

Intellect Response to Ofgem Annex 4: Data Privacy and Security October 28 2010

Russell Square House
10-12 Russell Square
London WC1B 5EE

T 020 7331 2000
F 020 7331 2040
www.intellectuk.org

Information Technology Telecommunications & Electronics Association



Do you have any comments on our overall approach to data privacy?

Intellect members fully support the steps being considered to protect safety, security and resilience to data integrity. Of particular importance is the principle that the consumer shall choose the way in which consumption data shall be used and by whom (excluding data required for regulatory duties). This is broadly seen by Intellect members as a positive step towards alleviating consumer concerns over data privacy.

It should be noted, however, that many Intellect members would also point towards a number of other considerations around data privacy that need to be taken into account. These include:

Privacy by Design

Data protection must be embedded within the core design of the system and should be introduced early to be in place for the mandated rollout. In practice, this protection needs to be in place prior to the establishment of the DCC in order to prevent experiences such as those which occurred in the Netherlands, where privacy concerns led to its smart metering bill being initially rejected.

Consumer Consent

Intellect members are in agreement over consumer consent for the collection. Moreover, some believe that further consideration needs to be given to the requirements of customers who may not be in a position to make informed decisions around what they are consenting to. Enforcement of consumer consent is also a cause for concern as the Data Protection Act may not be granular enough to cover specific meter data privacy. Furthermore, serious consideration needs to be given to how such consent management will be achieved where individuals are not 'digitally enabled' in an environment where meter & meter display functionality will be limited.

Data Storage

Data storage raises questions around data access and resilience. On access, two issues have been identified. Firstly, a number of industry bodies will require access to this data, not least the suppliers who would require regular and ad hoc access to data, albeit aggregated in order to make key customer and tariff management decisions; and, secondly, metering data only within the meters will create a technological as well as process impracticability. On resilience, singular data storage with no immediate back-up strategy will create resilience issues where meter data is lost by consumers (either wilfully or inadvertently).

Due to these concerns, one Intellect member has suggested that the programme should give consideration to the possibility of a centralised data store, perhaps within the DCC. They would envisage the DCC working alongside the Information Commissioner's Office (ICO) to create specific meter data protection standards which might be included as part of the DCC license.

Data Integrity & Confidentiality

Storage of large amounts of data locally within the meters also introduces security concerns such as the ability to hack into, or interrogate, meters, thus causing data integrity issues. This is closely linked to the concern around the sharing of meter data which could take place, for example, through rental turn-over or a change in the ownership of a property - a change in tenancy status would mean new occupiers having access to meter data from previous incumbents.

This could also cause a problem if residences change from domestic to non-domestic status, as this then raises questions over ownership of the data. Clearing down or sanitising this data without any other form of storage or data source would again cause loss of data, especially if the customer wishes their data to move with them.

We seek views from stakeholders on what level of data aggregation and frequency of access to smart metering data is necessary in order for industry to fulfil regulated duties.

Intellect members await further guidance on what levels of data aggregation and frequency of access to smart meter data are required. Our members are clear that it will be important for the regulated duties to be formed around not just the smart metering rollout but also the need to enable the overall ambitions of the smart grid.

Furthermore, our members note that whatever level of data aggregation and frequency of access is decided upon, there will be material implications on the security design and cost of operations of the overall solution - especially the 'thickness' of services required to be provided by the DCC. At this stage, they also note that some DCC functionality will be required throughout the roll-out stages.

Do you support the proposal to develop a privacy charter?

Intellect members support the proposals to develop a privacy charter to reduce concerns amongst the public and to ensure that all those involved in the smart metering supply chain understand the risks and governance challenges concerning privacy.

One Intellect members notes that in recent times, the privacy debate has moved away from surveillance and analogue interception and into networks capable of carrying millions of packets of personal data around the world to various companies and other third parties.

A privacy charter is therefore needed that takes account of these changes. To enable such a charter, the industry needs to be prepared to report against conformance with the charter, which will therefore need defined processes to underpin it and to deliver that adherence. To ensure such accountability, a method for auditing is also required. In the longer term, our members broadly believe that the DCC is best placed to oversee and manage compliance against the privacy charter, however in the interim this will be problematic and a suitable body will need to be appointed to undertake the enforcing role.

What issues should be covered in a privacy charter?

Intellect members have identified a variety of issues that could be covered in a privacy charter, a collection of which are detailed below:

- The right of the customer to have control over their detailed consumption data not just on a one off basis which they sign-off when they initially receive their smart meter but on an on-going basis
- In particular, controls need to be established so that the customer can readily see which companies have access to their data and for what purpose, as well as whether they are passing on any information to other 3rd parties. In effect, a dynamic data access lifecycle control process needs to be established which informs the customer and seeks consent when any aspect of this changes
- A best practice approach to ensuring high security and governance levels
- How to ensure anyone handling or processing data is held accountable and accepts ownership of risk
- How to ensure information is accurate, available and have the ability to be corrected
- How to assert that all processes and the existence of services requiring access to consumer data are transparent

- How to promise consumer safety and privacy, but be sure to limit the collection of the data to the minimum amount of personal information for the task required
- To what extent does the system manage consumer demand for data in the preference they wish
- How to enforce permissions for access to data that ensures the requirement of consent for data use or disclosure
- How to guarantee that expectations of the charter (such as data required for national security purposes or competition) do not infringe on the principles of the charter
- The charter should be supportive of the overall Smart Grid and Green Deal vision
- A charter could seek to insist on technical solutions to privacy issues rather than seeking to restrict access to information that may prove useful to effective and efficient grid operation, energy saving and carbon reduction.

In addition, Intellect members would expect that any obligations on the consumers would be included in the terms and conditions in the agreements between the consumers and suppliers or third parties.

Do you agree with our approach for ensuring the end-to end smart metering system is appropriately secure?

Intellect members broadly agree that the current approach is appropriate, though there remain concerns that certain issues have not yet been adequately considered – especially in terms of the ‘multi-staged’ deployment. In turn, Intellect members have highlighted a variety of other areas that warrant consideration from the project board:

- Because the metering solution is going to be used within a smart grid deployment, it is recommended that the programme board carry out an additional threat and risk analysis at the design stage, as the use of the data for making network operational decisions poses a different set of risks than for consumption settlement. An additional threat and risk analysis early in the design stage could reduce risks going forward.
- Ideally, security controls would not just be placed in the relevant application, but would include a combination of preventative and reactive controls that are natively embedded in each layer, in order to remove overdependence on application security
- There is a need for a central security governance authority responsible for the protection of the smart metering system that will ensure that security standards are agreed, adhered to, and independently audited. This body could facilitate co-operation across the industry, and will ensure that public and industry perception of the effectiveness of these standards remains positive.
- All stakeholders agree that interoperability is a key driver to the success of an end-to-end secure system. The smart metering system requires a central monitoring and brokering service to ensure all smart metering elements are able to interoperate in a secure manner from the outset a rationalised process framework with its associated cost savings for all parties.
- The approach of the Security Policy Framework (SPF) followed so far does not appear to provide a truly holistic security strategy and is unlikely to be understood or complied with by either the supplier and consumer communities. Any approach for securing a system end-to-end must include the availability and integrity impact perspectives and people and process controls perspectives if a holistic, and end to end, security solution is to be achieved.

- Although privacy is a major focus and concern for the Programme, equal consideration must be given to integrity and availability of the service from a supplier and consumer perspective. Integrity and availability, as well as privacy, should therefore also be major drivers in securing any system.

Intellect recommends that HMG security authorities need to be more fully engaged than at present, along with all industry parties and all as members of the PSAG, to reach an agreement that the end-to-end system will be appropriately secure.