The Foundation for Information Policy Research

Consultation response on

Smart Meters

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

In March 2009 the Joseph Rowntree Reform Trust published a report, 'Database State', that we wrote. This analysed forty-six public-sector systems that hold information on all of us, or at least on a significant minority of us. We rated eleven of these 'red' in that they almost certainly break human-rights law, and most of the rest 'amber' in that they have significant problems. Had the proposals for centralised management of smart meters been made at the time we wrote that report, they would have been on the list; we might well have rated 'big brother meters' at red rather than amber.

In addition to privacy concerns, many of the centralised systems that government has attempted to build over the past decade have simply not worked. The NHS National Programme for IT (NPfIT) is the biggest civilian IT project failure in history, and it is by no means alone. Centralised megaprojects are more likely to fail, for reasons discussed in our report, than the distributed systems that arise naturally (e.g., when hospitals and GPs were just allowed to buy their own systems). There are further problems with the way the UK civil service manages projects, and the way it recruits and trains its senior staff.

The government now proposes to build a system to read 46 million new gas and electricity meters every 30 minutes and collect the data centrally for billing, demand management and other purposes. Our reaction is: yet another 10-year, £10bn government IT project, driven by political targets, and being started in a hurry without a clear specification of what the system should actually do. It will probably not work; if it does, it will be privacy-intrusive, to the extent that it will probably be in breach of European human-rights law (regardless of any legislation the UK parliament may pass).

Will it work?

First, conflicts of interests will arise between the proposed centralised metering infrastructure and the energy companies that actually sell gas and electricity to consumers. The centre will have many targets whose priority changes from time to time, including 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. For their part, energy companies will seek to maximise profits by increasing sales volumes while shaving peak demand. If the government controls the data while the energy companies control the contractual interface with the user, tussles are inevitable. The government hopes that increased transparency of energy pricing will lead to savings, while the energy companies will continue to face strong incentives to make pricing opaque in order to maximise revenue.

But even if smart meters could deliver transparency, it is not clear that this will lead to savings; the lack of statistically significant savings in reports thus far from the Ofgem smart meter pilots casts doubt on even this most basic assumption. Getting people to forego tangible present benefits in return for intangible, uncertain benefits in the future is well known to be a hard problem (with dieting, saving, and charitable giving being other examples). We do not yet know what combination of prices, contracts, interfaces and social factors will actually persuade people to shift or reduce energy demand.

So it is not clear that the smart meter project has a realistic prospect of cutting energy use, and it is not at all clear that DECC will be any better than the DoH or the DCSF at specifying, procuring and implementing a multibillion-pound IT project. And if this system will be able to turn off anyone's (or everyone's) energy supply, it must be protected against hostile takeover. We see no sign of the serious security engineering that would be required. Will this only be recognised when it is too late?

Privacy and human rights

The second bundle of issues concerns privacy. The DECC Impact Assessment (May 2009) recognised that "Smart and advanced metering will result in a step change in the amount of data available from electricity and gas metering. There may be value and interest in using such data in new ways. Careful consideration of the implications both legally and in terms of public acceptability and transparency will be necessary."

It is time for this debate to start. We have no objection to meters being able to support contracts with finer time granularity of pricing; but if I contract with an energy company to buy electricity for 4p per unit from midnight to 6 am, 24p per unit from 4pm to 7pm, and 8p the rest of the time, then all my meter needs to tell the company is now many KWh I consume in each of these price bands in each billing period. It is not necessary for my meter to tell the power company, let alone the government, how much I used in every half-hour period last month. We have no problem with the Measuring Instruments Directive requiring the meter to keep a full log for dispute resolution; nor do we do object to consumers being able to share their power history if they wish with Google or AlertMe to get advice on how to reduce their costs. But it is excessive and, we believe, unlawful for this complete record to be shared without the consumer's free and informed consent, whether with the state or with the energy supplier.

One study suggests that the degree of personal data that can be gleaned from smart meter readings is considerable:

> "For example, it is suggested that the following information could be gleaned with the introduction of end-user components (these issues will become more practical concerns as appliances and devices become part of the grid): Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/ or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used. Combined with other information, such as work location and hours, and whether one has children, one can see that assumptions may be derived from such information. For example: the homeowner tends to arrive home shortly after the bars close; the individual is a restless sleeper and is sleep deprived; the occupant leaves late for work; the homeowner often leaves appliances on while at work; the occupant rarely washes his/her clothes; the person leaves their children home alone; the occupant exercises infrequently." [EL Quinn, "Privacy and the New Energy Infrastructure," SSRN Working Paper Series, 2009; http://ssrn.com/abstract=1370731]

Such considerations show that fine-grained household energy-use information is not merely personal data in terms of data protection law, but will in many cases be sensitive personal data. Its collection by the government will thus require either consent (which is not proposed) or specific legislation to limit the collection to that which is proportionate and necessary in a democratic society (no case for necessity has been made), and such that the effects on the data subject will be predictable (which is not proposed). In the circumstances it is highly likely that the proposed system will breach European human-rights law. For more details see the argument in chapter 7 of the 2006 FIPR report to the ICO on Children's Databases [http://www.fipr.org/childrens_databases.pdf]. We note that the courts in the Netherlands have already ruled against a not entirely dissimilar proposal there [see C Cuipers, BJ Koops, "Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM", Universiteit van Tilburg 2008].

But the effects of privacy failure are not limited to lifestyle disclosures, or targeting information for burglars. Privacy also affects competition in energy markets. 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. So privacy is a matter for Ofgem, not just the courts and the ICO.

What's more, should Britain suffer supply shortages in 2016–8, as some predict, there will be a temptation for policymakers to use smart metering data to target any needed power cuts. Will ministers cut off households who fail to meet savings targets? Or perhaps the most profligate household in each street? That would be a most unwelcome innovation in Britain's political culture.

What should be done

What we need instead is an interoperability framework to ensure that an E.ON customer who switches to EDF can do so without needing a site visit for meter replacement. As there are only three large meter vendors and six large energy companies, this should not require much government intervention. Rather than DECC trying to micromanage everyone's energy use, market rules should provide appropriate incentives to energy companies, for example by rewarding security of supply and not just sales volumes. Advanced meters that support finer time-granularity of billing can certainly play a role – for example to motivate consumers to shift demand away from the early evening – and energy companies should be encouraged to fit them. In the context of such a project, we see only three things that need to be done centrally:

1. clarifying how much data should be collected, where, and who's going to own it. Data should be collected in the meter, be owned by the customer, and by default only the data required for billing should be sent to the energy company;
2. establishing the communications and security architecture and standards for the connection between the home's meters and the head end;
3. ditto for the connection between the home's meters and the home area network.

When tackling the first of the above questions, the government should bear in mind the S & Marper v UK and I v Finland judgments of the European Court of Human Rights, and contemplate the consequences of a ruling that smart meters with central data collection are unlawful. It should also minimise the information passing from the home area network to the utility in order to prevent malware on home equipment being used to attack the utility, and remove the remote switch-off capability to prevent attacks that cut off customers – whether these are conducted for blackmail, or as a hostile act against Britain's critical national infrastructure by a foreign power or a terrorist group.

Ofgem should set out a timetable for agreeing the other aspects of 2 and 3 above with the ERA and other major stakeholders, in the process paying attention to the competitive aspects and representing the interests of consumers by ensuring that the technical architecture will support both privacy and competition. The draft architecture and standards should be subject to a full public consultation.

If the next government is serious about getting advanced meters installed in most homes by 2020, it had better abandon the current plans and let the energy companies get on with the job. If it does not, the most likely outcome is not just an eventual legal requirement that systems be redeveloped to support freely-given informed consent prior to any data transfer beyond the minimum required for billing, but a project disaster like NPfIT – with billions wasted, UK industry damaged and critical opportunities lost.

Ross Anderson FRS FREng
Foundation for Information Policy Research
Cambridge, January 2010