Monkton Reach, Monkton Hill,
Chippenham, Wiltshire, SN15 1EE
www.goodenergy.co.uk
enquiries@goodenergy.co.uk
0845 6011410

Smart Metering Implementation Programme – Roll-out team
Department of Energy & Climate Change
3 Whitehall Place
London
SW1A 2AW

13 October 2011

Dear Sirs

Data Access and Privacy call for evidence

Thank you for the invitation to respond to the above call for evidence. As you are aware, Good Energy is a unique small electricity and gas supplier, as we only supply customers with 100% certified renewable electricity, and gas which supports renewable heat. It is our mission to provide a blueprint for the UK to transform itself to a low carbon, 100% renewable economy through the work that we do and the actions of our customers and renewable generators.

Executive Summary

We believe that in this debate we must split the issue of security and privacy. Suppliers already hold customer sensitive information and the onus on us through data protection law already exists to protect any data we have and keep it secure. On the privacy side we believe it is not a question of access to data, but one of use of data.

We fully support the view that Suppliers should receive explicit consent to use the data to offer additional services to consumers, but several of the benefits set out in DECC's initial impact assessment are opaque to the customer, but will deliver costs savings through the industry, which will not be achieved if the industry if access is curtailed to only those sites giving explicit consent.

For your ease we have responded to the questions asked, expanding where necessary.

Q1. Please submit 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 believe that a distinction needs to be drawn between data privacy and data security. Data privacy is about what a legitimate holder of data can use it for, whereas, data security is about unauthorised access to the data. Public concern about the latter should not formulate the rules regarding the former. The question is not what data licensed industry parties hold, but what they use it for. General data protection law states that entities should only hold data reasonable to deliver the service required, and this should be the guiding principle.

Suppliers currently hold much more sensitive information about customers including bank account details, date of birth etc, and the premise should be that licensed supplier can hold whatever data they possess securely.

Q2. To what extent would different rules for access to data between suppliers and third parties be expected to impact on the development of energy services market (in terms of product and tariff innovation and/or entry to the energy market by third parties)? What are the particular data uses to which these concerns apply?

The distinction is not what data suppliers may hold, but what they may use it for. Suppliers should require explicit consent from customers to use their data for the offering of energy services. The only difference would be that they would already hold it, whereas 3rd parties would not only require consent, but also access to the data. It should however be borne in mind that an

energy supplier is a licensed and regulated activity, whereas 3rd parties providing energy services have no requirement to be licensed or regulated.

On tariff development, then there is already an onus on suppliers to guide customers to the tariff that best suits their requirements and therefore use of data for this purpose should remain a regulatory requirement.

Currently, new entrants to the energy market do not have access to physical reads, and thus smart metering should not change that situation.

Q3. Are there any data uses, apart from those set out below, where the arrangements for access to data could have an impact on the benefits of the programme. How does this analysis differ for the gas market?

Although not an immediate concern, the ability to access data in order to enable demand side response should not be hindered by data privacy rules. As we move to a market with a greater degree of intermittent and localised generation, then there could be a need for suppliers or network companies to load manage supplies. This can only be done effectively if they have sufficient granularity of data.

Q4. What type of energy services and energy advice could be provided by the market (by suppliers and / or ESCOs / potential new entrants) that require access to specific levels of data? What level of data granularity (frequency, time lag) are needed to provide such services and what is the potential impact of these services in terms of the percentage energy savings? Please provide empirical examples and explain the basis of any assumptions and distinguish between gas and electricity.

Energy companies and 3rd parties currently offer energy efficiency advice to customers without access to the customer's consumption profile. Customers will be able to access their profiled consumption using the IHD or alternative methods if offered, but this would be at the customer's consent. Providing unsolicited energy efficiency advice based on usage patterns is not likely to be cost effective, for electricity and even less for gas.

Q5 Should theft management be considered a regulated duty for which suppliers should 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? Please provide practical examples.

Theft is paid for by all customers and thus the use of metering data to deter and detect theft should be a reasonable use of the data concerned. In addition, meter tampering can make the supply dangerous and thus there are health and safety implications which need to be considered.

A certain amount of detection will achieved by access to tamper alerts and regular readings. Other cases may require a higher degree of granularity, possible at the request of law enforcement agencies. Suppliers should not be restrained from the granularity or frequency where theft is suspected.

Q6. 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 (for example where theft is suspected)?

It would not be practical to monitor all customers' detailed data to detect theft. However access to historic information once theft is suspected is needed both for comparison, and if taken to court quantifying the theft. As mentioned above, when investigating theft, there should be no curtailment on the amount of data accessed. However, such investigations should be approved by an appropriate officer of the company and the reasons for suspicion recorded.

Q7. What level of take up of time of use tariffs could be expected under different scenarios for access to data? What information is needed to design time of use tariffs? In particular would sample or anonymised data be sufficient?

The take up of time of use tariffs is currently constrained by the fact that settlement for domestic customers is profiled, thus any load shifting by customers is not reflected in their purchasing requirements. If the costs of settling domestic customers half-hourly could be reduced sufficiently, then bespoke ToU tariffs including DSR and dynamic tariffs could be a realistic option.

As tariff design will need to reflect certain characteristics, then anonmysing the data does not make sense. For example, designing a tariff for EV users would require data from customers with electric vehicles. The person doing the analysis may not need the customers name, but the customers characteristics would need to be held by the supplier's systems with the name and address somewhere. With regard to sample data, this may be possible for larger suppliers, but for smaller suppliers there may be a need to use all available data to achieve a robust sample size.

Q8. Do you agree that individual half-hourly data is not currently required for suppliers to meet their obligation in relation to settlement? Over what timescale are any changes to settlement likely to take place and what might be the implications in terms of data requirements?

As discussed in the consultation by Elexon, half hourly data is not currently required for settlement purposes for electricity. The views expressed in the consultation were that without a clear understanding around the DCC and availability and costs of HH data via smart metering, now would be the wrong time to make any decisions although there are benefits in switching to HH settlements. That said, voluntary settlement of smaller sites should be possible and the industry needs to drive down costs so that the cost benefits stack up.

Q9. How far might aggregated or sample data provide suppliers' with what they need for wholesale hedging? Please provide examples of how the data would be used and where possible quantify potential benefit s and costs

As long as settlements remain NHH then the need to use HH data for hedging is not necessary as profiling removes shape and volume risks are already improved by actual routine reads. If settlements were to move to HH for smart metering sites, then hedging would require the same degree of detail and thus sample would not work, but aggregated would. However, if HH data is collected for settlements, then it would make sense to use it for billing, and as such individual data would be required.

Q10. What level of data would be required and how would this be used to manage debt? Please provide practical examples.

The use of different granularity of data would be on a case by case basis in agreement with the customer in most cases, but it should not be restricted. For example, a supplier may be concerned about energy usage at an empty property, and the use of HH data could help establish why the debt is accruing with or without the bill payers consent. We do not envisage data above routine reads are necessary for identifying debt or high debt risk customers in the first place.

Q11. How would suppliers envisage using daily data to support debt management and what evidence do they have to support claims of additional savings that could be achieved with access to daily data as opposed to less frequent data?

Most customers in a debt situation would like to work with their supplier to manage their debt and as such are likely to agree to allow their supplier to use the data for this purpose. Where the customer's co-operation is not available, then access to real time data could offer alternative to disconnections by giving the supplier a better understanding of the properties energy use.

Q12. How could smart metering data be used to identify and protect vulnerable customers? Should such activity be considered a regulated duty and are there any licence changes needed to create particular duties on suppliers in this area?

Identifying and protecting vulnerable customers should not be a regulated duty. Where vulnerable customers are identified, then suppliers could use greater access to data to provide vulnerable customer services with the customers consent to the use of that data for that purpose.

Q13. Do you consider that the use of data by network companies to support them in maintaining an efficient and economic network should be considered a regulated duty?

Yes. Customers are unlikely to see direct benefits from this and as such it should be a regulated duty. However, it should be stated what are the specific

Q14. Do you agree with the requirement for such data to be anonymised or aggregated wherever possible, and how should this be monitored?

The question here is the degree of anonymisation. Network companies are likely to be able in some cases to identify individual properties, however, this should not require them to know the name of the property owner/occupier, thus it is partially annonymised. It may be that certain work can use aggregated data, however as the network company may need the data to be aggregated in a certain sample on their network, then they would need to hold the source data.

Q15. Would suppliers be expected to advise consumers of network company usage of data given that network companies do not have a direct relationship with customers?

When signing a supply contract, customers also sign the standard network terms. This information should be included in here.

Q16. Are there any alternatives to a basic opt in or opt out approach to consumer choice such as some form of 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?

We believe that the issue is not about access to data, but about restricting the use of the data. Suppliers and network companies need to access half hourly in order to efficiently deliver the service. Customers should then have to opt in to additional usage of that data, just as they currently have to opt in the receive marketing information from either the supplier or 3rd parties.

Q17. What evidence is there of likely take-up rates that could be achieved through different approaches to consumer choice?

If suppliers and networks have access to carry out their licensed activity, then take-up for additional uses of the data should only occur when a service is of value to the customer. The key issue should be that companies cannot analyse the data to access a customer's suitability for additional services, they should seek permission first. Thus giving customers the comfort that the data is only being used to provide electricity or gas in an efficient manner.

Q18. What current and future technical options exist for energy consumption data minimisation / privacy enhancement technologies? How might aggregated or anonymised data be provided in practice? Would this imply additional services to be provided by the DCC?

This level of complexity is difficult for smaller suppliers. The data should be stored once and aggregated as necessary. Given the supplier and network companies have the data for regulatory purposes, then to insist that different applications also store it in aggregated form is a wasted effort. As a matter of good data protection principle, where the data is provided to 3rd parties for analytical work, then it should be aggregated and/or anonymised unless the analysis required that level of detail.

Q19. What parts of the privacy policy framework do you think should be delivered by regulation and why?

The regulatory framework should identify the use of data constraints for the purpose of efficient delivery of electricity and gas. Once a customer gives wider consent, then standard DPA rules apply.

Q20. What is the most effective way to set out any sector specific protections around privacy (e.g. licence conditions or other alternatives)?

We believe licence conditions are the most appropriate. It is likely that the terms of this condition will need revising once smart metering becomes more widespread, either to clarify an interpretation or an unintended consequence and licence conditions are the best approach.

Q21. 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 most practicable option would be to copy the process of attaching additional devices to WiFi broadband by use of a numeric key. Suppliers should be able to either provide key data on Change of tenancy, and if a customer believes that data security has been accessed reset the key.

Q22. Are there other issues that need to be considered to make using the HAN a viable route for access to data in the home, rom either a process or consumer perspective?

As Suppliers do not have an enduring obligation to provide an IHD, then connecting to the HAN should not require the IHD to be a required to facilitate this connection.

Q23. What sort of arrangements would provide an appropriate balance between ease of access for consumers seeking to sign up to new services and adequate protection for consumers' data when accessed via the DCC?

It is important that there is an independent record of any arrangement between a non-SEC signatory and a customer, this will either have to be held by the DCC or the customer's supplier. This is needed to ensure that the access is curtailed on a change of occupier.

Q24. Are there other issues or options that the programme should be thinking about for the foundation stage or for non-domestic customers to facilitate access to data?

Confidence in the smart metering programme could be impacted if mis-use of data occurs in the foundation stage even if the meters concerned are not smart compliant. The general duty of care that exists under existing DPA should suffice, but an breeches should be reported to both the ICO and Ofgem. Where systematic breeches or mis-use are occurring, then Ofgem should act.

Q25. Do you have any suggestions as to how the foundation stage can be used to further learn about our approach to data access and privacy?

The foundation stage should assess whether there is a genuine concern about data privacy amongst consumers in comparison to data held by other bodies (telecoms, broadband, loyalty cards etc.) Building restrictive barriers around a threat that consumers do not believe is important should be avoided.

[redacted]