# The Foundation for Information Policy Research

**Consultation response on data access and privacy for 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.

We have a number of comments to make on the consultations on rollout obligations[1] and on privacy and data access. Our overall analysis and concerns are described systematically in the attached paper[2]. Here we tease out the specific implications for the consultation on data access and privacy for smart meters.

1. See the attached survey paper on smart meter security plus the other research publications that can be found at http://www.ross-anderson.com

2. The fundamental problem with the smart metering programme as presently constituted is that government hopes customers will save energy as a result of smart meters making their energy use more salient. However suppliers maximise their profits by maximising sales volumes and to do this they wish energy use to not be salient to the customer; for example they prefer creditworthy customers to pay by direct debit rather than prepaying as prepayment customers (ceteris paribus) buy less electricity. Worse, the industry bases its business model on confusion pricing – for exactly the same reasons as the banks and the telcos do. It is therefore most undesirable for the suppliers to have access by default to the customer's full energy use data. These data must remain the property of the customer who should be encouraged to share them only with ESCOs who will help her save energy. Attempts by suppliers to get access to full data whether by lobbying now, or by use of contract terms once the smart metering program is operational, must be stoutly resisted by DECC and Ofgem. Data control by incumbents will be used to suppress competition and stifle new market entrants. These considerations of strategic behaviour are quite independent of, and in addition to, any considerations of customer privacy.

3. We oppose the inclusion of gas meters in the smart metering programme. We believe that this was a serious error, of which ministers should recant.

---

[1] See our consultation response on smart meter rollout strategy at http://www.cl.cam.ac.uk/~rja14/Papers/fipr-sm-rollout2011.pdf

[2] http://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf

4. We don't believe this argument by the suppliers. Ministers must be adamant that suppliers don't get full data; only ESCOs get it, and only with full customer consent. Furthermore, there should be a bar on acquisitions of ESCOs by suppliers.

5–6. Theft management is best left to DNOs, for whose purposes the relevant data is the monthly total of energy sales to all premises supplied off a single feeder, which the DNO should balance against its feeder meter, This total should be provided by DCC.

7. Suppliers wishing to promote a tariff should make available a signed formal description of it in a tariff description language – which when applied to a customer's database of half-hourly meter readings will yield the tariff that that customer would have had to pay. The customer will store his usage history in his Open Home Controller, and download offered tariffs from comparison sites. On choosing a tariff she can switch to the supplier offering it. For designing such tariffs, a sample of perhaps 10,000 anonymised customer databases should be more than sufficient.

8. A future move to demand response, in order to accommodate larger-scale use of renewables like wind and solar, will eventually require supporting mechanisms of finer granularity. For now, a sample of 10,000 anonymised customer databases should do; in the future, we might have mechanisms to aggregate each supplier's customers' usage on a regional basis. However, doing anonymisation robustly is hard, and it is possible that we will use different mechanisms entirely. For example, if fine-grained time-of-use pricing leads to large peak-to-trough price differentials, this is likely to lead to the use of batteries for arbitrage, which might in turn lead to interruptible tariffs being offered to domestic customers.

9. The hedging argument is bogus, as the expenditures that suppliers may wish to hedge are precisely those for which they become liable as a result of settlement. Thus if the answer to question 8 is "not yet", the answer to 9 is the same.

10–11. Rather than using debt management as another excuse to demand full usage data on all customers (whose main incentive is anticompetitive as noted in 2 above) the suppliers should rather busy themselves designing tariffs that lie somewhere between credit meters and prepayment meters. They might for example allow a poor household a fixed amount of credit per month, beyond which the meter would require prepayment. Once the meters are programmable, this is just a matter of software (another of the advantages of a properly designed tariff description language).

12. This also seems to be completely bogus.

13–15. The DNOs should not be trying to use smart meter data for network management; this is just bad power engineering, and bad systems engineering too. Instead they should use feeder meters and other proper monitoring equipment in substations. In fact, if the DNOs actually owned and operated the smart meters (as economists such as Dieter helm have argued) then they would be able to make a

rational economic decision about the optimal amount of network monitoring, and its location. It is only to be expected that they will accept a second-class monitoring service from the smart meter system if they do not have to pay for it, and if the retailers suggest they ask for it to support the retailers' own wish to control all the data for anticompetitive purposes.

16–17. We anticipate efforts by suppliers to get customers to hand over their data via the terms and conditions of their supply contracts. This must be stopped, and that is not a matter of behavioural economics but of regulatory action.

18–20. Anonymisation tends not to work well in practice; in one application area after another ways have been found to re-identify things[3]. A better approach would be direct regulation: Ofgem should forbid energy suppliers for retaining more data on any customer than are required for billing, regardless of how that information came into the supplier's hands. This is the sort of question where Ofgem would be a much more appropriate lead regulator than the ICO as the main reason to prevent suppliers accumulating vast stores of customer usage data is competition rather than privacy.

21–22. Much more thought needs to be given to how the customer will interact with the meter, the HAN and the backhaul. We have argued in the attached paper that the missing piece of architecture is an Open Home Controller, as proposed by the Council of European Energy Regulators. This will be in effect a web server which the customer can access from her laptop, her iPhone, her iPad or whatever the fashionable device might be in the future; it will interact with the meter, her appliances and her supplier to provide the necessary information and control interfaces for her to understand her energy use and manage it.

23. Again, the missing piece of architecture here is the Open Home Controller (or something like it). The DCC cannot conceivably do all this work; as it is, the DCC project has a timeline that is so short it's probably impossible for any firm to deliver it on time. If customer interaction depends on the DCC, it's not going to happen any time soon.

24–25. A project of this scale should be taken more slowly with a large-scale pilot project to demonstrate feasibility in (say) a small city. That way, systems like the DCC could be properly debugged and stress-tested before national roll-out. What's more, the assessments of the pilot should be open and subject to peer review; the criteria for success should be spelled out in advance; and the structure should be such that if it's clearly not working, ministers can cancel it.

Professor Ross Anderson FRS FREng
Chair, Foundation for Information Policy Research
October 13 2011

---

[3] See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010)