MARCHMENT HILL
- consulting -

Meter data –a matter of privacy?

Smart meters, or indeed any form of time-of-use (TOU) meter, produce significantly more information about consumption patterns than the monthly or bimonthly read accrual meters. This information becomes powerful in terms of the ability to determine localised and customer-specific consumption information. It can be used for:

- Time-of-use pricing, which may better reflect NEM prices
- Influencing customer behaviours around pricing signals to encourage more low-cost off-peak power consumption and less peak consumption
- Demand side management to help shave high peaks through customer awareness and pricing
- Customer segmentation, including identifying customers who may benefit from education on how to reduce electricity costs
- Related energy services for customers (such as energy audits which can highlight the devices that are contributing to load at a particular time each day, thereby optimising the customer's load profile according to cost or another driver selected by the customer, retailer or network business

However, access to the meter data information – for purposes other than metrology – may also provide information to market participants, and possibly third parties, that may not be in the best interest of the customer. Information could be garnered as to the customer's usage patterns or appliance ownership, knowledge which could be valuable to certain parties. What then, should be done to ensure a customer's meter data is used only for the purposes it was intended and for which the customer agrees it can be used?

Recent media reports broadcasted significant customer concern over the installation of smart meters, particularly fears over privacy. But what are the sources of these fears and what are the potential outcomes of misuse of customer data? Is there a need for concern and, if so, what can be done about it?

"What ... should be done to ensure a customer's meter data is used only for the purposes it was intended and for which the customer agrees it can be used"

MHC perspective

Non-metrology uses for customer meter data

Customer time-of-use meter data information can clearly provide detailed information about customer usage patterns and, possibly, the appliances installed at the customer's premise. This can potentially:

- Classify customers through appliance ownership (e.g. wealthy, early adopters of technology or potential marketing targets)
- Initiate marketing activities by Distributors or Retailers (or third parties) based on either customer behaviour or appliance ownership. This activity may be seen by customers as either welcome, or unwelcome. Potential for sale of such behavioural or appliance ownership data (even if data is cleansed to meet specific criteria) to third parties may provide an additional (unregulated) revenue stream for Distributors or Retailers
- Raise questions about 'vulnerable' customers' energy usage (e.g. is the customer receiving too much welfare or are they spending time and money watching TV rather than buying food?) Can this customer segmentation lead to offers of social assistance or attract penalties?
- Identify and possibly penalise (through higher electricity rates) customers who do not change their electricity usage – not just through potentially larger time-of-use bills but unwanted attention by the Distributor or Retailer to further change their electricity usage. This may affect customers whose behaviour is relatively inelastic, such as shift workers or families with many children, and
- Correlate metering data with other forms of customer behaviour (e.g. linking a customer coming home late at night with credit card expenditure at a nominated venue, possibly leading to higher insurance premiums).

Unless they are prepared to be publicly scrutinised, it may be safe to assume that businesses overseen by an ombudsman or customer protection codes (such as Distributors and Retailers) are unlikely to use non-metrology data for purposes other than its intended use, without the appropriate permissions.

Compared to the infrequently-read accumulation meters, Distributors and Retailers will be holding much more data on their customers, making customer data more attractive, possibly to unauthorised third parties. This could include relatively benign parties (such as rival retailers) but could also include those with a more sinister motive (such as criminal activity). How, then, can we prevent this data from being accessed in ways it was not intended?

"Compared to the infrequently-read accumulation meters, Distributors and Retailers will be holding much more data on their customers, making customer data more attractive, possibly to unauthorised third parties."

Clearly, there are a number of issues to be considered in preventing unauthorised access to data. Security on the wide area network used to transmit customer data is paramount. Furthermore, security on the HAN (where enabled) used to provide data to the customer's own devices must be properly managed. Smart meters allow for

personal information to be stored in the meter itself, such as the account holder or last bill amount etc. There must be appropriate means for managing the data stored within the meter itself, including deleting security keys on move in/move out or on change of retailer. Distributors must be satisfied that this is sufficiently allowed for in the ZigBee Smart Energy Profile or other protocols used to transmit this data.

Despite high-level security, recent corporate data security breaches highlight the need to effectively prevent unauthorised access. Numerous security systems have been bypassed, including for example the breach of Sony's PlayStation network.

Appropriate consideration should be given to ensure that meter data is not shared with a third party unless the information is necessary to support a third party service that the customer has agreed to purchase. If this is the case, customers should be made aware of the information that the third party is entitled to access without the customer's explicit consent. The recently passed United States Electric Consumer Right to Know Act (e-KNOW) may drive similar legislation in Australia that supports this and further protects the customer.

Is this a material problem?

In addition to electricity usage, customers expose their behaviours in many other ways: consider lighting in the house, use of credit cards, mobile phones, GPS units, tracking of internet IP addresses or the presence of a car in the driveway. Are the risks introduced with TOU metering and access to this data any more material than other customer activities?

There are much easier means for customer behaviour to be identified for sinister motives than hijacking metering data. Of more concern is the potential for additional unwanted marketing activity based on customer metering data. Are the existing customer protection legislations, such as the Australian Privacy Act or the National Privacy Principle, sufficient to protect a customer's rights? Is this established in all jurisdictions or should a national approach be considered? Is there a need to include provisions for parties with which a customer has a contract (i.e. Distributors and Retailers) to prevent unauthorised or unwelcome direct customer contact?

"Are the existing customer protection legislations ... sufficient to protect a customer's rights"

Final thoughts

If potential concerns around the use of metering data are to be addressed, it is paramount that Distributors and Retailers act within certain bounds so as to not compromise the use of this data. The existing protections available to customers must be reviewed for their appropriateness and if found lacking, then further protection needs to be established to both safeguard customers, and to assist them in understanding that their activities could provide behavioural information that might be used for unauthorised purposes. With these protections in place, the full benefits of accessing TOU metering data be realised, with the support of customers.