Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

Call for evidence on data access and privacy – smart metering

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (ICO) welcomes DECC's call for evidence on data access and privacy and the opportunity to formally comment on the proposals. I appreciate that some of these questions are primarily aimed at the utilities providers so I have picked out the questions I feel are most relevant which should hopefully be enough to make our position clear.

I would like to pick up on the issue of consumer choice which is mentioned early on in this paper and in particular its references to explicit consent. First of all I should highlight that consent is not the only basis for processing personal data under the DPA, there are other conditions that are likely to be applicable. Secondly the phrase 'explicit consent' implies a high level of indication from the customer which may not always be required or even appropriate.

The phrase 'explicit consent' in DPA terms refers to the level of consent required for the processing of sensitive personal data such as criminal records, health records, sexual orientation… and means a clear indication of their agreement to process their data usually given in writing with the consumer's signature. It may often be more accurate to talk about the consumer giving 'informed' consent.

I understand that it is possible that smart metering might generate some sensitive personal data but much of the data will be less privacy intrusive. Perhaps the requirement for explicit consent for processing personal data gathered from smart meters would confuse suppliers or even distract them from legitimately processing personal data fairly. As a general guideline, if consent is the most appropriate condition for processing then you should first of all look at how intrusive the processing of the data is likely to be and then consider what the customer would reasonably expect. The more intrusive or removed the processing is from what a customer might reasonably expect the greater the level of care needed to ensure fair processing.

For example, where there are minimal amounts of personal data being processed or the data collected is fairly routine, such that the consumer might reasonably expect that their data is collected. It may be enough to give consumers notice or ready access to who is holding their data and how this is being processed.

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

Consumers should understand how their personal data is used and shared but this does not mean they need to be told what is obvious.

Data controllers should focus on what they will be telling their consumers in the context of providing clear explanation to how they gather and use personal data. This would go a long way to enabling the customer to making an informed choice which is important if the consumer is genuinely being asked to give their consent. The more intrusive processing of personal data is the more 'proactively' consumers will need to be told how their data is being used.

The other point to make about consent is that it must be 'freely given'. Smart meter suppliers should be careful not to claim that they have obtained the consent of consumers to processing their data by means that they have no real choice or control over. As I understand it one of the main aims of smart metering is to reduce the consumption of energy, by means of better network management or information given to consumers to be more energy efficient. This could pose the question what if a customer refuses to give their consent? If personal data is to be used this way and the consumer does not have any real choice about this then another condition for processing personal data should be relied upon.

Question 1 – Please submit any further evidence, such as surveys or consumer research, regarding privacy issues and smart metering. In particular is there evidence available about the effects of the availability and aggregation levels of more granular data (for example daily)?

We have no further evidence to add but we are supportive of the move to draw out the details of all privacy issues around smart metering at an early stage. The findings submitted to this response could provide valuable information that could help act as a basis for suppliers to carry out a Privacy Impact Assessment (PIA).

Privacy Impact Assessments are mentioned in the Article 29 Data Protection Working Party opinion 12/2011 on smart metering:

"Smart metering implementation should take place with privacy built in at the start, not just in terms of security measures, but also in terms of minimising the amount of personal data processed".

We expect suppliers to carry out an assessment of the privacy issues created by the implementation of smart metering as soon as possible. This approach can be useful to suppliers as it starts a thought process to look at the broader privacy risks raised by the implementation of smart metering and consider ways of mitigating risks at a very early stage. Sometimes we find that management of privacy does not go much further than looking at what the data security concerns are. Clearly privacy concerns are broader than security concerns for smart metering implementation.

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

The PIA is often a cost effective measure as it can save the industry from having to 'bolt on' privacy solutions at a later date which can often prove costly.

Already there has been some concern on the privacy impact of smart meters collecting more granular data from consumers. We hope that further evidence gathered from the industry and other parties concerned with smart metering will help to reach a solution that is practical to industry while respectful of individual privacy.

Question 5 – Should theft management be considered a regulated duty for which suppliers would have access to a certain level of smart metering data? What level of data would be required and how would this be used to manage theft?

Personal data relating to theft management is likely to be sensitive and we would expect the data to be offered greater protection as to who can access the data. This would mean that we would expect the data would only be accessible when appropriate

Please see question 6 for our response to what level of data is required.

Question 6 – Does data need to be collected from all customers all of the time, for theft management, or could there be a trigger for accessing more detailed data (where theft is suspected)?

The key consideration we would want suppliers to understand is whether collection and processing all customer personal data is a necessary and proportionate response to the problem of theft management.

We feel it would be hard to justify that in order for suppliers to combat energy theft effectively, they would need to collect personal data from their customers all the time. If such an approach were to be adopted we would then expect the utility sector to have strong arguments in place as to the necessity of the continuous collection of personal data so that the Commissioner would be satisfied that this is a proportionate response from the utility sector to the problem of energy theft.

I should draw attention to the Article 29 Data Protection Working Party opinion 12/2011 on smart metering:

"The Data Protection Directive regulates against the processing of personal data where the processing is excessive with regard to the purpose".

The opinion draws attention to the fact that although the collection of all customer personal data could allow for the 'identification of suspicious and, in some cases,

illegal activities'. This does not mean that all data should be collected just in case it reveals something untoward. The collection of personal data for the purposes of theft management should be enough so that the data is fit for purpose but not excessive.

Suppliers should consider what personal data needs to be gathered in order to act as a trigger that there may theft of energy and not collect data 'just in case' it might prove useful but its usefulness is merely speculative.

Once a trigger has been hit then clearly it is appropriate to warrant a more intrusive investigation in to the consumer's behaviour.

Privacy notices should reflect on the fact that the consumer's personal data may be gathered and used to prevent energy theft but suppliers may be able to rely on section 29 on a case by case basis where an investigation in to the consumer is warranted

Question 12 – How could smart metering data be used to identify and protect vulnerable customers? Should such activity be considered a regulated duty and are any licence changes needed to create particular duties on suppliers in this area?

The protection of vulnerable customers is of paramount concern to everyone but there is clearly a significant risk to the consumer and the reputation of the industry as a whole if suppliers somehow get this wrong. Therefore it is very important that measures adopted should treat the data securely to prevent exploitation and sensitively to save the customers from poor customer handling.

It may be helpful if the utility sector could consider this as a whole and adopt a consistent approach.

Suppliers need to consider what data would be useful in identifying and protecting vulnerable customers. How much personal data would it be appropriate to hold about customers deemed or suspected to be vulnerable? Does the data need to be shared between different suppliers?

It's my understanding that smart meter data could indicate unusual energy usage that could be indicative that the consumer could be vulnerable in some way. Clearly this is information suppliers would want to act upon and further investigate the customer's circumstances and report back on their findings but it raises the questions as to what data should be kept on file.

Customers may volunteer information about themselves and even explicitly consent to very sensitive information being kept on file. Yet it is more likely to be the case that either data collected by the smart meter or some form of customer contact may prompt a concern over the customer's welfare. The supplier may

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

want to flag that there is a possibility that a consumer is vulnerable so that they may be treated sensitively and with care but without making a whole list of assumptions about that person.

If there is a concern about the customer's welfare then it might be appropriate in some limited circumstances to mark the file as such. Yet this is less likely to require marking customer files with sensitive personal data such as a medical diagnosis as this could lead to unfounded assumptions being made about individuals. It may be more appropriate to record information about how the customer prefers to be contacted or details of a person who manages their affairs for them.

Suppliers should also consider periodically reviewing the data they hold on vulnerable customers so that customer accounts are kept up to date and accurate and not marked as vulnerable where there is no justification for doing so.

Consumers can change suppliers so it may be appropriate to share only relevant data with other suppliers in a way that is in the best interests of the consumer and does not discriminate against them in any way. Suppliers should be clear as to what information needs to be shared, ensure the data is accurate and periodically review the sharing of such data in accordance with the ICO Data Sharing Code of Practice.

Question 14 – Do you agree with the requirement for such data to be anonymised or aggregated wherever possible, and how should this be monitored?

The industry should use anonymised or aggregated data wherever it is practical to do so.

The benefit of using data that has truly been anonymised or aggregated so that no individual can be identified is that it is inherently more secure to individuals and less intrusive than using personal data.

I should make it clear that our view is that data is only truly anonymised or aggregated when there is no realistic possibility of identifying an individual.

The data will not be considered as anonymised or aggregated in the hands of any organisation that holds both the anonymised data and the key to unlocking the data. Any organisation capable of unlocking the data would be considered to be handling personal data for the purposes of the DPA and the usual requirements of the act still apply.

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

Question 15 – Would suppliers be expected to advise consumers of network company usage of data given network companies do not have a direct relationship with customers?

It seems reasonable to expect that suppliers should be transparent about how personal data is processed and how info that is 'created' by a household meter is used throughout the supply chain. This could be useful in making sure customers are not under the impression that personal data are being processed when in fact they are not.

The DPA requires the data subject to be informed as to the identity of the organisation in control of the processing and the purposes as to which the data will be used. However it is sometimes enough if the data subject has the contact details of the organisation in control of their data and details of any third party handling their data can be found relatively easily.

We would expect consumers to be advised of network company usage if the data that is being used in a way that could be intrusive to the consumer or is inconsistent for the usage the data was originally collected for.

Question 16 – Are there any alternatives to a basic opt in or opt out approach to consumer choice such as a prompted choice? What are the practical and consumer protection considerations in relation to different options (for example when and how)? From a consumer perspective what alternative approaches and vehicles (for example letter, e-mail, phone) to seek customer consent are there?

Typically organisations from all sectors tend to offer the consumer the right to either opt in or opt out when it comes to making a decision as to what information they'd like to receive in future.

The ICO's concern here is that the individual is presented with enough information to make an informed choice and that their decision is respected by the organisation offering the information.

While I can fully understand why suppliers want to maximise opt in to information from their consumers, they should take care to ensure that the consent they receive is genuine and freely given.

The industry should be clear that opting in to providing personal data to a supplier or third party may be subject to specific rules if the personal data are to be used for direct marketing purposes.

Question 19 – What parts of the privacy policy framework do you think should be delivered by regulation and why?

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

The key outcome is to have effective privacy controls and checks in place, providing clear accountability and instruction for consistency, but these need to be flexible enough to address unforeseen problems and allow for future change. Perhaps the most fundamental points relating to privacy could be set by industry self-regulation and the finer detail set out by agreement between suppliers.

Self-regulation is likely to be an effective measure towards achieving compliance because what is set out in this way is likely to carry more weight with suppliers and can provide absolute clarity to accountability, standards and consistency. Provided regulation is not left too wide open to create ambiguity.

We would hope that the framework would remove any ambiguity as to who is acting as the data controller at each stage of processing personal data.

We would also want a clear process for handling subject access requests from consumers which is a frequently overlooked issue which can become confusing, especially to the data subject, when personal data is being shared by a number of different organisations.

Question 20 – What is the most effective way to set out any sector specific protections around privacy (e.g. licence conditions or other alternatives)?

It seems entirely appropriate for the energy sector to identify privacy measures to be taken that are specific to their sector. We would have thought the most effective way to set out what these concerns are would be to look at what are the most privacy intrusive features of smart metering right from the very start and build in protections around them.

The key will be to identify from the beginning where the biggest privacy concerns are and focus specifically on how these can be addressed. For example, it seems to be clear that the biggest privacy concerns are not about the aggregated data that will be used to improve the efficiency of energy supply but will be more about the granular data that can be obtained from smart meters, who shall have access to this data and for what purposes will this be used.

Question 21 – What practical options for authentication would provide the right balance between allowing easy access to consumer data in the home while providing the necessary privacy protection? Are there any other issues or options that the programme should be considering in developing the approach in this area?

The options seem to be either asking the consumer to authenticate any further devices (and I presume updates) that can link in to the Home Area Network (HAN) of the smart meter or allow access to the smart meter via the DCC.

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

If consumer authentication is to be the preferred option, perhaps this could be achieved by pressing a single button rather than require manufacturers of smart meters to include a keypad on their devices just to input an access code printed on the meter.

The consumer selecting the button could initiate the pairing of devices within a set time frame allowing set-up. The new device could be loaded with a certificate from the smart meter provider/DCC which authenticates which data it is permitted to access.

Potentially the certificate could be forged but that would still require the user to have purchased it (possibly on the black market) and to have initiated the pairing event. The smart meter could also check for updates to a central repository of revoked certificates, e.g. held by the DCC. For example, if a third-party went bankrupt you could remote-kill all of their devices to ensure they cannot collect anymore data in a way similar to how websites authenticate themselves to browsers and negotiate a secure connection.

Alternatively access could be via the DCC to the smart meter for contractually committed third parties but this could present some security vulnerabilities and would need to have sufficient checks on place and an audit function, particularly around the most sensitive data.

Question 23 – What sort of arrangements would provide an appropriate balance between providing ease of access for consumers seeking to sign up to new services and adequate protection for consumers' data when accessed via DCC?

First of all we would hope that only authorised organisations would be able to access consumer personal data via the DCC and that they would only have access to relevant data that they require to provide their service or perform their function. Secondly the organisation taking on the role of DCC would need to have adequate security measures in place.