



Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Essential Services Commission

on

Smart meters

17 May 2010

The Privacy Commissioner wishes to acknowledge the work of Jason Forte (Policy and Compliance Officer) in the preparation of this Submission.

Office of the Victorian Privacy Commissioner (Privacy Victoria)

GPO Box 5057

10-16 Queen Street

Melbourne Victoria 3000

Australia

Phone: 1300-666-444

Fax: +61-3-8619-8700

Email: enquiries@privacy.vic.gov.au

Website: www.privacy.vic.gov.au

1. Introduction

1. The Essential Services Commission (ESC) has called for submissions in relation to the implementation of advanced interval metering (“smart meters”).
2. It is acknowledged that smart meters may be advantageous to both consumers and electricity providers by allowing consumers to manage their electricity use better and allowing providers to offer discounted rates for certain time periods (such as off-peak usage). It is suggested that smart meters will also improve efficiency by allowing electricity providers to manage electricity loads across grids.
3. Despite these advantages, smart meters have the potential to impact severely upon the privacy of individuals who have smart meters installed. These concerns go to the very heart of a right to privacy, given that smart meters collect detailed usage data in an area which is usually “off limits” – a person’s home. I acknowledge that unless a premises is singularly occupied, usage data from a smart meter will not identify individual usage; nevertheless, the data has the potential to be privacy intrusive.
4. Any encroachment into the privacy of a person’s domicile should be treated seriously and should only occur when absolutely necessary. Indeed, this principle is espoused in section 13 of the Victorian *Charter of Human Rights and Responsibilities*, which states that a person has the right not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with.
5. Smart meters, incorrectly implemented and regulated, run the risk of interfering with a person’s privacy. Accordingly, I note the following privacy concerns:

2. Privacy implications of smart meters

6. A person’s electricity usage data is not, by itself, “personal information”. However, by linking usage data to a customer’s account, which will list at the very least the customer’s name, address and contact details, information about a customer’s behaviour may be gleaned from the usage data. This is potentially intrusive where the use or disclosure of usage data goes beyond the primary purpose for which it is collected.
7. Given that a smart meter measures usage every half hour and communicates back to the electricity retailer, any person with access to usage data would be able to determine patterns of use which indicate personal details or behavioural traits of occupants of the house. For example, if an occupant’s usage shows minimal data over a period of several days compared with previous usage, it may be inferred that the occupant(s) are absent from their residence. Usage data could also be used to determine when the occupant uses certain appliances, when they wake, when they sleep, when they shower and so forth. 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. One can envisage situations where law enforcement agencies or insurance companies would desire this information as well.

8. The ESC Issues Paper does not specifically address how the data gleaned from smart meters will be used, disclosed or accessed by third parties in the future, apart from specific billing uses. With this in mind, it is my view that strict data security measures should be implemented to ensure that any secondary use is restricted, or that where possible an individual expressly consents to such usage.
9. Strict data security measures should also be implemented in relation to the transfer of data between the smart meter and the electricity provider. While the Issues Paper seems to suggest that smart meters use “two-way communications” to transmit usage data to the provider, how this occurs and to where the data is communicated is not made clear. Data should be encrypted and secure to avoid interception, and should only be sent to parties who require the information. Where customers are permitted to access their usage information online, security should also be of utmost concern.
10. The ESC should also consider in what way it can restrict or prohibit misuse of usage data (by, for example, employees of an electricity provider).
11. There is also the question of how long and in what manner an electricity provider should keep usage information. Under the current system, customers have a right of access to data within the last two years; however, it is possible that historical usage data may be kept by an electricity provider for longer periods of time so it may be used for other purposes. Given the granular detail of usage data, de-identification may not be sufficient if the provider intends to keep the information for longer than is required for billing. In any case, aggregating or cross-referencing data obtained from smart meters with other databases should be limited, if not prohibited, given that a person may be easily identifiable from usage data.
12. I acknowledge that metering data is currently classed as “confidential” under the Electricity Metering Code. However, it is unclear whether this will be sufficient to protect against the above concerns.

3. Other jurisdictions

13. As noted in the Issues Paper, smart meters have been implemented in Ontario, Canada, as well as other jurisdictions. In November 2009, the Information and Privacy Commissioner in Ontario published a white paper entitled “*SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*”.¹ The Ontario Information and Privacy Commissioner’s paper raises similar privacy concerns in relation to smart meters as this submission, and suggests that, at first instance, privacy should be “built-in” to all physical, administrative and technological aspects of the system. The Commissioner was of the view that earning the trust of

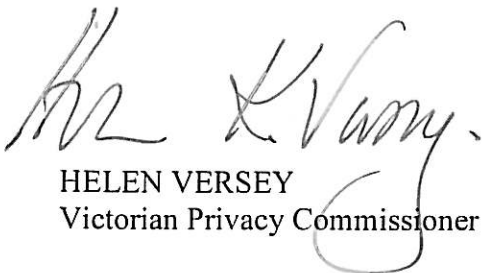
¹ Available from the Information and Privacy Commissioner of Ontario’s website: <http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf>

consumers was crucial to ensuring that consumers see the value of time and investment in the “smart grid”. The Commissioner also stated that the emergence of smart electricity use is an opportunity for commercial entities to improve methods by which the providers convey their data use practices to consumers so that consumers can make fully informed decisions regarding use of their information.

14. I agree that this is an important juncture in which privacy protections should be integrated with the smart electricity system so that it operates securely. Accordingly, the ESC should keep in mind privacy concerns at all times so that consumers can still obtain the benefit of smart meters while having, by default, control of their personal information.
15. The Ontario Commissioner also notes that “smart” appliances are becoming increasingly common. Smart appliances are appliances which can feed into the smart grid, some of which share information with smart meters. Whilst there has not been a suggestion that the smart meters being implemented in Victoria will interact with smart appliances, it is worth noting that when more smart appliances become available in Victoria, similar privacy concerns will be raised in terms of how usage information is shared between smart meters, appliances and the grid.

4. Conclusion

16. It is my view that any amendments to regulations regarding smart meters should ensure that the collection and retention of personal information and usage data is kept to a minimum where possible. If the information is to be disclosed to or shared with third parties, the express consent of the customer should be required wherever possible (“opt-in” rather than “opt-out”).



HELEN VERSEY
Victorian Privacy Commissioner

