Science and Technology Committee - Evidence Check Web Forum: Smart Meters

January 2016

Key Points

- **The amount of information given to consumers about smart meters varies between companies.**
- **Consumers should be asked to share a minimum amount of data as standard.**
- **The potential for mission creep is great; any changes must be fully explained to consumers.**
- **Citizens have to be reassured that their information will be kept secure, as well as what steps can be taken in the event of a breach.**
- **Any retention period must be properly justified.**

Information for the consumer

The project to roll-out smart meters to the general public has existed for a number of years. Whilst the emphasis has been on the financial and convenience benefits the scheme will bring, it is important that citizens are able to judge for themselves whether or not the scheme will be in their best interest.

In line with that, Big Brother Watch welcome the work which has been undertaken to ensure that the consumer is aware of the choices they have with regards to their energy data when using a smart meter.

However it is unfortunate that some companies are better than others at explaining to their customers the options available to them. Indeed some companies are not being completely clear that a smart meter is an option and not a service the customer has to sign up to. This is not acceptable. No customer should be obliged or feel forced to adopt a smart meter if they do not wish to.

Data choices for the consumer

The 'Rights and Choices' data guide document[1], used to inform the public about smart meters currently places emphasis on the consumer making informed choices, this is to be welcomed.

The document makes clear that the consumer can choose what level of data they are prepared to share with their supplier and with third party marketers about their energy consumption , and gives them the option to change their mind at any time.

[1] http://www.energy-uk.org.uk/files/docs/Policies/Smart%20Meter%20policies%20%20consultation%20responses/2013/smart_meter_data_guide_version_1-june-13.pdf

Should the customer choose not to change the basic settings it is understood that their data will be shared with the supplier on a daily basis. We would prefer that the basic setting shared the data on a monthly basis.

Mission creep

It is understood that currently only the customer can see the "*near real time*" use of their data using their In Home Display (IHD) this is welcomed. However the implied intention to "*pair*" smart meters with "*consumer access devices*" or to "*enable third party SME developers to offer innovative services*", including "*analysis or display of information on a smartphone*" as outlined in the 'Diagnosis and Plans' document accompanying this consultation, has the potential to fundamentally change who can access data.[2]

The 'Diagnosis and Plans' document also appears to suggest that "*as technologies evolve and consumers gain confidence with the opportunities offered by smart metering, data access roles may need to evolve*"[3]. This suggests that access to near real time data may not always reside solely with the consumer.

As with many new technologies the potential for mission creep raises a number of privacy and security concerns. These must be addressed quickly and clearly before they risk undermining the scheme as a whole.

The granular half hourly data which smart meters will generate can reveal when households are occupied and potentially enable inference of how many people live in a property. The "big data" opportunities for use of this data will be attractive to companies, organisations and researchers of varying kinds. However the intrusive nature of this data poses a significant risk to individual privacy, particularly if the data were to be hacked, stolen or abused or used for financial gain at the expense of the consumer.

Any move away from only the customer seeing this data must be consulted on broadly. Should new methods or devices be manufactured the consumer must be told that their data may, as a result, be accessible to the supplier and potentially other third party organisations such as app developers etc. and be given a clear choice to opt out.

Should Government departments or researchers wish to access this data now or in the future the data must be aggregated and it must be made clear to the customer what the data will be used for, who would be able to access it, how it will be accessed, stored and deleted before anything happens. The customer should have every opportunity to opt out of any scheme or research project which requires access to their data whether in an aggregated format or not.

Changes to data access or data sharing should not be seen as a logical next step which can naturally occur without transparent detail as to the benefits and pitfalls for the customer and without clear guidance on the necessity and proportionality of changes to the scheme.

---

[2] Smart Meters, Diagnosis and Plans, Paragraph 3, Page 1: http://www.parliament.uk/documents/commons-committees/science-technology/evidence-tests/smart-meters.pdf

[3] Ibid, Paragraph 14, Page 3: http://www.parliament.uk/documents/commons-committees/science-technology/evidence-tests/smart-meters.pdf

Security

Since the idea of smart meters was first presented the concept of connected technology and the internet of things has grown. With the move towards a completely connected society the issues of cyber security, cybercrime, data protection and encryption have moved up the agenda.

Cyber-attacks towards our national infrastructure are ever present. Last year former Chair of the Defence Committee Lord Arbuthnot was quoted as saying that "*Our National Grid is coming under cyber-attack not just day by day but minute by minute*."[4] The fact that other countries, such as the United States of America, have suffered hacks to their national grid demonstrates that this is a very real concern.

Whilst it is acknowledged that the data transferred between Home Area Network (HAN), the Smart Meter and the Wide Area Network is cryptographically protected, questions remain over the weakening of encryption and the threat of national, regional or individual cyber-attacks, all of which could make consumers personally identifiable data or the half hourly energy readings vulnerable.

Citizens must be reassured that their information will be kept securely, and what measures will be taken and what opportunities for recourse are available should their data be breached in any way.

Retention

As noted the information collected by smart meters can be very revealing. Clear information must be provided regarding how long the information will be stored for and what will happen to it, as outlined in the Data Protection Act 1998 and with an eye towards the General Data Protection Regulations which it is anticipated will replace that Act in the next couple of years. The need to properly justify any retention period is equally as important, evidence must be provided to show why the storage of information is necessary.

[4] Bloomberg Business, *Power Network Under Cyber-Attack Sees UK Increase Defenses*, 9th January 2015, http://www.bloomberg.com/news/articles/2015-01-09/power-grid-under-cyber-attack-every-minute-sees-u-k-up-defenses