April 2017
ISBN 978-1-922017-10-9

Smart Meters: What does a connected house really mean?

Key Findings:

- Smart meters are revolutionising Australian households, but while the energy sector is pedaling the benefits, the risks are not being fully communicated.
- Smart meters can either be one-way or two-way communication devices, with two-way devices being more expensive and less secure.
- Security, privacy and competition issues need greater consideration to fully realise benefits for consumers.
- As evidenced in Victoria, the introduction of electricity smart meters has not been a success based on cost-benefit analysis. Utilities introducing smart water meters can learn significantly from this experience.

Introduction

Smart meters electronically record water, electricity and gas usage and transmit this data to the utility operator in real-time. Smart meters are at the core of the global Internet of Things (IoT), and their communications abilities record and track details of water, electricity and gas usage in homes and businesses to increase the overall efficiency and reliability of an outdated and overburdened water, gas and electrical grid. It is important that any introduction of smart meters provides benefits for consumers and utility operators.

What is a Smart Meter?

A smart meter is a digital device located at a home or business that measures the amount of water, electricity or gas used, virtually in real-time. Unlike a traditional meter, a smart meter electronically reads and stores the usage of water, electricity or gas over short intervals and then remotely sends this information to energy distributors and retailers. Smart meters may operate in two formats. One is where there is a one-way transmission of data. That is, the amount of water, electricity or gas which is used is collected at a pre-set interval and transmitted to the provider. This is the most cost effective and secure method, which still provides significant consumer and operator benefits.

About the Author

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on strategic digital issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre is hosted within the Faculty of Business, Government & Law at the University. The University of Canberra is Australia's capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis

The second method, and that used most commonly in electricity installations is a two-way communication where not only is usage transmitted to the energy provider, but the electricity provider can also push data and instructions back to the meter. This method is more costly and opens up cyber security and privacy issues.

For the purposes of this research we will separate smart meters into two categories, electricity and water. These two categories are very distinct in how a smart meter may function, for example an electric smart meter already has power available, whereas a smart water meter requires power to be delivered. They are also at very different stages of roll-out in society, with smart electric meters already mandated in Victoria and at advanced stages in other jurisdictions, whereas smart water meters are very nascent in residential or commercial use.

The water industry, like many others, is currently undergoing a process of transformation through the use of ICT and near real time data generation. The aim is to increase operational and management efficiencies, whilst reducing expenditure and carbon footprint through smart water metering.

The Internet of Things

Smart meters will be at the core of the global IoT, and their communication abilities will record and track details of energy usage in homes and businesses in order to increase the overall efficiency and reliability of often outdated and overburdened utility networks. IoT covers quite an array of "things", and it is easy to become overwhelmed by the subject. Simply relating to objects that have networking connectivity, the IoT can bring many advantages to businesses of all shapes and sizes. And as the IoT enters our everyday world, it brings with it more opportunities for change and innovation.

Smart meters are a classic IoT advancement. It is predicted IoT will have an economic impact of more than $11 trillion per year by 2025.[i]

Electricity

Smart electricity meters generally offer two-way, digital communication systems that record electricity usage usually every 30 minutes, automatically sending this data to a customer's electricity distributor. The concept is to end estimated bills and manual meter readings. Having real-time usage allows consumers to change electricity suppliers without a manual meter reading. They are also designed to provide data that enable customers to make choices about how much energy they use by allowing them to access accurate real-time information about their electricity consumption, either through a web portal, smart phone application or an in-home display. Such access via interactive devices is designed to provide information about hourly, daily, weekly and seasonal consumption, so users can view their real-time energy usage.

Water

Smart water meters not only give residents an accurate and up to date picture on their water consumption habits, they also help utilities to detect thousands of potential leaks in their infrastructure and at properties potentially saving water and money.

Smart water meters have electromagnetic levels which are very low, using just 25mW power emission. Mobile phones use 80 times more (2,000mW) and Wi-Fi four times higher (100mW).[ii]

Why Introduce Smart Meters?

The smart water metering market emerged to provide near real time data and analytics to deliver more predictive and proactive services. The backbone of this effort is Advanced Metering Infrastructure (AMI) technology. AMI can provide a remote and constant data link between utilities, meters and consumers. Communications are delivered through various technologies including power line communications, telephony, broadband, fibre optic cable, wireless radio frequency and cellular transmissions.[iii]

The timely collection and analysis of water usage data, and the timely relaying of this data to the water user, can result in significant changes in water use behaviour. The benefits include immediate leak detection and consequent remedial action that can save precious quantities of water.

Smart electricity meters have been in existence for some time, but as has been seen from the Victorian government Auditor-Generals report, the supposed benefits to consumers have not been realised. Consumers have been slow to 'shop around' for better energy deals, which could be put down to lack of communications to consumers to notify them of their options, lack of real competition in the retail energy market and the inability for consumers to easily change from one provider to another. Whilst there are consumer protection laws to enable competition, the electricity market in particular is at the same stage as the telecommunications sector some decades ago prior to phone number portability being introduced.

Transmit and Receive

Smart meters work under one of two concepts. Those that only transmit data of household usage patterns and those that not only transmit this data, but can also receive data from the network. The majority of electricity meters contain two-way radios.

One-way meters which only transmit are the safest and most secure option. They are low in energy use (critical for water infrastructure where meters have to be separately powered), cheaper to manufacture (by a factor of six), still allow users to track their consumption via smart phone apps, are significantly more secure against cyber-attack and offer much better privacy protections.

Two-way meters, where the network can 'push' data to the meter open significant security and privacy issues. Hackers can compromise the smart meter (and where part of a smart-home infrastructure, cause much more damage) causing financial and potentially physical damage for only a very small benefit to the consumer. Utility providers can notify change of tariffs depending upon load and/or time of day whilst providing total energy services. Whilst this may seem desirable to some households, there is limited education provided on the informed consent consumers are providing, often making it hard for them to switch providers.

Water utilities often debate whether to fully convert to AMI or run an Automatic Meter Reading (AMR) water grid instead. The truest of smart water grid definitions requires AMI technology and its enabling two-way communications. Many water

utilities do not see a clear advantage of AMI on a cost-benefit analysis and discovered AMR is the most fit-for-purpose response. A modern one-way smart meter has a battery life of around 15 years, which is the life of the meter, whereas two-way, or AMI technology reduces this to around 8 years.[iv] In Victoria the single largest benefit category of the AMI program relates to the avoided cost of replacing and manually reading the old accumulation meters. However, accumulation meter costs have been replaced with AMI smart meter costs that are much higher.[v]

Receiving one-way information for accurate billing, leakage and non-revenue water detection solves the bulk of water utility needs. Apart from security and privacy considerations, practically speaking there is no need to send remote upgrades or other notifications to a house as centralised alarms will be sufficient and utilities will rarely (if ever) restrict water flows into homes, even if this may be legally permitted.

Essentially, one-way radio transmission is more secure for the customer.

Threats

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data, loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of- service attacks, and potential disruptions to critical infrastructure.[vi]

The threats from smart meters are broad with criminals having attacked insecure smart utility devices for a variety of purposes, in particular financial fraud. In Puerto Rico, criminals used laptops containing software widely available in the internet underground to make "service calls" to both businesses and the general public. For fees ranging from $300 to $1,000 for residential customers and $3,000 for commercial clients, these criminals successfully reprogrammed the smart meters in order to save its "clients" up to 75 per- cent off their monthly electricity bills. According to an investigation into the incident by the FBI, the Puerto Rican electrical and power authority affected lost nearly $400 million in revenues annually as a result. Like all computers, smart meters are also vulnerable to malware attacks, and security researchers at IOActive have devised a worm capable of rapidly spreading from one infected AMI smart meter in a home to another, eventually infecting a whole neighbourhood and plunging it into darkness.[vii]

This raises the issue of responsibility for security. For behind the meter scenarios (a house or business), there are many providers of smart meters and poor security, versus in front of the meter (the grid) there are fewer providers and much better security. The Australian energy sector is immature in this respect and requires a robust consumer protection framework which identifies and introduces controls for all risks involved.

Smart-meter information, much of which is transmitted in an unencrypted format, can reveal details such as the brand and age of your appliances and when you are using them in which rooms of your home. Extrapolating such data

reveals how much time you spend cooking and when you turn on the TV in the bedroom.[viii]

Researchers in Germany revealed that smart meters could also tell what television programs people were watching at what times, because of the specific electricity required to display the scenes of each show on the screen. By measuring these in the aggregate, the researchers were able to create individual profiles for all television programs, and it turns out episode 71 of *Star Trek* has a different power signature from episode 17 of *Modern Family.* Of course, there are potentially billions to be made selling this data to third parties. Indeed, in May 2014, WPP, the world's largest advertising agency, announced it was teaming up with the London-based data analytics company Onzo to study ways to collect smart-meter data in order to "open the door of the home" to advertisers.[ix]

Working hand in hand with a AMI smart utility meter will be a home's smart thermostat. Nest Labs has completely reimagined the clunky old thermostat, creating a Wi-Fi-enabled thermostat replete with cutting-edge sensors, including temperature, motion detection, humidity, and light. Nest employs adaptive artificial intelligence algorithms designed to learn what temperatures make people happy and when. Nest also has an auto-away mode that determines when there hasn't been any motion or light near the device, correctly deducing when residents are not at home. Nest has other products, such as its multi-sensor Wi-Fi-enabled smoke alarm. Just a few years after its founding, Nest was purchased by Google for $3.2 billion.[x]

Google clearly sees the opportunities in the Internet of Things, and Nest is a powerful hardware product to anchor its ambitions in the battle for what it is calling the "conscious home." But Nest thermostats and smoke detectors with all their embedded sensors are prodigious producers of data, and just as the Android mobile phones brought new advertising and data sales opportunities, so will Nest Labs products. Google now owns not only your Web searches, email, mobile phone, maps, and location but also your movements inside your own home.[xi]

An insecure and accessible smart meter is a great way to tell when homeowners are away for extended periods of time. Rather than search Facebook postings, burglars will just be able to tap into video feeds, query the refrigerator to see when the last time its door was opened, or simply ask the smart thermostat if it is in extended holiday mode. The Nest thermostat has already been successfully hacked allowing just that, giving hackers potential remote access to the device, including monitoring whether an owner is home via the embedded motion detector or even cranking up the heat full blast.[xii]

Privacy

The promotion of privacy issues and the importance of the protection of personal information is critical to ongoing functioning of the online environment. Today, almost all individuals have digital footprints, created via interaction on social networks, through web search, participation in e-commerce and other online activities. Technology can deliver significant benefits, but we need to take care: how our digital footprints are collected and managed by the organisations we have relationships with will have long term implications.

If there is one thing that's certain, it is that online interactions with customers can generate an amazing array of specific and general data which, depending on the service, such as a smart meter, can be tied to an individual.

There are many privacy concerns surrounding the collection and use of the information contained in the digital footprints we leave during online transactions. However to put this in context we need to understand the length and nature of the relationship between a customer and, for example, an e-commerce website, an energy retailer or utility company. We also need to understand how such information is collected and the context of which it is likely to be used.

Personalisation is a function of an organisation's knowledge of a customer. Collection of data will always warrant consideration of the privacy implications and concerns by consumers, businesses and regulators - and brings significant obligations to the entity collecting the data.

A consumer's decision to participate in an online transaction is a result of their own cost-benefit analysis. Product personalisation experiences must be clear to consumers allowing them to measure the vendor's reputation and allow them to value a more personalised service whilst contrasting privacy concerns. The previously mentioned Nest technology pushes the boundaries on this, where Google will integrate the information captured with other data such as web search or geo-location. Energy utilities and retailers need to fully explain the cost-benefit analysis to a consumer of two-way smart meter technology, including how a dwelling (and the people tied to it) will be identified and where appropriate anonymised; what future adjacent commercial services will be pushed to the consumer; and how they can opt out of future 'personalised' services in the future.

The *Privacy Act* 1988 regulates how personal information is handled. It defines personal information as:

…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.[xiii] As technology solutions for billing, customer service, asset management and modelling will become more advanced and offer a greater depth and accuracy in analytical ability, the definition of personally identifiable information needs to be broadened in this context, ensuring consumers with two-way AMI technology have greater control over the data their meter/s produce, whilst energy utilities and retailers enforce data sharing policies which are dynamic and context dependent. Critically does the customer:

- know what data is being collected?
- know what the data will be used for?
- know who will have access to it?
- give consent - informed consent - for its collection?
- have the ability to opt out of such data collection and still be able to use the service?

These questions are consistent with the trend towards personalisation and the notion that some of us may choose to provide information in exchange for better deals, better targeted products, and better services.

The February 2017 passing of the *Privacy Amendment (Notifiable Data Breaches) Bill* 2016 establishes a mandatory data breach notification scheme in Australia. This amendment will mean energy utilities and retailers covered by the *Privacy Act* need to notify any individuals affected by a data breach that is likely to result in serious harm – though these Entities will likely struggle to assess the seriousness of harm, given that individuals impacted by a breach may have varying tolerances for what is deemed harmful to them.

Additionally, the Office of the Australian Information Commissioner will be advised of these breaches, and can determine if further action is required. The law also gives the Information Commissioner the ability to direct a business to notify individuals about a serious data breach.

The new scheme will strengthen the protections afforded to a consumer's personal information, and is designed to improve transparency in the way that the public and private sectors respond to serious data breaches. It will also give individuals the opportunity to take steps to minimise the damage that can result from unauthorised use of their personal information.

Competition

The 2011 cost-benefit analysis for the Victorian role out of smart electricity meters estimated that $778 million of benefits associated with the uptake of flexible tariffs.

This was on the basis that 4 per cent of consumers would take up flexible electricity price offers, however, only 0.27 per cent have done so. There was a goal to reach 15 per cent uptake by end of 2017. Accelerating the uptake and benefits from flexible price offers relies on retailers providing better value-for-money options compared to the existing flat tariffs, and increasing consumer awareness of the availability and benefits of such offers.[xiv]

Improved communications to consumers, combined with 'plain English' information, much the same way as the finance industry provides easy to read information for their customers. Under the national energy retail law, energy retailers must offer fair contracts with clear terms and conditions so customers can understand the energy offer and provide a written summary of the offer (called an Energy Price Fact Sheet) when marketing to customers.[xv]

Building Public Trust in Data

A significant problem in cyber security is data manipulation. We are now in the era of Big Data, where organisations base pivotal decisions on information they collect, presume accurate and analyse. Assuring data integrity means securing the environments where it's stored, transmitted, and accessed.

Smart meters as part of the IoT-powered home provides many opportunities and threats for data integrity. Criminals are not only focused on data theft, but are now examining IoT's weaknesses to discover where data manipulation at the micro level can have the largest downstream macro impacts. The Mirai-based botnet attack – the first

comprised entirely of ordinary internet-connected home products such as digital video recorders and web cameras – of October 2016 directed huge volumes of internet traffic to cause a distributed denial of service attack. Typically, criminals looking to build a botnet have to find a way to infect tens of thousands of PCs with malware. In contrast, IoT devices are far easier to break into. And criminals can build much bigger botnets simply because of the larger number of devices that are available to exploit.[xvi]

Every digital home must have protected IoT devices. Manufactures must produce secure-by-design smart meters which can be patched and updated against known security vulnerabilities. Consumers need to be educated and empowered to change default user names and passwords of IoT devices, whilst acknowledging that two-way AMI devices increase security risks. Policy makers need to regulate device manufactures, making them accountable for securing their products.

Responses

As with all cyber security efforts, IoT risk mitigation needs to be a constantly evolving and shared responsibility between government and the private sector. Unfortunately, in a rush to market, many smart meter vendors are either not building in security-by-design or providing weak security protocols, including:

- Encryption keys using weak or outdated encryption methods.
- Pairing standards with no authentication required, allowing an attacker to simply ask the smart meter to join the network and receive keys in return.
- Hardcoded credentials, allowing administrator access with passwords as simple and guessable as the vendor's name.
- Code simplified to work on low-power devices skipping important checks, allowing nothing more than a long communication to crash the device.

There is also a role for government. Over the past 60 years governments have mandated cars to be safer, legislating for them to be equipped with seat belts, airbags, anti-lock brakes, etc. Now consumers look for the 'star' safety rating when buying a new car and make choices based on safety equipment. We need to bring this thinking into the online environment, particularly smart meters and develop digital security standards that generate a positive impact. A safe user experience should be coded into every connected smart meter.

*This research and analysis has been funded by Taggle Systems

Case Study: Victorian Government Introduction of Smart Meters

In 2006, the Victorian Government mandated the rollout of smart meters to all households and small businesses across Victoria. Consumers have been paying for this since 2009, not through tax dollars, but through additional charges applied to their electricity bills. When the rollout was announced, the benefits were promoted widely. However, when

the government reviewed the program in 2011 it was clear there would be no overall benefit to consumers, but instead a likely cost of $319 million. When the continuation of the rollout was announced, it was said to be the 'better option' for Victoria, but it was not made clear that this was based on excluding the costs that consumers had already incurred.

By the end of 2015, Victorians had paid an estimated $2.239 billion in metering charges, which includes the cost of the rollout and connection of smart meters. The Department of Economic Development, Jobs, Transport & Resources does not have a full understanding of the cost of the program, which it does not track.

Further, the single largest benefit achieved to date—which accounts for around 40 per cent, or $1.4 billion of the total expected $3.2 billion benefits from smart meters over the life of the program—relates to the avoided costs of accumulation meters for things such as their installation and manual meter reading. These costs are saved as smart meters replace the old accumulation meters, but they do not represent any additional value generated by the program. Furthermore, the overall costs of the smart meters program significantly outweigh these savings.[xvii]

Case Study: Mackay Regional Council

In 2011, challenged by a growing population increasing pressure on water infrastructure, Mackay Regional Council (MRC) was fast reaching capacity in its main water treatment plant. While one option was to build a new water treatment plant ($100M price tag), the non-capital solution identified was to better manage demand. Initial calculations indicated a 10% reduction in per capita consumption could likely delay the new plant by 4-5 years.

A demand management initiative was planned around that target, which included an extensive social marketing campaign, starting with a comprehensive consumer survey. Observing that outdoor water use was the major contributor to the peak demand in the critical dry season (which determined capacity requirements), the campaign focussed on watering lawns & using water-wise plants

An important element for the initiative was obtaining detailed information around usage patterns and water losses, of which MRC had little or no information. After much research into technology options, MRC settled on a Low Power Wide Area Network (LPWAN) communications platform from Taggle Systems, to enable automatic reading of its meters on an hourly basis. As an emerging technology, while LPWAN was identified as a higher risk option, it enabled MRC to achieve its objectives at a price point that facilitated a positive business case.

Increasing from 80,000 (approx. 40,000 meters twice a year) to around 300 million meter reads per year, required a specialised software system to deal with the large quantity of data.

The data analysed highlighted many aspects of consumption which were previously unknown. Identifying customers' water leaks and informing them quickly, resulted average leak duration reducing from 150 to 60 days.

The data has also helped MRC to significantly improve its level of consumer engagement. A dedicated customer portal enables consumers

to view their daily consumption, understand how they compare to their peers, and set up customised alerts to help manage consumption.

Daily per capita consumption (lpd), has dropped 15% from around 240 litres to 200. The $100M treatment plant, initially planned for 2022, has been pushed back to 2032. Capital deferment and cost efficiencies, have enabled MRC to freeze prices for water and sewerage for two years.

MRC's outstanding work was recognised in 2016, winning both national and international awards for transforming their water business.

---

[i] IBM. 2016. *The Internet of Things is changing the world*. https://www.ibm.com/blogs/internet-of-things/changing-world-iot/
[ii] Pearce, T. http://www.teresapearce.org.uk/2014/04/smart-water-meters-frequently-asked-questions-faqs/
[iii] Water & Wastewater International. Smart Water Meter Networks an Intelligence Network? http://www.waterworld.com/articles/wwi/print/volume-26/issue-5/regulars/creative-finance/smart-water-metering-networks-an-intelligent-investment.html
[iv] ibid
[v] Victorian Auditor-General. 2015. *Realising the benefits of Smart Meters*. http://www.audit.vic.gov.au/publications/20150916-Smart-Meters/20150916-Smart-Meters.pdf
[vi] U.S. Department of Homeland Security. *Strategic Principles for Security the Internet of Things*. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf
[vii] Goodman, M. 2016. *Future Crimes*. Random House
[viii] ibid
[ix] ibid
[x] https://nest.com
[xi] n 7. Goodman
[xii] ibid
[xiii] Australian Office of the Information Commissioner. *Privacy Act*. https://www.oaic.gov.au/privacy-law/privacy-act/
[xiv] n 5. Victorian Auditor-General
[xv] Australian Energy Regulator. *Managing Energy Services at Home*. Fact sheet
[xvi] Vijayan, J. *What you need to know about the botnet that broke the internet*. http://www.csmonitor.com/World/Passcode/2016/1026/What-you-need-to-know-about-the-botnet-that-broke-the-internet
[xvii] n 5. Victorian Auditor-General.