

For public release

26 May 2017

Public statement about bulk disclosure of smart meter data

Under section 13(1)(h) of the Privacy Act 1993, I have the ability to make a public statement about any matter affecting the privacy of an individual or classes of individuals. Smart meters raise potentially complex issues of involuntary collection and device-based surveillance¹ as well as the definition of personal information.²

Discussions with sector stakeholders (retailers, metering companies and distributors) between October 2016 and March 2017 have revealed that bulk disclosure of smart meter information is taking place under existing Use of System (UoS) Agreements.

Bulk disclosure of individual household level smart meter data risks infringing individual privacy, and damaging public trust in how the sector handles customer data.

In order to avoid these risks, New Zealand electricity distributors should, in summary:

- review their privacy statements and consider updating them to include assurances regarding the use of smart meter data;
- review whether the individual household level data currently being provided by retailers could be aggregated and still meet network planning needs;
- ensure that personal information is not collected unnecessarily, or held for longer than necessary; and
- aggregate meter data where individual household level data is not required to meet network planning needs e.g. through amalgamating half-hourly data from small groups of households, or by receiving the half-hourly data at the street level.

Regional retailers and metering companies could also benefit from reviewing their privacy statements and policies around smart meter data to ensure they accurately reflect how they use and disclose customer data.

¹ Case note on smart meters and personal information: <https://privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-251185-2015-nz-privcmr-3-use-of-smart-meters-by-utility-companies/>

² Advisory opinion issued to the New Zealand Fire Service about what constitutes personal information: <https://www.privacy.org.nz/news-and-publications/advisory-opinions/addresses-of-fire-incidents/>

Background

Between October 2016 and January 2017, my office received enquiries from several electricity retailers expressing concerns about bulk disclosure of detailed smart meter data to electricity distributors for network planning purposes.

Approximately 70% of households in New Zealand currently have smart meters and this is likely to increase to 90% within two years. These smart meters can automatically record and transmit power usage data in half hourly intervals, which can reveal significant detail about a household's movements and patterns. This is in comparison to traditional electricity meters, which tend to be used for monthly or even bi-monthly manual readings of total consumption. In its raw form, the data collected by smart meters is associated with an installation control point (ICP) number that identifies the meter itself, rather than any particular person. However, usage information collected from smart meters can become personal information once it is associated with an account holder. For instance, if a person were to claim to have been in their house at a given time, the meter data could provide evidence to support or disprove that claim.

A University of Auckland academic conducted a review of privacy and technology issues around smart meters and noted "There is general consensus that smart meter data should be managed according to the provisions foreseen for personal data".³

In 2011, the Article 29 Working Party, an influential body composed of privacy authorities from European Union member states, released a Working Paper, "Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy". The paper contained eight recommendations setting out an approach that ensured electricity consumers would have the privacy of their data respected without the need to take any specific actions (privacy by design). In particular it noted that "research has shown that utilities may not need detailed energy consumption information about individual consumers to perform load balancing functions. To achieve as little personal data flow as possible utilities may use techniques such as anonymisation, pseudonymisation, or data aggregation".

Following that paper, the EU Data Protection Supervisor prepared a 2012 opinion on preparations for the roll-out of smart metering, concluding: "considering the risks to data protection, one of the key pre-conditions for the rollout of smart metering systems is to ensure a high level of protection of personal data."⁴

Discussions with sector stakeholders

In discussions with my staff, retailers said their three key concerns about bulk disclosure of smart meter data were that:

- the disclosures, though made in accordance with UoS Agreements, were excessive

³ <https://www.cs.auckland.ac.nz/~asghar/papers/asghar12-smartgridsec.pdf>

⁴ https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

as distributors did not appear to need half hourly data at the individual household level in order to do network planning;

- the information may be insecurely stored by the distributors; and
- the distributors may use the data for purposes other than network planning.

The retailers were also concerned that, should the data held by the distributors be used inconsistently with the purpose for collection or inappropriately disclosed, they risked significant loss of customer trust and reputational capital as a result of actions that weren't in their control.

Electricity sector agencies have the following obligations under the Privacy Act 1993:

- principle 1 – individual households' data should only be collected where the collection is necessary for the agency's lawful purposes;
- principle 5 – reasonable steps should be taken to prevent data being accessed, used or disclosed in an unauthorised way; and
- principle 10 – data should not be used for purposes other than that for which it was collected unless an exception applies.

Staff from my office discussed the issue with the Electricity Authority, and were told that it supports efforts to improve security, clarity and transparency around information sharing in the electricity sector, such as by aggregating meter data, so long as this does not increase barriers to new entrants and innovative services or prevent better outcomes for consumers.

Staff from my office also met with representatives from electricity metering and distributing companies to discuss retailers' concerns. A representative from a metering company at these meetings stated that:

- metering companies would be an appropriate medium through which smart meter data could be aggregated and then passed on to distributors; and
- having retailers aggregate the data themselves before passing the information to metering companies could cause data quality issues especially if retailers act independently from one another and therefore do not apply a consistent standard.

Conclusion

A data breach or demonstrated misuse of such detailed and potentially sensitive data could lead to serious consequences for the individuals affected and retailer reputation. For instance, electricity usage tracks closely with house occupancy. If detailed usage information became publicly available it would be possible to track and anticipate a household's movements and use that information in ways the individuals neither expected nor wanted.

In order for distributors to carry out their role efficiently and cost effectively they require a certain level of detail about the network. However, based on my investigations it does not appear to me that they require household level data for network planning. Aggregating the half-hourly data, whether by street or even by small group of houses, would appear to meet both the retailers' concerns and the distributor's needs. If not, the onus would then be on distributors to demonstrate how more detailed information was necessary for them to carry out their functions effectively.

While the privacy interest in a given person's household level data is, in most circumstances, marginal, the privacy concerns being raised by retailers about bulk disclosure of data are genuine, particularly in the context of significant and growing threats to privacy from Internet of Things devices. Loss of trust from deliberate or accidental disclosure is likely to impact strongly on retailers. Finding a privacy-friendly solution is in the interests of both consumers and businesses.

In order to avoid this risk, while ensuring that retailers and distribution companies can continue to make appropriate use of customer data, I propose to NZ electricity distributors that they should:

- review their privacy statements and consider updating them to include assurances regarding the use of smart meter data;
- review whether the individual household level data currently being provided by retailers could be aggregated and still meet network planning needs;
- ensure that personal information is not collected unnecessarily, or held for longer than necessary; and
- aggregate meter data where individual household level data is not required to meet network planning needs e.g. through amalgamating half-hourly data from small groups of households, or by receiving the half-hourly data at the street level.

Regional retailers and metering companies could also benefit from reviewing their privacy statements and policies around smart meter data to ensure they accurately reflect how they use and disclose customer data.

Aggregating the half-hourly data by households would be one way of alleviating the privacy concerns identified by the retailers, allowing for provision of rich data while still protecting electricity consumers' reasonable expectations of privacy. Other solutions could be discussed with retailers and metering companies. If a satisfactory resolution can be arrived at that allows for provision of rich data while still protecting electricity consumers' reasonable expectations of privacy, it is unlikely I would need to consider taking more formal steps in relation to smart meters.

The retailers also brought to my attention some current research competitions that are using smart meter derived data to encourage innovation in the sector. I encourage and support research and innovation; however companies should be mindful of the ability of researchers or the public to re-identify the data they disclose. Retailers and distributors should also ensure any research initiatives have security protections against inappropriate access to data.

I am grateful to electricity retailers for bringing this matter to my attention and to other sector stakeholders for their cooperation.

Yours sincerely

John Edwards
Privacy Commissioner