On the security economics of electricity metering

Ross Anderson and Shailendra Fuloria
Cambridge University Computer Laboratory

Abstract

Smart grids are a hot topic, with the US administration devoting billions of dollars to modernising the electricity infrastructure. Significant action is likely in metering, where the largest and most radical change may come in the European Union. The EU is strongly encouraging its 27 Member States to replace utility meters with 'smart meters' by 2022. This will be a massive project: the UK, for example, looks set to replace 47m meters at a cost of perhaps £350 each. Yet it is not at all clear what it means for a meter to be secure. The utility wants to cut energy theft, so it wants the ability to disable any meter remotely; but a prudent nation state might be wary of a facility that could let an attacker turn off the lights. Again, the utility may want to monitor its customers' consumption by the half hour, so it can price discriminate more effectively; the competition authorities may find this abhorrent. Other parts of government might find it convenient to have access to fine-grained consumption data, but might find themselves up against privacy law. There are at least half-a-dozen different stakeholders with different views on security – which can refer to information, to money, or to the supply of electricity. And it's not even true that more security is always better: some customers may opt for an interruptible supply to save money. In short, energy metering is ripe for a security-economics analysis, and in this paper we attempt a first cut. We end up with five recommendations for the regulation of a future smart meter infrastructure.

1 Introduction

There has been considerable interest worldwide in the concept of a "smart grid" – a more efficient and reliable infrastructure for the transmission and distribution of electricity. This term means different things to different people, and has attracted a lot of hype. As a working definition, we will take the smart grid to mean a future electricity distribution network that saves energy by matching distributed generation resources intelligently with demand; that enables consumers to save money by helping shave demand peaks; and that has a self-healing property which enables it to recover rapidly from failures. The concept became US policy with the Energy Independence and Security Act of 2007 and came forcefully to public attention when President Obama allocated $4.5bn to its development as the headline measure when he signed the American Recovery and Reinvestment Act [21]. The European Parliament followed with a 2009 law requiring member states to conduct an economic assessment of smart metering by 2012, and if they found it beneficial, mandate its use by 2022 (with 80% adoption by 2020) [15]. These mandates and their associated funding have led to a gold rush, with power companies, meter vendors, patent owners, Google and others jostling for advantage.

In this paper, our focus is on smart meters. While traditional meters measure cumulative energy use by day and night tariffs, and are typically read once each quarter, smart meters will be able to read energy use with much finer granularity (typically by half-hour time segments)

and also to communicate – both upstream to a head-end, operated by the energy company or the government, and downstream to a home area network. They will interact with the customer, whether through a display panel or a web service (the server might be either in the meter or at the energy company); the idea is that they will enable consumers to conserve energy and adapt usage to supply conditions. Electricity already costs more at peak times than domestic customers pay – in the UK, for example, they are charged about 50% more for daytime use than at night, while in wholesale markets the time-of-day price variation is about a factor of three. So if we could charge by the half-hour rather than the half-day, we could charge people more in the early evening peak, and get them to use less; peak demand shaving could save the utilities a fortune. The move to renewables, and particularly to solar and wind generators whose output fluctuates unpredictably, will further increase the incentives to modulate demand. Promoters of smart meters hope to use a mixture of voluntary and automatic mechanisms; the former include more fine-grained and variable tariffs, communicated to the customer via improved interfaces, while the latter include remote-control mechanisms for operating space heaters or charging electric cars at a time of the utility's choosing, and even turning off airconditioners during peak periods.

But smart meters raise a thicket of security issues.

1. The large volumes of data they can collect may raise acute privacy concerns; a court in the Netherlands, for example, has found a smart meter law there to be contrary to the European Convention on Human Rights [9].

2. The availability of fine-grained consumption data to utilities raises the prospect of predatory pricing and increased lock-in of their customers.

3. The existence of a remote off switch for the electricity (and gas) in everyone's homes raises the prospect of blackouts being caused by a nation state attacker, a terrorist or even a criminal group. However the main attraction for the energy companies is the ability to switch nonpaying customers to a prepay tariff; remote switch-off makes this possible by reprogramming the meter rather than replacing it. (Governments may also like to move people to prepayment as this generally cuts energy use.)

4. There is the fear that some governments might use targeted power cuts as a coercive measure to meet energy savings targets or pursue other policy objectives, such as punishing dissent (or perhaps illegal downloading).

5. There can be significant conflicts of interest between energy companies (which want to sell more energy) and governments (which want to meet supply security and carbon targets); these may work out through tussles for control of technical standards and/or usage data.

6. Finally, security standards wars have become the battleground for patent owners. The new Zigbee standard that will be used in the USA to enable domestic appliances to communicate with smart meters was going to mandate elliptic curve cryptography; this would have meant that Certicom will get a royalty of 7c on every appliance capable of communicating with an electricity meter. We now hear that this may be reconsidered by standards bodies.

In navigating this thicket, we hope that an analysis based on security economics might provide some useful guidance. In the rest of this section, we set out the historical background. We then move on to an analysis of the competing interests in Section 2, and finally move to recommendations in Section 3.

1.1 The early years

Until the late 1870s, electricity was used only in specialised applications such as telegraphs and arc lighting. After inventing the incandescent electric light bulb in 1879, Edison set out to develop an electric system that would provide a source of power for a mass market. Once his Pearl Street Power plant began spinning in New York City on September 4, 1882, about 85 customers in lower Manhattan could receive enough energy to light 5,000 lamps. He initially charged a flat fee per lamp; this turned out to be unsatisfactory. Mechanical meters had existed since 1872, when Samuel Gardner had patented one based on a clock that was started and stopped by an electromagnet; but this measured only time. Edison invented a meter consisting of a jar holding two zinc plates: each month the electrodes were weighed and the customer billed according to the change in their weight. This at least measured ampere-hours rather than just hours, but was not very robust [10].

The commercial exploitation of electricity really took off when George Westinghouse developed the alternating current (AC) system in the mid-1880s; this allowed power to be stepped up and down in voltage so that it could be transmitted over distances with only moderate losses. He built a hydro power station at Niagara Falls in 1896 and transmitted the electricity to Buffalo, 20 miles away. This won him the "war of the currents", an early standards race [6]. The metering part of his technology package arrived in 1885, when Galileo Ferraris of Turin discovered that out-of-phase AC fields could make a solid disc rotate. This paved the way for the induction motor and the watt-hour meter, which was developed by Shallenberger and marketed by Westinghouse from 1888. The next decade saw rapid meter innovation to cope with varying voltages and power factors, and patent fights between Westinghouse and Edison's company General Electric until they eventually signed a cross-licensing agreement in 1896. In 1899, GE introduced the first prepayment meter. There was a further wave of innovation after the initial patents expired in 1910. And after a long series of mergers and acquisitions, there are now four large metering companies that dominate world markets: Landis+Gyr, GE, Itron (formerly Schlumberger's metering division), and Elster (formerly ABB's metering business). For more on the engineering history, see [10].

Although the AC mechanism was much more efficient for transmission and distribution than DC, the technology of a hundred years ago limited transmission to a few hundred miles. Thus, by the early 1920s, energy networks mostly operated in local pockets: each utility supplied electricity to its local city or neighbourhood and was completely isolated from others. Thus each utility was vertically integrated, responsible for electricity generation, transmission, distribution to customers and subsequent billing.

In the early years, electricity was not a necessity but a luxury: people got electric light not just to read books in the evening but to show off to their neighbours. The utilities cashed in on this by charging premium prices. In today's dollars, electricity cost almost $5 per kilowatt-hour in the 1890's – 70 times more than an average household customer pays today! And although Edison spoke in support of making electricity practical and inexpensive, the reality was that utility owners exploited their local monopolies shamelessly. The technology sometimes helped them; power surges, which were particularly common in rural areas due to lightning, tended to demagnetise the meters of the time, causing them to run fast [10]. Customers realised they were paying over the odds, which encouraged electricity theft; this had been declared a crime in some US states by 1900, though the UK did not criminalise it until 1916 [27].

The Depression led to increased losses. First, electricity had become a mass market service, with 67% of US homes having electricity in 1932 compared with 8% in 1907; second, the technique of bypassing meters with a jump lead became well known. A typical case was that

of the rancher Joe King, who was accused in 1931 of "looping a wire connection over a meter, thus obtaining a live current without registration upon the meter" thereby stealing from South California Edison Company [19]. Carlo Laury of Florida was fined $50 for using this trick to bilk Florida Power and Light Company in 1933 [29], while one Oscar Fortin got fined $100 in 1934 for using it against Montreal Light, Heat and Power Consolidated [24]. The industry responded with two measures. First, the National Electric Code was changed in 1931 to allow the meter to be connected ahead of the fuses, which made it harder to tap into the unmetered part of the electrical service, and meters were moved outside the home so the meter inspector could read them unannounced and without the cooperation of the customer. Second, the utilities installed balance meters, also known as feeder meters, which record the total amount of electricity supplied to a small area by a feeder and are balanced against the total sales recorded by individual meters.

The security economics of early utilities were straightforward. The utility protected its interest by a combination of technical protection mechanisms (making it inconvenient to bypass the meter using a simple jump lead, and using metal bases to make it harder to slow down the meter using a magnet), audit mechanisms (feeder meters and home visits to read and inspect meters), together with criminal sanctions for electricity theft as a deterrent. The desired outcome was to keep "non-technical losses", as they are called in the industry, below a certain target.

As for consumer protection, against both unreliable meters and against the bigger threat of monopolistic behaviour, that took regulation, which arrived following industry consolidation. By the late 1920s, the 16 largest power companies controlled 75% of US generation. This was driven by economies of scale. Large, efficient power plants were constructed near fuel sources (such as coalfields and rivers); their electricity went via a high voltage transmission network to major load centres where it was stepped down in voltage to the distribution network for dispatch to customers. The view emerged that electricity was a natural monopoly, most efficiently provided in any given area by a single company, which led in turn to government regulation (for a history of US regulation, see [12]).

1.2 Early digital meters

Electricity metering technology started to change in the early 1990s thanks to digital technology, and there's an interesting case history in South Africa, which was one of the pioneers. There, the state-owned Electricity Supply Commission (Eskom) owned generating plant and the transmission network; it sold power via over a hundred local authorities who managed distribution. In the run-up to the transfer of power to the African National Congress, Eskom started developing low-cost digital pre-payment meters as a way to enable service provision to rural populations (who lacked basic infrastructure such as house addresses and postal services, let alone credit ratings) and also as a response to politically-motivated withholding of utility payments in the townships. It was quickly realised that prepayment meters could be much cheaper than billed meters: the total costs of billed meters were in the range of 20–30% of turnover, thanks to the labour costs of meter reading and bill collection, and the writeoffs when poor people got into debt, while a prepayment system can be operated for 5–10% of turnover.

By the time Nelson Mandela took power in 1994, South Africa had 850,000 prepayment meters, and the prepayment system helped him make good on his campaign promise to electrify a further 2 million homes by the end of his term in 1999. The economics worked as follows. A customer could have his home electrified for a one-time payment of US$15, while the rest of the US$1000 electrification cost was recovered through the tariff over 15 years. The target was to keep collection costs to 5% of the turnover; local shopkeepers sold prepayment tokens for a 2%

commission. Some early systems used magnetic tickets as tokens; the technology that won out uses a 20-digit number to take an encrypted command from the vend station to the meter. Its critical advantage was that tokens could also be purchased from ATMs.

The more complex model of operations meant that there were several principals in the security game with conflicting interests – Eskom, the local electricity distributors, the token vending agents, the customers, and even the equipment vendors – and the games they played are documented in [2]. First, there were frauds and thefts in the distribution chain, particularly of token vending machines; this was fixed by using tamper-resistant modules containing not just the vend keys but also a value counter that would limit abuse. For example, the vending machine in a local shop might have a limit of R20,000 (US$2000) worth of tokens that it could dispense, before it had to be replenished with a token of its own from a machine one step up in the hierarchy. Second, a number of distributors simply got into debt, especially in the run-up to the transfer of power in 1994. Third, a number of the systems had exploitable vulnerabilities discovered in them. For example, customers in Soweto noticed that their meters would set themselves to maximum credit in a brown-out (a voltage reduction to 160-180V) because they had not been tested adequately for African conditions; this only came to light when customers started throwing chains over the 11kV feeders in order to credit their meters. Various other hacks were used by customers against token and refund systems, and by vending staff against bookkeeping systems. It took several years to shake the system down, fix the vulnerabilities and get it all under effective management. The net effects were, first, significant centralisation of control at Eskom; and second, a broad move to prepayment because of the cost savings. While prepayment meters used to be aimed at poor customers in South Africa, it is now common for even middle-class people to buy their electricity using prepayment tokens they get from ATMs.

The lessons learned in South Africa were applied elsewhere – in Brazil, Russia and even the UK, where a large deployment of prepayment meters in Northern Ireland led to a reduction in peak electricity consumption of about 10%. This cut in overall demand helped get policymakers interested in changing the way people buy energy. Their policy goals include cutting energy consumption, cutting carbon emissions, promoting energy security, dealing with the less predictable supply from renewable sources such as windmills, and (in the case of the UK) mitigating the effects of a foreseen "supply crunch" in 2016–18 when a number of existing coal and nuclear plants reach the end of their planned lives, before new capacity to replace them is due to come onstream.

Such policy considerations led the European Union to introduce an Electricity Directive in April 2009 under which Member States must replace all meters with smart meters by 2022 unless they determine by September 2012 that this uneconomic [15]. The directive also orders deregulation of European energy markets, so we will describe that briefly next.

1.3 Electricity markets and market failures

In the early 1980s, Chile pioneered the privatisation of electricity, where the idea is to unbundle the contestable functions of generation and retail from the natural monopoly of transmission and distribution. A key event occurred in 1989 when Britain broke up its state-owned generation and distribution utility, the Central Electricity Generating Board (CEGB) [28]. Now there are six large energy generators (plus a number of smaller ones) that supply electricity to the transmission network, the National Grid. The distribution network is owned by regional distribution network operators which are privately owned but regulated [13]. Retail companies, the energy suppliers, buy electricity from the generators and sell it on to the customers. The suppliers contract with the generators for the power. Most sales happen through bilateral agreement between the

generator and the supplier; there are also spot and futures markets to provide liquidity, with the spot market matching buyers and sellers for the following 24 hours in half-hour slots using an auction. There are also mechanisms to pay for dependability: there is a surcharge on spot prices that pays for spinning reserve to provide resilience in the face of unexpected demand, and the charges made by the National Grid include a 'security factor' depending on whether the network to a customer has single or double redundancy against failure [26].

While the utilities are still concerned about electricity theft, and customers about security of supply, governments worry most about power companies manipulating the markets. In normal times, their market power increases energy costs to the whole economy; when things go wrong, it can lead to an energy crisis. The textbook case is the California crisis of 2000–2001 [33]. California had followed the UK's lead and broke up its energy industry in the 1990s: the three main Investor Owned Utilities (IOUs) – Pacific Gas and Electric, Southern California Edison and San Diego Gas and Electric – were forced to sell off a major part of their generating capacity to unregulated companies like Enron, who subsequently sold them the electricity back wholesale. However, regulatory pressures drove wholesale and retail markets apart. The California government tried to keep retail prices low to win votes, so voters didn't conserve electricity, and the generators were able to sell electricity at much higher prices at times of peak demand. The IOUs lost money and the generators had insufficient incentive to invest; and things were brought to a crisis by a combination of low hydro output during the summer of 2000 and high demand in the desert southwest. California's average hourly imports fell from 6,800 MWh in the summer of 1999 to 3,600 MWh in 2000.

Even then there was enough technical capacity – but generators had enough market power to boost peak prices by shutting down some of their plants for "maintenance reasons". They had learned this trick in 1998 when the replacement reserve price of electricity peaked at $9,999.99/MW in July as against the average of $10/MW for the first three months of the year [33]! These maintenance shut-downs forced California grid managers to buy from the spot market at outrageous prices. Although these prices were partially regulated, they were linked with the price of natural gas: companies like Reliant Energy and Enron also supplied natural gas and manipulated both markets at once.

California's energy crisis is now seen as being the result of misdirected regulation, as much as of market manipulation by companies like Enron. Another recent example of a regulatory approach undermining security of supply comes in the form of NERC–CIP. The North American Electric Reliability Corporation (NERC) released a set of standards for Critical Infrastructure Protection. These standards are about operational security; Part 2 calls for the utilities to identify the 'critical cyber assets' in their systems and take steps for their protection. Failure to comply leads to heavy fines (as much as $1 million per day). A plant with a 'black start capability' is one that can start up when the rest of the grid is down (such as hydro power, or coal-fired stations with auxiliary diesel generators), and is considered critical – such stations are needed to reboot the grid in case of a blackout. However, once NERC-CIP came out, it was revealed that some plants removed their auxiliary generators so that they were no longer critical and therefore did not need to take computer security measures [31].

2 Smart grids, smart meters

This sets the scene for the move towards 'Smart Grids': future electricity distribution networks that match generation intelligently with demand and help shave demand peaks. Following its launch in 2007, this project received billions of dollars via the American Recovery and Rein-

vestment Act [21] and aims to revamp the entire electricity network – right from electricity generation to the metering of consumption. Europe is right behind; its Electricity Directive of 2009 aims to establish a common European market in electricity [15]. The UK, which helped push the Directive, has announced its own smart meter project that aims to replace 47 million existing meters by 2020 [11].

There are a number of options facing countries developing smart metering projects. The first is whether to develop a two-way system, where a customer might not only be a consumer of electricity from the grid, but also a producer; he could sell back to the grid any excess energy that he generates from his windmill. Germany has pioneered the use of a 'feed-in tariff' which guarantees a (subsidised) price for the output of microgeneration plant and has greatly boosted investment in renewables. However the number of feed-in customers is likely to be so low that supporting it on mass-market meters may not be economic. Of more acute interest may be the nature and volume of communications between the meter and the head-end.

2.1 Privacy – centralised or decentralised management

So far, public concern in the USA and Europe has centred on privacy, and in many countries there is a lack of clarity about what data will be shared with whom – and even about the metering and communications architectures that will be on offer. Energy management may or may not be centralised. If it is decentralised, the meter communicates with the utility once per time period (of perhaps a day, or a month). It sends the energy supplier the energy usage in each billable time segment of the previous period and receive the prices for each slot in the next period, in the event that they were due to change. The meter may also receive real-time requests from the utility to shed load. The actual management is performed on the customer's premises, either by manual intervention or by a separate system under her control: this might be a wall-mounted display device replacing the current thermostat, or a local device that communicates with her home computer, laptop or mobile phone. It might well involve a third-party specialist company, or a large service firm like Google or Microsoft, to which she subcontracts energy management.

In the centralised architecture, the meter passes detailed usage and home appliance information to head end, which in turn provides the customer with a web interface to manage energy use. Parts of the US Smart Grid effort are going in this direction, and the UK seems set to follow suit; the government wants to have half-hourly meter readings collected by a head-end system under its control, to which it will give access to the customer's energy supplier and also to a nominated energy management company such as Google. Most of the smart metering projects currently being run by utilities are also centralised. There are two clear implications.

First is the storage of huge volumes of data. Austin Energy, for example, has an installed base of about half a million smart meters in the US, from which it gathers about 200TB per year (the sample rate is 4 per hour rather than the UK's 2 per hour). Following this model, the data generated by 47 million smart meters in the UK would amount to 9Pb per year with 2 readings per hour; the US with five times the population and four readings per hour might generate ten times this amount. Shipping all this data will be expensive; in the UK, for example, it's proposed to use GPRS, but it's not at all clear that existing radio networks have the capacity, or who would pay. And even if all this data could be collected, storing and managing it will not be cheap.

The second issue is user privacy [22]. Studies [18, 20] show that it is possible to identify some of the appliances in use through load monitoring. It might also be possible to detect the lifestyle of the customers – when they eat, which programs they watch on TV, when they take a shower, whether individuals tend to cook microwave meals or on the stove, whether they have

breakfast, the time at which individuals are at home, and so on. This information could be of value to advertising companies, and so it's not surprising that Google has entered the energy management business through Google PowerMeter [17] and Microsoft through HOHM [25]. Other studies [30] show that fine-grained meter data, combined with side knowledge such as work hours and whether one has children, could yield sensitive personal information: that the homeowner returns shortly after the bars close, or is a restless sleeper, or leaves late for work, or leaves appliances on while at work. Governments keen to cut CO_2 emissions have also talked about giving each customer a carbon ration card [32]. Although this might not happen tomorrow, we can't totally exclude it as a possibility in the future.

In Europe, citizens have the right, under section 8 of the European Convention on Human Rights, to respect for the privacy of their family life, and this privacy right has got in the way of a number of central data-collection initiatives by various governments [3]. The first smart meter case has already happened: on 7 April 2009, the Dutch First Chamber declined to approve a Smart Metering Bill that would force all Dutch citizens to have smart meters installed in their home; it considered the mandatory nature of smart metering as an unacceptable infringement of citizens' privacy and security, following opposition by the Dutch consumers' association to central collection of energy data [9]. European privacy law is principally expressed in the IT sphere via the Data Protection Directive [14] according to which personally identifiable information may be collected for the purpose of performance of a contract or enforcement of a legal obligation, but it may be processed only in so far as it is adequate, relevant and not excessive in relation to these purposes. It is quite unclear that centralised metering, as a general proposition, would be consistent with EU law. Most consumers will not want a contract that burdens them with 48 different prices for every day of the year; even big businesses who can already buy electricity by the half-hour almost never do so. If the contracts offered to domestic customers are anything similar to those already offered to commercial customers, it will not be necessary to collect fine-grained data to enforce them[1].

Finally, there is a 'Big Brother' issue of what a state might do if it's more keen to save energy than its citizens are, and it's reluctant to ration by price alone. Given the California experience, governments should be very wary about letting retail and wholesale markets get out of synch. But suppose, for example, there's a crisis that can't be managed by pricing because of the short-run inelasticity in demand. Suppose that the UK faces a supply crunch in 2017 as old power stations near the end of their design life. Might ministers be tempted to cut off households who fail to meet savings targets? Or perhaps the most profligate household in each street? Many people would find this an unacceptable level of intrusion. Is it prudent to build the possibility of such action into the infrastructure? We will come to policy recommendations in section 3.

2.2 User interfaces and behavioural aspects

If a system can cause nontrivial privacy harm, then the next thing to ask is whether it brings sufficient benefits to balance the harm. Here there is a big question mark. In the UK, the Office of Gas and Electricity Markets (Ofgem) – the regulator – has run a smart meter pilot with over

[1] An EU Measuring Instruments Directive requires the meter to keep enough audit data for dispute resolution, but it does not require its transmission in the absence of disputes. A typical modern meter complies with this by having two nested units: a core metrology unit which is tamper-resistant, factory-sealed, and exports a read-only database of six months' readings; and a communications unit, sealed by the utility, that talks to the head-end and to customer equipment, and also implements secondary metering functionality such as tariffs and prepayment functions. In the event of dispute, the metrology database can be read out directly by an auditor.

50,000 homes and thus far found no statistically significant savings. So if smart meters are to reduce electricity demand, we need to know what incentives will cause consumers to change their patterns of energy use. The trials to date generally used simple displays and existing tariffs. Yet the behavioural economics literature suggests that energy-saving decisions will be difficult for the same reasons that decisions concerning dieting, saving or charitable giving are difficult: they involve intertemporal choice among both tangible and intangible goods, and are prone to 'time-inconsistent' preferences where people favour a tangible benefit today over and intangible one in the future, and this lack of self control in the short term subverts long-term goals.

As noted above, the widespread introduction of prepayment meters in Northern Ireland led to peak demand savings of about 10% – presumably because energy costs become more salient when they are tangible, namely when electricity is bought for cash rather than billed in arrears and taken from a bank account by direct debit. Innovative interfaces which compare current energy use with last year's may also help, and social comparisons may be even more effective: experiments by Cialdini found that people were most likely to save energy – whether by using less electricity, or by reusing towels in a hotel – when told that others in that neighbourhood, or hotel, had saved energy. What's more the biggest savings came when the smallest group was used for comparison [8]. It's clear that research should be done here to find out what works, and how well. It's worrying that large investments are being undertaken in its absence.

2.3 Price variability, electric cars and domestic UPS

Perhaps the most important factor in the long term is price. At present, power is cheap: people in developed countries spend about 1% of their income on electricity. As India and China compete for finite supplies of oil, energy prices will rise, and in the long term they should at least quadruple in order to make renewables economic.

In the short term, though, demand for energy is inelastic for two main reasons. First, lifestyle changes and major investments (such as insulating a house, or moving to a more energy-efficient one) take time. Second, the customer is not exposed to the real-time prices in the wholesale energy market. In the UK, for example, installed meters support peak and off-peak (night) rates; typical prices for one kWh are 11p and 7p respectively. However, wholesale prices are much more variable, with an average time-of-day variation of about 3.

Smart meters will lead to more variable retail pricing. For example, rather than offering me a 7p night / 11p daytime tariff, an energy supplier could offer 5p at night, 15p in the early evening, and 10p the rest of the time. Customers who can cut their early evening demand – singles who go out in the evening, shift workers, pensioners who can eat their main meal at lunchtime – will switch to this tariff, putting ever more pressure on any firms who keep on subsidising an 11p peak rate. Eventually we might expect to see broadly the same diurnal variation in wholesale and retail markets.

Interestingly, in the one market that already has a three-times diurnal price variation – Japan – households are starting to buy batteries, which they charge off-peak and draw down during peak periods. Batteries are already used in developing countries, which ration electricity using power cuts, and to guarantee security of supply to facilities such as computer rooms. These 'uninterruptible power supply' (UPS) systems are likely to become much more popular once households are exposed to real market prices. At present, US customers can buy a 5.5 kW/15kWh domestic UPS for $10,000, and prices are bound to fall as sales volumes grow. Electric vehicles will also help. First, owners will want to charge vehicles at trough prices; second, by 2015 there should be 15GWh of second-hand vehicle batteries on the market – batteries that are no longer good enough for traction but are quite adequate for domestic backup; third, people

may use their electric car as a backup power supply for their home. The spread of domestic UPS systems may even enable households to save money by switching to the interruptible tariffs currently used by some industrial customers, where the utility can suspend the supply at times of shortage.

The macro effects are less clear. Both the move to electric cars and the adoption of domestic UPS will increase both trough demand and overall demand (the typical battery-based UPS has an efficiency of only about 70%). This should increase price elasticity and reduce price variability. On the other hand, investment in fluctuating renewable generation capacity should increase both supply volatility and the price incentives to manage it. And as generators such as windmills are unpredictable, we may need near-real-time response to supply conditions. This is used as an argument for the centralised approach.

We believe however that in a future Europe where many households have UPS and are open to interruptible tariffs the way forward is not in a central ability to cut power to selected households, but rather for the utilities to enter into interruptible supply contracts with users. Furthermore, UPS engineering will be much simpler if households can continue to rely on the grid if they need to. Thus the response to a drop in the wind in Yorkshire, or clouds blocking solar-thermal plant in Spain, will not be a message from the government commanding '13 Acacia Avenue, switch off now!' but rather a message from the energy company notifying the customer '13 Acacia Avenue, we're invoking your supply interruption clause, and five minutes from now your price per kWh is going up from 20p to £1'. This would lead the customer to switch over to UPS – but leave the mains supply available if her battery were flat, or she were in the middle of cooking a dinner party that involved too many oven rings for her UPS to cope.

2.4 Conflict of interests

Energy producers and suppliers used to rely on increasing sales volumes to grow their revenues and profits. Government objectives are different. The UK, for example, is committed to reduce CO_2 emissions by about 60% (against a 1990 baseline) by 2050 with major progress by 2020 [7]. There are also fears of an electricity supply crunch by 2016 as a number of power stations reach their end of life [5]. In reality, governments have many objectives, some of them in tension with each other – cutting overall energy demand, cutting peak demand, cutting demand for gas, cutting carbon emissions, and scheduling any needed power cuts according to the political priorities of the day.

The resulting conflicts of interest between government and energy companies may be most obvious in the case of a centralised network architecture and a single head-end for energy reporting. If the government controls the data while the energy companies control the interface with the user, tussles are inevitable. For example, governments hope that increased transparency of energy pricing will lead to savings, while the energy companies will want to keep pricing opaque in order to maximise revenue.

If large quantities of data are collected in a decentralised system where the meter reports directly to the energy supplier, we might face problems of a different kind. If an energy company knows everything about its customers' habits, it can sell them exploitative contracts: a risk-averse but lazy customer might be sold a flat-rate contract with buyback, in the expectation that she would like the certainty of the flat rate but not bother to exercise the buyback. This might lead to deeper price discrimination, increasing customer lock-in, and diminished competition.

One possible fix is for each customer to have an energy management agent, which acts for them to monitor their energy use, advise them on savings, and look for the best supply deals. Companies like Google and Microsoft are entering this market; there are also small players, and

there's no particular reason why the management should not be performed by a local system in the customer's home and completely under her control. Just as people who want a quick and convenient solution to the word-processing problem use Google Docs while people who are careful about privacy and want to control their data will buy a copy of Microsoft Office or download a free copy of OpenOffice, so also there should be online energy management services sponsored by advertising as well as both free and paid-for local options.

A particular problem in the UK is that the Department of Energy and Climate Change (DECC) has outsourced the smart metering project to Ofgem, the regulator. The regulator thus has an interest in a centralised approach with a single government head-end under its control. It's not a good idea for the referee in a football match to be one of the players. It's also not a good idea for a critical IT infrastructure project to be run by a public agency with no IT experience of any significance and no experienced systems engineering staff. The history of government IT projects in the UK (and elsewhere) is not reassuring; while perhaps 30% of big software projects in industry fail, only 30% of such projects in the UK public sector succeed [3]. The smart metering project shows all the classic signs of incipient project failure; it's becoming politically untouchable even before a specification has been agreed. Worse, meetings to work on the specification have excluded not just potentially critical academics, but also the technical staff of the meter suppliers.

This is reminiscent in many other ways of past spectacular failures, such as the London Ambulance Service disaster, which is used as a standard teaching example of 'how not to do it' in university software engineering courses [16]: besides the incomplete specification the lack of consultation and the determination to ignore advice on realistic timescales, other similarities include unrealistic timescales, lack of experienced project management, no systems view, and confusion over who's responsible (Ofgem? DECC? the energy companies?). If this project is to be rescued, it will need new management and new rules. In the next section we will try to work out what better regulation and a better approach to smart meter introduction might mean in practice.

3 Policy options and technical solutions

We've described the main tussles in the smart meter space. They are driven by obvious incentives: energy companies want to maximise profits, customers want a dependable supply, while government wants to 'save the planet, keep the lights on, and without it costing the earth' [23]. This analysis lets us take a view on what needs fixing before the design of smart meters is finalised and the large-scale roll-out begins.

3.1 Non-essential data

The first issue is whether fine-grained metering information should be made available to the government, the energy companies, or both. The UK government has decided it wants all the data; it wants a gas and electricity meter reading from every household in the country every half hour. But as we already discussed (and the Dutch courts already decided), this isn't consistent with EU privacy law.

Now to the practicalities. If a typical tariff has three rates – night, day and peak – then the information essential for billing is simply the cumulative total of kWh used per billing cycle in each rate period. The Dutch courts have decided that the mandatory collection of nonessential fine-grained metering data is contrary to ECHR, which is also the law in the UK.

The energy supplier will argue for access to fine-grained usage data, though here the issues centre on competition: if your energy supplier knows much more about their customers' energy use than anyone else, they can price more aggressively and deter them from switching. The argument here may be less clear-cut; no doubt Ofgem will argue that it regulates the industry well enough already. But many customers are likely to object to their energy company having fine-grained usage data on their household, and so consent may not be assumed. A third aspect is that some engineers like the idea of being able to get readings of line voltage from smart meters, so they can manage the network better. We don't know whether this will be of any real value to the distribution companies; quite possibly they can get enough data from the feeder meters. However, the main concern of the regulator should be to prevent the abuse of market power by the energy suppliers, and so its interests should be aligned with the customers' interests and it should promote privacy – not data collection. As for who collects how much data beyond that strictly needed for billing, the market is surely the best arbiter.

In our view, the most appropriate starting point here is first principles, and in Europe that means the human-rights law that flows from the European Convention on Human Rights (ECHR), according to which sensitive personal information should only be shared with consent, or according to law. Furthermore, the laws must also meet certain criteria. We incorporate these in our first recommendation:

> **Recommendation 1:** Smart meters should by default only send such information to the utility as is necessary for billing and for technical operations. Information sharing with other entities – including energy management companies and the government – should require the customer's consent, or be done in accordance with the law. Laws requiring information sharing must be sufficiently narrowly targeted for the customer to foresee their effects, and they must be proportionate and necessary in a democratic society.

Some technical information may indeed be useful to distributors, such as whether a meter has a mains supply or not; instant notification of power cuts caused by distribution failures helps resilience and leaks no private data. But where technical information is 'nice to have' rather than necessary – such as voltage data from domestic meters, and where private data may leak (as voltage drop depends on current drawn), it is harder to justify the resulting invasion of privacy; and the same goes in spades for fine-grained data collection by energy suppliers. Of course, it may remain open to them to offer customers a cashback in return for more data, and the regulator can keep an eye on what this says about the value of the data. However, to be ECHR-compliant, we cannot have a central data collection system operated by the state. Customers must at least be able to opt out.

We propose instead an interoperability framework to ensure that a customer who switches energy supplier can do so without needing a site visit for meter replacement. As there are only four large meter vendors and six large energy companies in the UK, this should not require much government intervention. However we need to have the other stakeholders present too – the distribution companies the energy management companies, and the customers. In this, the regulator should argue the customer's corner, rather than getting trapped as the system operator – a task for which it does not have the experience or the mandate.

> **Recommendation 2:** The industry should develop open standards whereby smart meters can communicate as necessary with distributors, energy suppliers and energy management companies.

This analysis suggests a technical research project: to design a command language for meters that enables an energy company to specify complex tariffs in a piece of signed downloaded code that would implement a particular contract between the supplier and the customer. The sort of tariff we have in mind is: "Your basic rate is 5p from midnight to 0600, 15p for the peak from 1730 to 2100 and 10p the rest of the time; however the 15p basic peak rate applies only provided you restrict demand to two kilowatts else it becomes 50p. Furthermore we may at any time request you to limit consumption to 1kW and if you don't then any half-hour segment during which you draw more than 1kW at any time will be charged at 50p". The code would have to export to the energy company enough data for it to bill the customer correctly, and enough to the distibution company for it to operate the system efficiently. This problem is nontrivial but we believe it is solvable.

We also need some means of assuring the distributor and the market operator that the energy company is not cheating; anyone who peruses the consumer pages of the British press will observe that energy companies are frequently accused of sharp practice (which has also happened in the personal experience of one of the authors). Auditing the energy companies' behaviour is an interesting problem: from the technical point of view it can be done using a combination of code review and audit of household meter data against feeder meters. However, there is also a mechanism design problem. If this task is simply left to a centralised government system – well, government priorities may include carbon reduction and energy security and even law enforcement, but chasing small-time electricity theft is likely to be very far down the list of priorities. The parties with a clear financial incentive to discover and punish energy company cheating are the customer (where customers are the victim) and the distribution system – the National Grid and the regional distribution contractors – where energy companies are cheating each other. The distribution system not only operates the market but also bears the brunt of the difference between the power supplied by the generators and the power paid for by users, both in the form of technical losses in transmission and non-technical losses due to fraud. There are some subtleties here, due to the possibility of energy companies lying about the precise time at which their customers consumed energy, but enough of the resulting loss would fall to the distributors and the market maker for them to have an incentive to police this.

> **Recommendation 3:** Auditing the energy used by the customer and billed to the energy supplier should be primarily a task for the distributor.

It is not our goal here to sketch a design for the meter auditing and billing system – merely to observe that this is a security engineering problem that someone needs to tackle if we're going to have a decentralised system that respects customer privacy. The only capable entity with the motive to do this properly is the distributor. (We note in passing that the customer also needs to be able to audit her energy bills, but this is already a requirement of the Measuring Instruments Directive.)

3.2 The nuclear option

The next hot issue is whether meters should have a remote switch-off facility. The prospect of this is the big carrot for the energy suppliers; when a householder falls behind with bill payment, the premises can just be moved automatically to prepaid operation. This saves the supplier court action, and perhaps the need to force an entry to change the meter; human-rights law in much of Europe prevents defaulters simply being cut off. In fact the country with the most advanced smart meter program is Italy, where ENEL have installed over 30 million. There, the only benefit they claim is a reduction in losses, not a reduction in energy use.

Governments are in two minds about the off switch. On the one hand, energy ministries may like the idea of a facility that would enable them to adopt fine-grained coercive measures to save power; on the other, the national security establishment should be alarmed (and in some countries, is starting to be alarmed) at the prospect of a strategic vulnerability. An attacker who subverted the mechanism could wreak tremendous havoc. Such a power should thus either not be created, or guarded and controlled extremely closely. Given the growing interest in 'cyber-warfare', and the combination of skill and persistence displayed by (for example) the Chinese government in compromising systems from the Dalai Lama's private office to Google, it can be expected that if anyone has a master off switch for America's power and light, capable motivated agencies will devote considerable resources to getting access to it. Being able to turn out the lights in another country is the cyber equivalent of a nuclear strike – a completely disabling strategic attack that would reduce the enemy population to nineteenth-century standards of living.

It is not at all clear that the same effort is being put into thinking about the implications of this as has been invested in other strategic national systems, such as the command and control of nuclear weapons. Our view is that such a facility should not be built into meters; if a democratically elected Government decides that it must be (as the UK government appears to have done in March 2010) and its decision withstands any legal challenges under human-rights law, then some very serious security engineering indeed is called for. One possible approach is that there should not just be a single crypto key in each meter, but multiple keys that back each other up; perhaps one for each energy company, one from the meter vendor and one from the regulator, with appropriate rules for backup and recovery.

In addition, it would be very unwise for the 'off' switch to have immediate effect. If a meter were being switched from credit mode to prepay mode, for example, it would be reasonable to notify the customer. Interaction, and a notice period, are a legal requirement at present when switching energy company and this clearly ought to continue as the system goes 'smart', with decisions being taken by meters that are at present implemented in assorted utility back-end systems. So an energy company wishing to move a defaulting customer to prepay should also give notice to the customer, so that she can either pay up, or declare a dispute and sign up with a different supplier. A prudent energy company might also keep the relevant keys in a hardware security module and use this to impose rate control – for example, the module might prevent more than 1,000 customers being moved from credit to prepayment mode in any one business day.

Also, as noted above, it is preferable for interruptible tariffs to be supported by mechanisms other than a hard switch-off from a government computer. A request would be more robust than a command: 'please switch off or cut back use if you can' backed by a higher tariff if the household continues to abstract power from the mains during the crunch period. That not only allows less reliable backup power supplies to be used; it also prevents the mechanism being abused for attack. For these reasons, our third recommendation is

> **Recommendation 4:** Active demand management should be left to private contract between the energy companies and their customers.

Again, it is not the purpose of this paper to attempt a detailed design – merely to point out that the 'nuclear problem' of a remote switch-off facility being abused by strategic or criminal adversaries can be greatly mitigated, using a combination of mechanisms embedded in meters that limit the impact of switch-off commands and make their existence manifest several days

before they take effect, rate-limiting protocols, and mechanisms for shared control at the level of key management. We will be writing separately about these technical aspects in another forum.

3.3 Other consumer issues

The third bundle of issues concerns how the meter will communicate with home area network devices. As noted above, there has already been some standards work on using a new version of Zigbee for this in the USA, with pressure from patent owners to incorporate elliptic curve cryptography. We understand that the industry is starting to push back on this. Of more importance are standards to minimise the information passing from the home area network to the utility in order not just to protect customer privacy but also to prevent malware on home equipment being used to attack the utility; this is beginning to receive attention from NIST.

Above all, it is important that someone should play the role of consumer advocate as this system evolves. In an ideal world, the regulator would shoulder this burden and ensure that the technical architecture supports both privacy and competition. But this world isn't ideal. In the USA, standards-setting involves a number of players including NIST, NERC/FERC and the DHS, as well as trade associations. The number of standards and regulatory bodies gives rise to concern that they will end up pulling in different directions; it would be helpful if the US government could settle these turf wars and provide a clear direction for future regulation. Who will be the consumer's advocate?

In the UK, the regulator Ofgem has been working far too closely with the government on this particular programme and has in effect become its owner. This has to stop. It is both important and urgent for the UK government to revisit the decision to have a centralised system whose design and procurement is supervised by the regulator. Quite apart from compromising the regulator's independence, this is likely to make the project a failure; most large public-sector IT projects fail while most private-sector ones succeed.

> **Recommendation 5:** The smart grid needs an independent regulatory authority that has both the capability and the motivation to stand up for the interests of energy users. It needs to ensure both security of supply and market competition.

4 Conclusion

The large-scale move to 'smart meters' which is being driven in the USA by the stimulus package and in Europe by the Electricity Directive has raised a number of fascinating security-economics problems. The 'smart grid' of the future will not be a monolithic entity under the control of a single company or ministry, but rather a complex socio-technical system of energy generators, distributors, regulators, market-makers, aggregators, advisers and suppliers, interacting with both industrial and retail customers. In this paper we have made a first stab at setting out the multiple conflicts of interest. We have traced how these have become progressively more complex over the years: from single-utility islands where the only issues were whether the utility would cheat its customers or they would steal electricity from it, to early digital metering systems in networks with tiers of distributors who might also try to cheat their upstream suppliers.

This led us to an analysis of the environment in which smart meters are starting to be deployed, and the big policy issues. Should the processing of metering data be centralised, say in a government agency, or decentralised to energy suppliers? How much fine-grained data about household consumption is it necessary for supplier systems (or central systems) to hold on customers? Should all meters have a remote off-switch facility, and if so how can one deal with

the national-security threat that an opponent might get his hands on the nation's off switch? And how should meters interact with domestic devices?

We've shown that when these problems are considered in the context of the less-obvious security and dependability requirements, such as how to prevent energy companies cheating their users (and each other), how future grids are to deal with the fluctuating supplies from renewable sources such as wind, and the role of local storage and demand shifting, that their solution is nontrivial – but that there are probably some quite practical ways forward.

We made five specific recommendations. First, smart meter data should belong to the customer, who should be forced to share it with the utility only to the extent necessary for service provision and billing. Further uses should be a matter for the customer's discretion. Second, rather than a centralised system for data collection, what's needed is a framework of standards that allow data to be shared between energy suppliers, distributors and management companies. Third, the distributors should do the heavy lifting when it comes to audit; they alone have the incentive to do it vigorously. Fourth, rather than dreaming about being able to inflict power cuts on targeted citizens at will, governments should leave active demand management to the energy companies. And finally, in a market as prone to abuse as the energy market is, we need a regulator who will stand up for the customer – rather than acting as the government's surveillance and policy agent. The interests of governments and customers are not identical, however much the former may be elected to represent the latter. The regulator should not set technical standards, far less run the metering network; its role should be limited to ensuring security of supply and market competition.

There are a number of practical consequences for research, both on technical and policy matters. What sort of incentives will really cause customers to save energy, and what implications does this have for the design of tariffs and indeed meters? How can we design a tariff description language that will enable an energy supplier to download a tariff to a customer's meter, in such a way that both the customer and the distributor can audit what's going on? How can we be confident that features such as a remote off-switch (or for that matter the tariff description language) aren't abused for service-denial attacks? And perhaps of most interest for the security-economics community, what sort of regulatory structures are likely to work best as the industry moves from being a staid vendor of energy at regulated prices into a complex socio-technical system?

Acknowledgement

We are grateful to Tyler Moore and to colleagues at the security group at Cambridge for helpful comments. The second author's research is funded by ABB. The contents of this article do not necessarily express the views of ABB.

References

[1] R Anderson, *'Security Engineering – A Guide to Building Dependable Distributed Systems'*, Wiley 2008

[2] R Anderson, SJ Bezuidenhoudt, "On the Reliability of Electronic Payment Systems" in *IEEE Transactions on Software Engineering* vol 22 no 5 (May 1996) pp 294–301, at `http://www.cl.cam.ac.uk/~rja14/Papers/prepay-meters.pdf`

[3] R Anderson, I Brown, T Dowty, P Inglesant, W Heath, A Sasse, *'Database State'*, Joseph Rowntree Reform Trust, March 2009; at http://www.ross-anderson.com

[4] Association of Electricity Producers, at http://www.aepuk.com/

[5] BBC, 'UK could face blackouts by 2016', Sept 11, 2009 at http://news.bbc.co.uk/1/hi/8249540.stm

[6] T Bernstein, "A Grand Success", *IEEE Spectrum* Feb 73 pp 54–8

[7] Department of Business, Enterprise and Regulatory Reform, *'Meeting the Energy Challenge'*, http://www.berr.gov.uk/files/file39387.pdf

[8] R Cialdini, "Descriptive social norms as underappreciated sources of social control", in *Psychometrika* v 72 no 2 (June, 2007) pp 263–268

[9] C Cuipers, BJ Koops, "Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM", Universiteit van Tilburg 2008

[10] D Dahle, "A brief history of meter companies and meter evolution", at http://watthourmeters.com/history.html

[11] DECC, A Consultation on Smart Metering for Electricity and Gas. May 2009.

[12] Dept of Energy, "History of the U.S. Electric Power Industry, 1882-1991", at http://www.eia.doe.gov/cneaf/electricity/page/electric_kid/append_a.html

[13] National Grid, Distribution Network Operator (DNO) companies, at http://www.nationalgrid.com/uk/Electricity/AboutElectricity/DistributionCompanies/

[14] European Parliament and Council, *'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data'*

[15] European Parliament and Council, *'Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC'*, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:EN:PDF

[16] A Finkelstein, "London Ambulance Service – Computer Aided Despatch System", at http://www.cs.ucl.ac.uk/staff/A.Finkelstein/las.html

[17] Google Power Meter Project, at http://www.google.org/powermeter/

[18] GW Hart, "Nonintrusive Appliance Load Monitoring," in *Proceedings of the IEEE*, Dec 1992 pp 1870–1891

[19] Los Angeles Times archive, 'Rancher Pleads Guilt in Theft of Electricity', Oct 30, 1931.

[20] C Laughman, K Lee, R Cox, S Shaw, S Leeb, L Norford, P Armstrong, "Power Signature Analysis" in *IEEE Power and Energy Magazine* March/April 2003 pp 56–63

[21] M LaMonica, "Obama signs stimulus plan, touts clean energy", CNN, Feb 7 2009, at http://news.cnet.com/8301-11128_3-10165605-54.html

[22] MA Lisowich, S Wicker, "Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems", in *IEEE Proceedings on Power Systems* v 1 no 1 (Mar 2008) pp

[23] David MacKay, DECC chief scientist, talk at Cambridge University, Jan 18 2010

[24] The Montreal Gazette, 'Electricity theft charged in court', Mar 22, 1934.

[25] Microsoft HOHM, at http://www.microsoft-hohm.com/

[26] National Grid, "Statement of the Use of System Charging Methodology", version 5.1, at http://www.nationalgrid.com/uk/Electricity/Charges/chargingstatementsapproval/index.htm

[27] The New York Times, 'New Crimes and Penalties', Oct 7, 1900.

[28] Office of Public Sector Information, 'Electricity Act 1989' at http://www.opsi.gov.uk/ACTS/acts1989/ukpga_19890029_en_1#Legislation-Preamble

[29] The Palm Beach Post, 'Theft of electricity is charged in court', Jan 18, 1933.

[30] Elias Leake Quinn , *Privacy and the New Energy Infrastructure*, Feb 2009 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731

[31] J Weiss. *'Electric Power 2008 is NERC CIP Compliance a Game?'*, Control Global Community, Sep 5 2008, at http://community.controlglobal.com/

[32] P Wintour, "Miliband plans carbon trading 'credit cards' for everyone", in *The Guardian* Dec 11 2006; at http://www.guardian.co.uk/politics/2006/dec/11/uk.greenpolitics

[33] Frank A. Wolak, 'Diagnosing the California Electricity Crisis', Sept 2003 at http://www.ef.org/documents/CA_crisis_Wolak.pdf