Data Privacy and Security for Smart Meters – Response to Ofgem's Consultation

Ross Anderson, Shailendra Fuloria, Éireann Leverett
Computer Laboratory, University of Cambridge

This is a response to the consultation on 'Smart Metering Implementation Program: Data Privacy and Security' published by DECC/Ofgem on 27th July, 2010. While we commend Ofgem for taking into account the importance of security and privacy, we would like to point out several areas where more work is needed.

We support Ofgem's policy of assigning the ownership of meter data to the customer, as we suggested in our own work[1]. This consultation however suggests that the customer will have to pass on data required for 'regulated duties'. This is too vague; if it ends up with DECC or Ofgem wanting a copy of everything, it will be open to legal challenge (as in the Netherlands). The customer should only have to pass to the retailer the data required for billing, and to the DNO the data required for maintaining service and for auditing the retailer.

Section 3.15 of this consultation discusses the default policy for data sharing for customers – whether it should be 'opt-out' or 'opt-in'. By default, all meters should only send the data which is necessary for billing and essential technical operations for managing the grid. Other data should be sent only after the customer has given explicit, informed and voluntary consent.

In our first response last month, we advised strongly against the centralised model proposed by DECC and Ofgem, as unlikely to work either as a regulatory mechanism (as it fails to facilitate new market entrants into the energy saving business) or at all (as it sets a quite unrealistic timetable and repeats essentially all of the major errors made in previous failed public-sector IT projects). If ministers nonetheless decide to proceed with this architecture then serious thought needs to be given to how participants acquire customer consent for data sharing. In a centralised world, where many of the principals have no contact with the customer, the Data Communications Company (DCC) appears to be the default party for acquiring consumer consent – first, as it would be the data controller as a matter of fact and thus of law, and second because holding DCC accountable for consumer consent will incentivise them to be prudent about sharing.

Chapter 4 of this consultation is the core of this proposal and is also referred to in other documents that DECC and Ofgem have published. So we expected detailed technical and

[1] R Anderson, S Fuloria, 'Security Economics of Electricity Metering', Workshop on Economics of Information Security, Harvard University, June 2010

policy discussions; but the security chapter is just four pages and says in effect 'trust us'. This approach stands in stark contrast indeed to that taken in America, where smart grid security is done openly by NERC and NIST with over three hundred industry engineers and others on a range of standards bodies. Security must be built in from the start; security is an emergent property of systems and is extremely difficult to retrofit. Furthermore, in an open system such as the proposed smart metering system the standards will have to be open. It is not acceptable to sweep privacy and security under the carpet, and leave the details to be fixed up later – trusting meanwhile in a cloak of official secrecy. The meters, gateways and home controllers will be manufactured by the million and will be studied by both analysts and attackers; flaws will be found eventually, and it is far better that this review process take place prior to the scheme being launched rather than afterwards. Ministers should not repeat the mistake that the banks made with Chip and Pin, where systems designed in secret had serious flaws found once they were fielded.

With regards to the discussion on disabling and re-enabling gas and electricity supply, we compliment DECC/Ofgem for taking on board the risk of unauthorised access to the remote disconnection functionality that we raised earlier this year[2]. However, we would like to point out that the impact of such an attack will depend on the metering architecture. A centralised architecture like the one proposed by Ofgem will be much more vulnerable than more distributed systems. So we do not think it is prudent to just wait to see what other countries in Europe do (as implied in section 4.8).

While the requirements are still being deliberated by DECC and Ofgem, some energy suppliers have already begun to roll out meters. We may have a few million smart meters in the field even before the security specifications are finalised. We would like to know whether DECC/Ofgem have reviewed the privacy and security policies and mechanisms that are being employed by these suppliers; and what will be done to bring existing meters into compliance. Has DECC/Ofgem the stomach to compel the replacement of insecure meters, or meters that compromise customer privacy – or will the existence of such devices result in back pressure on DECC/Ofgem to tone down its requirements?

In summary, we will briefly answer the consultation questions.

1. The overall DECC/Ofgem approach to data privacy, namely letting the customer control their data, is unobjectionable: the customer should control the data with the exception of data required for billing, auditing and network management.

2. However we fear that the devil will be in the detail. If a customer enters into a monthly contract with a retailer for electricity at 5p per until from midnight to 6am, 20p from 6pm to 9pm, and 10p at all other times, then the customer is likely to take the view that the

[2]R Anderson, S Fuloria, 'Who controls the off-switch', presented at the IEEE conference on SmartGridComms, NIST, Gaithersburg, USA, 2010

information required for billing is the monthly total of units at each of these three prices. The retailer will no doubt ask for a complete schedule of each customer's consumption by the half hour, while for market settlement aggregated half-hourly data would be sufficient. If Ofgem gives customers vague assurances of privacy but then hands all their data over to the retailers, it will be open to accusations of regulatory capture and breaches of human-rights law. We need clarity now, at an early stage in the design process, of who will get what data and when. We suggest that officials consider the proposals in other EU countries such as Germany.

3. We find it difficult to be enthusiastic about a privacy charter. The regulation of privacy in the UK has long been defective; the first Data Protection Act was admitted at the time to be aimed at minimal compliance with the Council of Europe, while the UK faces litigation by the European Commission over the inadequate transposition of the Directive into the second Data Protection Act. Privacy is actually governed in the UK by section 8 of the ECHR, of which the Data Protection Directive is a partial implementation, and yet the ICO and his predecessors have refused to attempt to enforce European law. In short, the UK has a long history of 'privacy theatre': of providing legal and bureaucratic mechanisms that give the appearance of protecting privacy but don't in fact do it. An informed citizen would likely consider the suggested privacy charter to be just more window dressing. In any case, if a customer's privacy rights are infringed by Ofgem, she will have to sue, as the ICO is unlikely to do anything effective.

4. See above.

5. Ofgem's approach to smart meter security is not credible. The approach is, in essence: 'We've talked to GCHQ and some others, but we're only going to tell selected insiders what we're doing about security. We're the Government; trust us.' This tune is familiar from government systems projects in the past, but it has no traction any more – the HMRC debacle put paid to that. People in the information security business are well aware of the public sector's shortcomings, just as people in the smart metering and smart grid business are aware of Ofgem's lack of systems engineering knowhow. Information security professionals are always wary of security by obscurity; in this application it is inappropriate, and given the open approach in the USA it is unsustainable.

   To regain credibility, Ofgem must develop and publish a threat model, a security policy, a specification for how the policy will be implemented, and plans for the evaluation, accreditation and if necessary replacement of systems that are deployed as part of the smart meter scheme. It must also tie these to its governance arrangements, so that whenever the initial liability for some failure does not lie with the party best able to prevent that failure, there is a robust and explicit mechanism to realign incentives.