilities under NPP 4. NPP 4 provides:

'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 National Privacy Principle 2.'

The OAIC is concerned about the privacy implications of retaining data on meters for 200 days, and National Electricity Rules that require retention of metering data for seven years.

The OAIC supports the ESC's suggestion that appropriate privacy protections could be achieved through the aggregation and anonymisation of data after a reasonable period of time.[31]

Possible Continuing Issues

The Lockstep Privacy Impact Assessment (the Lockstep PIA) discusses a series of community concerns that have not been addressed in the ESC Recommendations.

Flashing Meter Lights

The Lockstep PIA draws attention to community concern that flashing lights are visible from the street when energy is in use, indicating whether people are home or not. Lockstep recommends a consumer education campaign to inform consumers of the meaning of the flashing lights.[32]

The OAIC considers that more detailed information should be provided in the PIA on the purpose of the lights, and potential actions that industry could take to mitigate the risk posed by the lights.

Release of Data to Potential Property Purchasers

The Lockstep PIA discusses the potential issue of the release of energy data to purchasers of premises.[33] The OAIC considers that data about the energy use of

---

[30] *Smart Meter Privacy Impact Assessment Draft Report*, 32.
[31] *Smart Meter Privacy Impact Assessment Draft Report*, 32.
[32] Lockstep Consulting, *PIA Report Advanced Metering Infrastructure (AMI) Version 1.2*, (2011) Department of Primary Industries Victoria, www.dpi.vic.gov.au/smart-meters/publications/reports-and-consultations/lockstep-dpi-ami-pia-report at 30 May 2012, 35.
[33] Lockstep Consulting, *PIA Report Advanced Metering Infrastructure (AMI) Version 1.2*, 44.

individuals is potentially personal information, and should be distinguished from the energy efficiency of specific premises which could be assessed without the release of personal information. The OAIC recommends clarification of when and why personal information would be released in this manner, and whether such disclosure would be authorised under the NPPs.

Direct Marketing

Lockstep predicts that InHome Devices could be used to provide more targeted advice to customers in relation to energy efficiency and cost saving measures, and has questioned whether this would be a secondary use directly related to the primary purpose of collection that would be permitted by NPP 2. The OAIC agrees with the Lockstep recommendation that better privacy practice would be to assume it is not a related or directly related secondary use, and that organisations should obtain specific customer consent.[34]

Once again, thank you for the opportunity to comment on the Draft Report. I hope our comments are of assistance. If you have any questions or concerns, please contact Melanie Drayton, Director – Policy, on (02) 9284 9682 or at Melanie.Drayton@oaic.gov.au.

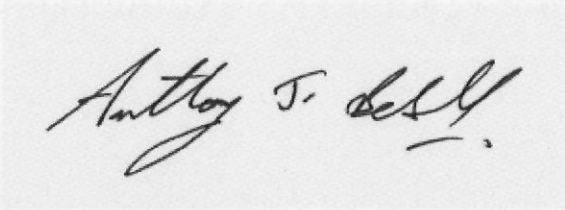
Yours sincerely

Rachael Spalding
Assistant Commissioner Policy
18 June 2012

[34] Lockstep Consulting, *PIA Report Advanced Metering Infrastructure (AMI) Version 1.2*, 40.

While the majority of organisations involved in the smart metering scheme will fall outside of the jurisdiction of the *Information Privacy Act 2000* (Vic), the Victorian Privacy Commissioner has a general function to examine matters that affect the privacy of Victorians. I support and endorse the comments of the OAIC in this submission which I consider will strengthen regulation relating to the handling of personal information collected by smart meters.

Office of the
Victorian Privacy
Commissioner



Dr Anthony Bendall
Acting Victorian Privacy Commissioner