



**Consumer  
Focus**  
Campaigning for a fair deal

# **Consumer Focus response to Smart Metering Implementation Programme: Data privacy and Security**

October 2010

# Contents

Introduction	3
Specific questions	4
Consumer Focus summary of recommendations/views	14
Annex 1: Our privacy concerns	16

## About Consumer Focus

Consumer Focus is the statutory consumer champion for England, Wales, Scotland and (for postal consumers) Northern Ireland. We were formed by the The Consumers, Estate Agents and Redress (CEAR) Act 2007.

We operate across the whole of the economy, persuading businesses, public services and policy makers to put consumers at the heart of what they do.

Consumer Focus tackles the issues that matter to consumers, and aims to give people a stronger voice. We don't just draw attention to problems – we work with consumers and with a range of organisations to champion creative solutions that make a difference to consumers' lives.

Consumer Focus has strong legislative powers. These include the right to investigate any consumer complaint if they are of wider interest, the right to open up information from providers, the power to conduct research and the ability to make an official super-complaint about failing services.

We receive about a third of our funding from BIS. Funding also comes from licenses paid by energy suppliers and the postal industry. We are also able to raise our own funds – for example, through externally funded projects.

# Introduction

---

Consumer Focus supports the rollout of smart meters as a way to end estimated billing – a major source of consumer complaints – and as a tool to help deliver public policy goals of carbon reduction, security of supply and affordable energy. We also see great opportunities around the improved delivery of social assistance to vulnerable and low income households.

However, we have consistently raised concerns that – without the right regulatory framework, technology and the appropriate rollout mechanisms – smart metering could result in increased detriment for consumers and failure to realise the proposed benefits.

Rollout needs to be delivered in a way that maximises meaningful consumer choice, drives down prices and enables customers to make well-informed and effective purchasing decisions. We think that all these goals can be achieved without sacrificing essential consumer and human rights to privacy and data protection and this view shapes our response to this consultation.

Consumer Focus has consistently highlighted the potential risks that new smart functionality poses – in particular, around data protection and privacy<sup>1</sup>. We welcome Government and Ofgem’s recognition that this is an issue that needs to be taken seriously as well as the decision to set up a Privacy and Security Advisory Group to look at this issue in more detail. The experience in the Netherlands, where privacy concerns contributed towards the halting of rollout of smart metering, is a stark reminder of the importance of tackling existing and potential consumer concerns over a ‘spy in the home’. This is necessary, not only to protect consumers, but also to maximise consumer engagement.

It is also essential that privacy risks are tackled as a matter of urgency as tens of thousands of consumers already have smart meters, and the early rollout of this technology by some energy suppliers means that millions of customers are expected to have smart meters within the next couple of years. We look forward to further working with Ofgem, DECC, industry and the Information Commissioner’s Office (ICO) in this area.

Our response to this consultation on Data Privacy and Security should be read alongside our responses to the smart metering consultations on:

- Implementation Strategy
- Rollout Strategy
- Consumer Protection
- In-Home Displays (IHDs)
- Non Domestic Sector

---

<sup>1</sup> See Annex 1 attached on Consumer Focus’s privacy and security concerns.

# Specific questions

---

## Question 1: Do you have any comments on our overall approach to data privacy?

Overall we commend the pro-consumer way in which the smart metering implementation programme intends to address the issues of privacy and security and the focus given to this. Consumer Focus's research and wider evidence indicates that despite changing social norms, personal privacy and misuse of personal data are key concerns for many people<sup>2</sup>. Protection against hacking and security breaches will be essential not only for national security but also to prevent unauthorised disconnection of individual appliances or energy supply, which could have dire consequences for vulnerable consumers who are dependent on energy for their health and well being.

In particular, we support the principle of adopting privacy by design for the end to end smart metering system,<sup>3</sup> and using the meter as the primary depositor of historic energy consumption information, in terms of data handling and access practices. Consumer Focus has pressed for this approach and is pleased to see it in the proposals.

By linking the meters to the in-home display (IHD) consumers should be able to directly access information on their historic energy consumption and related costs, free of charge, in a way that that best safeguards personal privacy. This is also in line with the EU Third Energy Package's requirements around provision of information on energy use.<sup>4</sup>

We note and welcome the consideration given to the experiences in other countries and the active monitoring of work at the European Union (EU) level, in particular the multi-stakeholder Expert Group 2 of the Smart Grid Task Force on security and privacy issues. Consumer Focus has actively contributed to the work of this Task Force through our umbrella association BEUC (European Consumers' Organisation), and so far we are broadly pleased with the results delivered by this multi-stakeholder group<sup>5</sup>.

However, this Prospectus document is very high level and only addresses, for the most part, the general principles in the existing data protection legislation, as they would apply in the case of smart meters. It does not address the possible gaps in the existing Data Protection Act (DPA), or other legislation that may apply because of the smart meter's new role as a communication device; and it does not address commercial/marketing implications that may arise through increased disclosure of consumer energy consumption and consequently lifestyles.

---

<sup>2</sup> See Annex 2 attached: This includes a summary of Private lives: a people's inquiry into personal information. Peter Bradwell. Demos (2010). And an ICM online survey of 2,000 people on behalf of Consumer Focus March 2010. See also Annex 1.

<sup>3</sup> Our fundamental requirement is for privacy by design, which means that the communications and security architecture and standards should be built in at the outset for the hardware, software as well as any systems and processes rather than bolted on later on. This should apply to connections between the home meter and the energy supplier, home meter and the central communication provider, as well as the in-home local area network. Systems and meters should be road tested before mass roll-out, for a minimum of six months.

<sup>4</sup> Directive 2009/72/EC (concerning common rules for the internal market in electricity), Annex 1 Measures on Consumer Protection art. 1 (h), (i)

<sup>5</sup> The Task Force on Smart Grids Expert Group 2. Regulatory Recommendations for data safety, data handling, and data protection. Report Version 1.2. July 29, 2010

The lack of detail at this stage makes it difficult to assess whether the final policy and practice will achieve the right balance between consumers' personal information privacy, industry needs and wider societal interests. In several places there is an underlying tension between the good and strong intentions to safeguard personal information privacy and the reflected desire and need of some of the stakeholders to acquire it.<sup>6</sup>

We therefore also strongly support the intention to consult stakeholders further and recommend that, at the earliest opportunity, as proposed: a) the Privacy and Security Advisory Group is expanded to include a wider range of external stakeholders, and/or b) that a task force or working group is set up, on the model and with a remit similar to the EU Task Force Smart Grids Expert Group on data privacy and security. This group should comprise all relevant stakeholders, including experts from academia and non-governmental privacy organisations and legal experts on data protection. It should also make good use of the work already carried out by EU's Task Force.

It is essential that any potential consumer privacy and security concerns have a safe forum in which they can be aired and promptly addressed. As mentioned, the experience in the Netherlands is a reminder of what can happen when consumer groups are left 'outside of the decision making tent'.

We also request that a timetable for action is outlined as a matter of priority. With more than two million meters with some form of 'smartness' expected to be installed by 2012, it is essential that protections are put in place as a matter of urgency.

Consumer Focus has recently issued an information request to suppliers to establish current practices in relation to smart data and is seeking legal advice on whether company activities are in breach of existing privacy legislation including in relation to Article 8 – Right to Respect for Private and Family Life, of the European Convention on Human Rights. The findings of this investigation will be made available to Ofgem and DECC.

The following are more substantive comments on sections in the document:

### Existing safeguards (3.1 to 3.2)

- This section mentions the Data Protection Act, while the European Convention on Human Rights is mentioned elsewhere in passing. The Privacy and Electronic Communications (EC Directive) Regulations 2003 might also apply in the case of smart meters and smart grids, whether they use GPRS or any other communication protocols. These regulations, inter alia, lay down provisions regarding confidential communications, the processing of traffic and location data – these can well be personal data, so the application of this legislation in the case of smart meters also needs to be assessed. This is one of the tasks being carried out by the EU task force group mentioned above.

The supporting document also mentions elsewhere (section 2.27) that the programme has considered the online targeting of advertising and prices market study recently published by the Office of Fair Trading (OFT) and recognises that there are potential lessons there for the smart meters too. Our view is that the lessons from the internet marketing and advertising 'eco-system' are to be taken very seriously in the case of smart meters. This is particularly important as the targeting and the capture of data from single households can be far more precise than in the case of internet browsing – both the households and their in-house display systems are potential sitting ducks for ruthless marketing practices.

---

<sup>6</sup> This comes out for eg in sections 3.14, 3.15 and 3.17

Consumer Focus recognises that there may be benefits to communicating certain types of information to customers via their IHD, eg notice of service interruptions, re-enablement of supply etc but careful consideration will be needed about what information is communicated and customers must actively opt into this rather than messages being sent to the IHD as the default setting. Consumer Focus is carrying out research into customer attitudes towards receiving messages via the IHD and will share this with Ofgem and DECC when it is available.

- Gaps in existing legislation, and related to specificities of smart metering need to be identified and addressed; in particular the UK DPA is considered to be weaker than its European counterparts in a number of areas, including the ICO's enforcement powers and its definition of consumer consent. Particular weaknesses, also in the EU legislation, include the responsibilities of third parties who may also process personal consumer data. These weaknesses need to be addressed in any approach towards smart meters.

### Low levels of compliance

There is an 'abysmally low' level of compliance with data protection law by 'data controllers' and 'data processors'. For instance, the transparency rules – ie the legal obligations to inform consumers and citizens (data subjects) about the collection and processing of personal data – do not work. Many privacy policies, particularly those of online service providers, do not abide by the compulsory transparency rules; many do not have privacy policies at all<sup>7</sup>.

### Inadequate redress procedures

The rights of consumers (data subjects) are increasingly abused and it is very difficult for ordinary people to identify and correct errors, which may only become apparent when something goes seriously wrong. There is also very little that consumers can do if their data is disclosed deliberately, hacked into or lost through negligence. When these rights are breached, consumers do not receive redress. The remedies provided on complaints to the ICO are very limited, while litigation is not practical and very expensive for the majority of people, so in reality civil actions are rare or non-existent<sup>8</sup>.

Privacy guidelines for smart meters will need to include advice, dispute resolution and redress issues – specifically who is to be charged with these responsibilities. The natural home for enforcement and redress in this area is the Information Commissioner, however Consumer Focus has concerns that this office does not have sufficient resources to investigate and enforce adequately the existing environment.

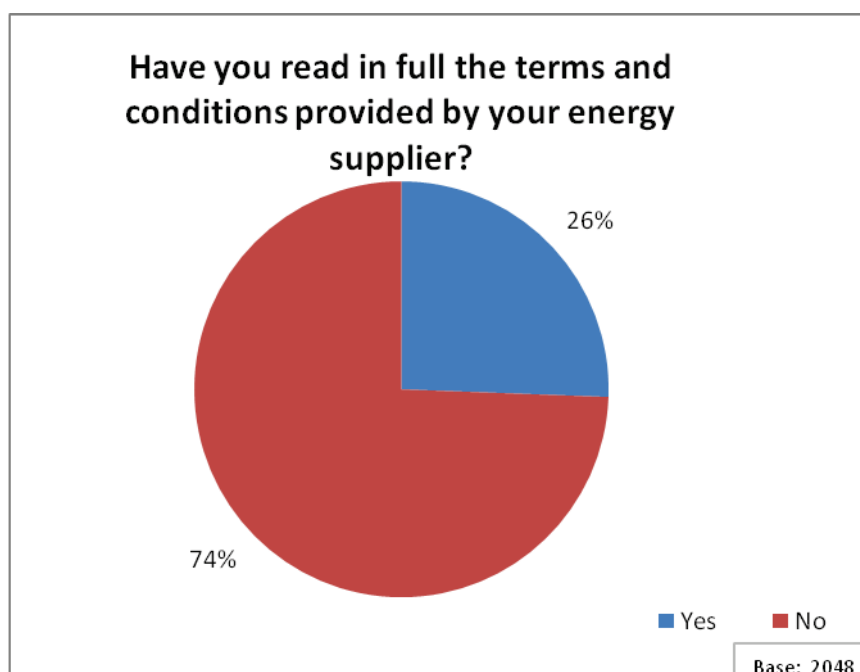
---

<sup>7</sup> See inter alia: New Challenges to Data Protection, Final Report, European Commission – DG JFS, January 2010, page 45, also Annex 6, United Kingdom Country Study, <http://bit.ly/bkJsSx>. Also Data sharing and data protection – National Consumer Council's response to Data Sharing Directive 2008, <http://bit.ly/as9VK4> and more generally evidence provided in the Consumer Focus response to ICO consultation on a Code of Practice for personal information online, March 2009, <http://bit.ly/auMbTY>.

<sup>8</sup> Ibid. Regarding applicable law, see also BEUC response to the consultation on the EU Data Protection Framework, December 2009, p.7 <http://bit.ly/aQoL0Q>

## Consumer understanding of their privacy rights is poor

The vast majority of consumers do not read privacy notices, because they are long, over-complicated, incomprehensible and obscure on vital issues, such as with what third parties data is shared with, and who these third parties are or what they intend to do with the data<sup>9</sup>. Consumer Focus's survey (March 2010) found that only 26 per cent of people have read in full their energy terms and conditions<sup>10</sup>. This is a reminder of the importance of consumer opt-in mechanisms as a meaningful way for giving consent.



## Rules around transmission of data are weak

Energy suppliers/distributors are global companies, and may wish for economic and other efficiency reasons to store data in another country out-of-EU jurisdiction (for eg if they have out-of-EU server facilities) or to use a third party to process and store data in a different location.

If the harm is done when information is stored or transferred overseas, there are questions of applicable law as well as other practical barriers. There would be no possibility for group action, which would help larger groups of consumers whose personal information has been disclosed illegally for example.

Export of UK consumer personal information to third countries (outside EU) with weaker data protection legislation, and legal uncertainty regarding applicable law and the competent jurisdiction raise serious concerns. This issue is increasingly acute with the advent of 'cloud computing', as well as extensive use of call centres outside the EU. It is also compounded by the EU's slow process in confirming which countries have adequate data protection legislation (the adequacy test) and by the very poor implementation of the US-EU Safe Harbor agreements, whereby US companies who want to do business with the EU self-certify that they adhere to the EU data protection principles.

<sup>9</sup> Research from other market sectors. For example: Research report: Fair Processing Notification, current effectiveness and opportunities for improvement, IC, 2007 <http://bit.ly/9A0siR>.

<sup>10</sup> This stretches from 20 per cent for 18-24s to 35 per cent of 55-64s. Those in social groups DE said they were most likely to read the Terms and Conditions; 30 per cent versus C1 23 per cent and AB 25 per cent.

## No legal responsibilities for third parties

There are no legal responsibilities for third parties, with the result that many companies collecting personal data pass it on to third parties that often process this data for different purposes from those initially notified by the data controller. The regulatory framework neglects altogether the area of liability for third party data loss and negligence<sup>11</sup>. This is particularly important given the day to day involvement of third party agencies in the energy industry such data management companies, meter installers, network operators, etc. It is crucial that any third parties are appropriately accredited before they can access, store and use personal energy data.

## Lack of meaningful user control

In practice consumers often sign away control of their data, as picking the default option is a typical human characteristic (behavioural economics) and especially in the UK data protection law, implied consent is permitted. Consumer Focus research shows that even when consumers don't mind giving away personal information for certain purposes, such as behavioural advertising, they still like to know what is going on and have control over what goes on. In practice, at present, there is also no easy way for consumers to know what data is held about them; there is also no easy way for consumers to get their data deleted without needing to prove damage of abuse<sup>12</sup>.

## Very poor enforcement of the legislation

The ICO is under-resourced both in powers and resources and not yet well equipped to tackle this issue; it appears to have fewer powers to investigate and enforce the law than its counterparts in other EU countries, although it does now have the power to audit government departments and the levels of its fines have been increased for serious cases<sup>13</sup>.

The UK's DPA does not implement European law properly. There has been criticism from the EU, as far back as 2007, that the UK has failed to fully implement the current EU Data Protection Directive, in roughly a third of its articles, including the powers of the ICO. These relate to, among others, the articles about definitions of personal data, conditions when sensitive data can be processed, fair processing notices given to individuals, rights granted to subjects and ability of individuals to seek a remedy, which have not been properly implemented<sup>14</sup>. The UK Government has not shed light on these claims except to say that they are being investigated.

However the European Commission recently acknowledged this fact with a public call to the UK to strengthen its data protection laws, followed by the recent announcement of the referral to the European Court of Justice<sup>15</sup>. Recent in-depth academic comparative analysis for the Commission confirms these claims.

Government needs to ensure that effective mechanisms are in place to properly monitor activity and that enforcement is effective and provides a suitable deterrent and sanction against bad practice.

---

<sup>11</sup> Eg about 350,000 third party applications are offered through Facebook, which by default have access to user information.

<sup>12</sup> Private Lives, a people's inquiry into personal information, by Peter Bradwell, Demos, with support from Consumer Focus and the Information Commissioner's Office, March 2010.

<sup>13</sup> See in particular the European Commission DG JFS report (note 4 above) Annex 6, United Kingdom Country Study.

<sup>14</sup> The claims were first reported in 2007, following a FOI request to the European Commission, see [www.out-law.com/page-8472](http://www.out-law.com/page-8472).

<sup>15</sup> See <http://bit.ly/de3c2W> and <http://bit.ly/cmlUIJ>.

### Data control, access rights and customer choice (3.8 to 3.18):

- We agree that the key requirement for the programme in respect of data protection is to map out in detail the different data elements, what they are needed for and in what form (eg technical or consumer data), as well as detailed responsibilities and roles regarding access to these data; this would include for example the data access, type of data and handling needs of the contracted supplier, the network, any necessary third parties (eg communications network provider, IHD software provider, etc) (3.9)
- Any assessment should start with the public policy and consumer aims of smart metering, not the commercial drivers, and then consider in each instance:
  - What information is needed to deliver each goal?
  - Does it need to be personal data or can it be aggregated in some way?
  - What detail and frequency of data is required?
  - Can it be stored in the home or must it be exported?
  - Who needs access to the necessary data and why?
- Regarding data grouping and aggregation – given the stated aim of the programme to adopt privacy by design, including minimisation and anonymisation, it follows that data grouping and aggregation should be the norm rather than the exception, whenever possible (see also below and Q2) (3.10)
- The ‘umbrella’ principle that ‘the consumer should choose in which way consumption data shall be used and by whom’ is the right principle to adopt in our view. However the exceptions related to ‘data required to fulfil regulated duties’ will need to be tightly defined, as to our knowledge there is no description of ‘regulated duties’ either in the suppliers’ licence conditions or elsewhere at the moment
- A transparent discussion needs to take place around how “regulated duties” are defined as part of a broad and open consultation as well as what any other smart-related exemptions might be. The duties will need to be listed, comprehensibly, together with the associated data requirements and details about who will require access to this data, and why. Without such tight definitions and listing it won’t be possible to assess whether the principle and the exception have real meaning, since any consumption data, whether it is fulfilling ‘regulated duties’ or not, that can be traced back to an individual or household, is considered as personal data and therefore subject to lawful processing under data protection legislation
- Without detailed guidance for example, “regulated duties” could be interpreted as the mandated duty to install smart meters with time of use (TOU) tariffs seen as part of this given their role in the business case. Such an approach would undermine any privacy protections
- We would expect ‘regulated duties’ to mean little more than the personal data needed to fulfil the contract between supplier and consumer, such as billing and other essential services, or to fulfil the consumer protection obligations. Such duties may also include some specific technical data required to ensure optimum network functioning and delivery of the benefits of smart grids or broader environmental or social purposes
- Consumer Focus is particularly interested in exploring where data sharing could help more effectively target assistance at consumers struggling to afford to keep warm. Smart meters will enable load limiting – the provision of a lifeline of energy as an alternative to disconnection for electricity customers.

Consideration should be given to an obligation on suppliers to monitor and provide help to PPM customers who are no longer topping up or are relying on this trickle flow of electricity as they may be in financial difficulty.

In Tasmania, for example, suppliers are required to contact customers who self-disconnect three or more times for at least 240 minutes on each occasion, in a three month period. They have to offer these customers advice on alternative payment options, provide advice on government assistance schemes, and (where the customer has consented) make referrals to the scheme<sup>16</sup>

- Careful consideration will need to be given to the use of data for security purposes. While we recognise there are benefits to sharing data to identify and tackle illicit activities eg energy theft, we have real concerns that access to information could be misused. There needs to be an open public debate around what information can be used for police or Government surveillance purposes

### Customer choice and control

- Consumer Focus has concerns that at present energy suppliers abide by the letter of privacy law by listing their privacy policy, and purposes for which they collect the data in their contracts and terms and conditions, but don't give consumers any kind of choice in what data they share or any kind of opt-out. Consumers only have a choice in as much as they can decide not to sign a contract. But as far as we understand it no supplier's contract gives the customer the choice to opt-out of sharing half hourly data. This effectively means that they have no choice if they want to have access to the essential service of energy supply
- It is not clear how the proposed principle with its exception will make a substantive difference to the status quo, except when it comes to access by third parties or providers of extra services (3.11)
- We think that the discussion regarding opt-in and opt-out (3.15) is premature until the 'regulated duties' and the framework are more clearly defined, at which stage an informed and constructive discussion can take place on how to ensure consumers exercise a meaningful and informed choice

### Enforcement

- We strongly support in principle the view that smart meter specific data privacy requirements should be included in a licence obligation, as this could provide a stronger and more effective tool than a set of detailed guidelines on their own. As we understand it, while existing licence obligations are only on the supplier, suppliers are ultimately responsible for the activities of third parties they have employed eg metering agents. This approach could therefore help address identified specific gaps in the DPA, for example with regards to third parties as well as existing identified gaps in standards for example for data handling.<sup>17</sup> Certainly there will need to be strong rules and governance around the DataCommsCo (DCC)

---

<sup>16</sup> <http://bit.ly/bCyV8T> Cited in Smart Prepay in Great Britain. March 2010. P.21 Sustainability First. Gill Owen and Judith Ward. This research was part-funded by Consumer Focus. <http://bit.ly/dzwEeM>

<sup>17</sup> The EU Task Force Smart Grids, Expert Group 2 identifies a clear gap within EU standards relating to company data handling for smart meters/grids although there are handling guidelines for many other industries such as banking and payment cards, etc. Internal systems for processing/handling of data are not mentioned in this document, and they're part of the privacy by design principle. The Expert Group proposes a list of high level principles for data handling on EU level which can be used by industry to design their systems and processes.

## **Question 2: 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?**

As stated above, Consumer Focus does not think that it is possible to have an informed opinion on these issues until 'regulated duties' which relate to personal information collection and processing are clearly defined and a privacy/security framework mapped out. Broad consultation is needed as a matter of urgency.

The programme should learn from the Dutch experience for example, where such a framework has been created, via a number of logical steps, starting with an overview of all relevant stakeholders and their demands and expectations re smart meters; official rules and regulations (ie regulated duties); norms and standards; risk analysis; considerations and choices, etc. Without such a properly evidenced and transparent mapping or framework, the industry will no doubt claim the need for as much and as detailed personal information as possible. Meanwhile consumer and privacy advocates will demonstrate that most needs can be fulfilled through aggregation or consent driven consumer research, including the need for the Government to monitor its policies and build statistics. This includes being able to manage the grid and ensure security of supply. What is deemed to be 'regulated duties' will need to stem from a clear understanding of the aims of mandating smart meter rollout. Any other approach, we feel, is putting the cart before the horse in terms of decision making.

In the meantime and until this information is mapped out, the policy baseline in terms of data access frequency should be the current status quo, ie readings for billing purposes. Customers should not have to share any more data than they do now with their existing 'dumb' meters until appropriate protections are in place. Customers participating in time of use or other smart meter trials should be made aware of the privacy implications of their participation prior to commencement of the trial. The case should be made to them by the supplier so they can make an informed decision on whether to consent to opt-in to sharing additional data.

## **Question 3: Do you support the proposal to develop a privacy charter?**

A customer facing charter could be a useful additional communication tool to inform consumers of their privacy rights and the responsibilities of their energy supplier. Its effectiveness however depends on how it is done, what it contains and how it is promoted. We have seen many such charters (including privacy ones) developed by industry which have had little impact and been used mainly as a public relations tool. If a charter is developed it must be part of a wider communications campaign to raise consumer awareness of their rights in this area, the implications of sharing personal data and signing up to particular deals. It should be industry-wide and included within all suppliers smart meter packs and have a high level of cross-supplier standardisation.

## **Question 4: What issues should be covered in a privacy charter?**

A privacy charter should be written in simple and direct language and contain the consumer rights in respect to metering and their energy consumption including:

- **Consent:**  
Consumer consent must be actively sought for the collection and use of their data – contract default setting is 'opt-in' to share more. Customers should opt-in to sharing any more data than that which is needed for 'regulated duties' or agreed broader environmental or social purposes (official exemptions).

If technological developments enable access to greater amounts of data in the future, consent should be sought again before any party accesses this. It should include a description of the potential benefits, risks and consequences of disclosing detailed energy consumption information to various parties

- **Notice:**  
Consumers should be given high level notice of how energy information is collected, used, stored and by whom. Customers should be made aware of their rights and what they are obliged to give out and for what purposes
- **Access:**  
Customers should be able to access at least a full year of their own historic consumption information for free via their in home display. They should be able to have timely access their historic energy usage information via alternative media eg via the internet, hard copy or telephone, also for free. All data should be in a format that allows like for like comparisons with other deals available in the market. This is essential to ensure that customers can make informed switching decisions. Consumers should also be informed as to how they can find out in more detail exactly who is accessing their data and for what purpose. Third parties seeking access to data eg switching sites, should be accredited
- **Enforcement and complaints:**  
Customers should be made aware of the complaint handling and redress procedures and their rights in this regard. This should include contact details about where they can go in case of a breach and how enforcement will be monitored. It should include a freephone help line (free from mobiles as well as landlines), and email contact as well as mail

There must be reference to clear and precise privacy policies and where they can be easily found.

### **Question 5: Do you agree with our approach for ensuring the end-to-end smart metering system is appropriately secure?**

In principle yes, though we do not have in-depth technical expertise on security issues:

- We welcome the approach of security by design and the commitment to a full risk assessment looking at the end to end system – IO Active reports that substantial numbers of existing smart meters on the market have poor authentication, lack of encryption and inadequate authentication processes making them accessible to hacking. These experts suggest that addressing security concerns once devices are installed would be cost prohibitive. We therefore urge decision makers to get this right before rollout and that decisions around DCC and meter design, functionality, operation, management and technology are taken following key decisions on security.

IO Active's worm simulation demonstrated that it was possible to hack into and take control of more than 15,000 smart meters out of 22,000 in just 24 hours<sup>18</sup>. The speed of attack could only be halted by disabling entire energy supplies with a resultant instability on the grid. The impact of this on consumers, in terms of inconvenience, cost, and potential danger to health for those who rely on their energy supply, are very significant

- We note and welcome that the programme is consulting with the key players in security and industry sectors and appreciate that engagement on this issue will need to be subject to appropriate controls given the national security implications.

---

<sup>18</sup> *Securing the Smart Grid. To Act without Delay* IO Active.  
<http://bit.ly/aZ7KgQ> . Also <http://bit.ly/bfV7cB>

Major internet service provider and/or big software companies could also be consulted as the security risks they have to tackle can be parallel, particularly on the software side. Academics may also add value.

A recent paper by the Cambridge University Computer Laboratory deals with the security issue of smart meters in depth, providing a number of possible technical solutions used in other fields<sup>19</sup>. We also support monitoring of developments at an EU level and urge cross European and international liaison in this regard

- We urge Ofgem to develop a security governance framework that considers not just the implementation of smart metering in the next few years but will carry out ongoing monitoring and enforcement against risks as technology develops
- We support an independent review of the standards of existing technology, especially that which is already installed, and the setting of minimum standards for smart grid products and any related devices, whether by the European Standards Organisation (ESO) or another body to ensure that they have the appropriate levels of security
- Consumer Focus warns against industry complacency. The recent problems experienced by the energy industry with regard to electricity PPMs, where it has been discovered that fraudulent keys capable of loading credit onto the meter and wiping the existing data held on the meter, have already affected over 100,000 households and show the vital need to ensure meters can be made safe from criminal activity. Consumer Focus feels that had organisations been more vigilant and mindful of security issues, fraudulent activity would have been less likely to have spread throughout the country before it was noticed by suppliers. Lessons must be learnt from this
- There will need to be clear roles and responsibilities around data security and privacy and strong enforcement mechanisms for failure to deliver the appropriate standards or service
- We seek reassurances from DECC and Ofgem that security issues will be resolved before wide spread rollout of smart meters with remote disconnection functionality and active wide area networks. All technology and systems must be appropriately tested before they are introduced into people's homes

## Further issues: wider smart-related data sharing

Consumer Focus supports an enhanced home visit service for low income and vulnerable consumers. Sharing of Department of Work and Pensions data such as benefits information could help identify householders who are vulnerable and on low incomes. This could be used, as has been done with the Digital Switchover campaign, to target an enhanced installation service at customers potentially in need of additional assistance and could help maximise take-up and targeting of the priority services register benefits or the new suppliers obligation as part of the Green Deal. This may require legislative change, which perhaps could be facilitated by an amendment to the upcoming Welfare Reform Bill or Energy Bills.

---

<sup>19</sup> *Who controls the off switch?* Ross Anderson and Shailendra Fuloria, Computer Laboratory, Cambridge University, <http://bit.ly/9MNNqc>

# Consumer Focus summary of recommendations/views:

---

1. We support the principle of **privacy by design and security**, including data minimisation and anonymisation. This principle should be applied both to processes and in-built technology and include robust testing.
2. We support the **meter being the primary depository** for historical energy consumption.
3. We support the right that consumers own and have access to their own data – in order for this to be effective the definition of '**regulated duties**' must be clearly defined, along with any exemptions to existing data privacy legislation. Also further discussion is needed around **consent** mechanisms. Consumer Focus believes that customers should not have to share any more information than at present with 'standard meters' until protections are in place.
4. At the earliest opportunity there should be **broader and open stakeholder consultation**, including: a) the Privacy and Security Advisory Group should be expanded to include a wider range of external stakeholders, and/or b) a task force or working group should be set up, on the model and with a remit similar to the EU Task Force Smart Grids Expert Group on data privacy and security.
5. Privacy and security obligations should be outlined in **specific licence conditions** in order to address weaknesses in existing privacy legislation. Until protections are put in place customers should not have to share any more data than they do currently with their 'dumb meters'.
6. Detailed **guidelines should be developed** and issued to underpin obligations outlined in licence conditions. The duties will need to be listed, comprehensively, together with the associated data requirements and who will require access to this data, and why.
7. We welcome the proposal to carry out a **privacy impact assessment (IA)** on all aspects of smart meters and grids. Such assessments have been carried out in the US, eg by the Cyber Security Co-ordination Task Group and have revealed a number of serious concerns, particularly related to consumer to supplier information exchanges.
8. There should be an independent **internal audit of supplier's security and privacy** processes to evaluate risks around their practices.
9. A **strategy for monitoring and enforcement** of these rules needs to be developed including resourcing and **complaint handling and redress**. Consideration needs to be given to unlimited fines for a breach, mandatory notification of breaches, compulsory audit and inspection, annual reporting etc.
10. Development of a clear and co-ordinated strategy for **consumer education** so that consumers are aware of their rights and know how to complain and seek redress.

11. **Consumer representation** in any governance structure surrounding the central communications provider.
12. **Limit the numbers** of smart meters installed until data privacy and security protections are in place.
13. A **plan and timetable** to deliver the above action on behalf of consumers.

# Annex 1: Our privacy concerns

---

## Customer attitudes

It is often assumed that with so much of our lives conducted online and in public spheres that social norms have changed and consumers care less about privacy. But Consumer Focus's research and wider evidence outlines a more complex picture:

- *Private lives: a people's inquiry into personal information*<sup>20</sup>, found that people have various degrees of tolerance toward data sharing depending on the area in question (so health was the most important in terms of safeguarding privacy). However, even when they are relatively tolerant, as in the case of targeted marketing, they absolutely want to know and understand what is going on, so transparency is essential; and they want to exercise control over whether or not their data is shared or collected or not. They also want to be able to change their minds according to circumstances. They are always aware that there might be people more vulnerable than them, such as children or the elderly. Key recommendations from consumers are that there is transparency and ability of authorities to take control, monitor and regulate. There was a lot of cynicism regarding private companies' motivation, but more cautious trust in the motives behind public authorities' actions
- The ICO's own annual tracking report on individual attitudes and awareness of data protection (2009) shows an overwhelming majority of respondents are concerned about how their personal information is handled (93 per cent of respondents are concerned about protection people's information – up 23 per cent since 2004)<sup>21</sup>
- The public is also showing high levels of concern about potential mismanagement of their own information, with the two highest concerns being passing or selling personal details to other organisations (97 per cent) and security (96 per cent)
- Furthermore evidence from other sectors shows that consumers' concerns over safety of personal data may undermine their confidence to engage in the use of new technologies, such as e-commerce or online public services. There is no reason to suggest attitudes towards engagement with smart metering will not be the same<sup>22</sup>
- Navetas's Smart Meter research (May 2010) found that 49 per cent of consumers were happy to share information on appliance consumption with their energy provider, 10 per cent with other companies, with 39 per cent saying that they would rather their information be kept within their home<sup>23</sup>

---

<sup>20</sup> Demos research, supported by Consumer Focus and the ICO examined, through ground-breaking deliberative research methodology over several weeks, people's attitudes to information privacy linked to communication data, targeted advertising and health records. Participants learned first about the issues in depth from experts (including industry), and then discussed, came to conclusions and made recommendations.

<sup>21</sup> ICO Annual Track 2009. 4.1 and 4.2

<sup>22</sup> See for eg Office of Fair Trading recent study of e-commerce that confirms some of these concerns <http://bit.ly/aaeRZz>.

<sup>23</sup> Navetas Smart Meter Evaluation. Prepared by Optimisa Research, May 2010

## Overview of consumer issues

The GB energy industry already processes large amounts of metering data on a daily basis. There are numerous complex and substantial data flows and collection procedures which are used to manage the millions of domestic gas and electricity accounts. But smart metering is likely to result in:

- Massive increase in volumes of data, collected, analysed and stored – in the words of one data management company – ‘there will be a tsunami of new data’
- Increase in sensitive and personal nature of data
- Easier access and transmission of data
- New participants wanting access to/or to hold smart meter data eg switching sites, energy services companies, bodies responsible for carbon reduction etc

The adoption of a DCC provider model brings forward considerable challenges to ensuring individual information privacy and data protection. As the smart metering/grid technology is essentially a customised network based on the internet protocol, the privacy risks and issues that apply are similar to those evidenced for the online digital environment. Lessons should be drawn from other sectors. In addition there are certain notable features that add an additional risk:

- The sensitive and personal nature of the data collected can potentially be far greater, and have far greater impact, than anything that can be revealed even on the most open of the social networks
- Unlike in other sectors, in practice consumers are unlikely to have a choice on whether to have a smart meter in their home. If they want an energy supply they will have to accept the terms and conditions offered to them. The basic terms and condition and minimum data access must be considered carefully
- Although decisions around the Data Collection Company (DCC) have yet to be finalised, its broadly assigned role is likely to involve handling and storage of large amounts of consumer data on some form of central database. In addition energy companies will also have to keep their own customer databases to enable customer services and billing. Problems in terms of privacy, data protection and data sharing for such databases, both in the public and private sector, have been widely evidenced and reported, both in terms of data leaks and breaches, and in terms of third party access or their conformity with data protection and human rights legislation
- The structure of any central data communications body, governance and access to information also has implications for competition in the energy, communications and other sectors – potentially impacting negatively on consumer choice and price of services

7.4 The aims, the technology and the model considered together mean that a great new number of participants will want access to the data for various purposes, sometimes conflicting. As the Government itself acknowledges in its IA of May 2009, this brings forward additional and considerable implications in terms of transparency, legality, oversight, consumer acceptance and dispute resolution or redress.

## Key issues

1. **Threat to personal privacy** – smart meters make it possible to monitor consumers' energy consumption on a minute by minute, half hour, day or week and potentially the precise appliances that they are using at any given time. This raises significant privacy issues as it potentially gives a detailed insight into activities within the most private of places, people's own homes. One analyst at the Centre for Energy and Environmental Security in the US reportedly referred to smart metering and smart grids as '*inadvertently raising a monster with unparalleled abilities to invade personal privacy*'.
2. **Energy data processing could give an insight into:**
  - a) **Patterns of living** – when someone gets up, goes to bed, eats etc
  - b) **Occupation of premises** – whether someone is at home or away
  - c) **Make up of household** – eg could know if there is a baby in the household if they know that they use a baby monitor
  - d) **Technical appliances in the home** – what you use and don't use, how many you have. Also the life cycle of your appliances, how old are they, might you be due for a new kettle, appreciate a TV with extra functions?
  - e) **Conduct on the basis of appliances** – how someone lives their life on the basis of their appliances eg use of sun beds, dialysis machines, TV watching. This could have insurance implications
  - f) **Security** – whether you have an in-home security system, when you are likely to be out of your home

**Key questions to ask:** *What kind of data should be collected by the smart meter and for exactly what purpose? Who owns this data? What data needs to be exported out of the meter, to whom and for what purposes? How long it is to be stored and by whom? What should be the frequency of the meter readings (every quarter hour? once per day? once per week?) And what is rationale for the chosen frequency? Who should have legitimate access to this data and for what purposes: Energy companies? Energy conservation organisations? Security companies? The police? What are the implications of this potentially very detailed information – could consumers be penalised for excessive energy use or the information used for any future carbon rationing for example? Would divorce lawyers be able to comb through meter records to see who was in the hot tub when an aggrieved husband/wife was away on business?*

### 3. Security of personal data

Data storage and collection is:

- a) **Vulnerable to commercial interest** – eg companies could target you with marketing about appliances you don't possess, or old appliances you might be willing to upgrade
- b) **Vulnerable to criminal interest** – there is a growing instance of identify fraud resulting from remote services. There are also concerns that information about energy use, if it falls into the wrong hands could be misused. Burglars could tell if you were in or out of the house, or on holiday

- c) **Vulnerable to police interest** – under what circumstances will the police be able to monitor your smart information?

**Key question:** *What are the risks? Where can the threats come from? Eg external parties, inside the energy or telecommunications industry? What measures should be put in place, both technical and in terms of systems and processes to ensure security of energy-related data in private homes? Who is responsible for the security of the data, and what are the sanctions for breach? What are the ongoing governance structures?*

4. **Transmission of data** – our energy suppliers/distributors are global companies, and may wish for economic and other efficiency reasons to store data in another out-of-EU jurisdiction (for eg if they have out-of-EU server facilities) or to use a third party to process and store data in a different location.

**Key question:** *How do we ensure, and what guarantees will be put in place that countries where UK consumer energy data may be exported have adequate levels of privacy rights protection?*

5. **Consumer profiling** – smart meters could result in increased consumer profiling with negative effects. For example, detailed information about consumers' lifestyles could result in higher insurance premiums. Stigmatisation and discrimination of low income consumers is a real concern which could lead to discriminatory behaviour or reduction of choice for certain types of consumers. Already we are hearing anecdotally that some suppliers have considered whether smart meters could facilitate those with poor credit records being charged tariffs that reflect their debt risk. Regulation allows for cost reflective pricing in this way.

**Key question:** *How can we protect vulnerable and low income consumers? How can we use the opportunities created by smart metering and grids to improve the delivery of assistance and customer service to low income and vulnerable households?*

6. **Targeted marketing and unwanted sales** – detailed data collected by the meters is a potential treasure trove for marketing companies, even more so than following their behaviour on the internet. Consumers are concerned about commercial use of personal data carried out without their awareness or consent. Messages could also be transmitted to customers via their energy display into the most private of places, their own home.

**Key question:** *How do we ensure that people are not victims of unwanted targeting, profiling and marketing activity particularly if displays are able to receive incoming messages?*

7. **Remote management of appliances** – It is likely that in the future an external party – distributor or national grid will be able to control appliances within consumer's homes. This may be needed to help balance the grid as we use an increasing amount of renewable and low carbon energy. Eg turn off our fridge temporarily, reduce heating on a swimming pool.

**Key question:** *Should this be permitted and if so, under what conditions? What should be the hierarchy of control? How do you prevent unauthorised use?*



## Smart Metering Implementation programme

For further information on this submission, please contact Zoe McLeod  
Principal Policy Advocate on 020 7799 7973 or email [zoe.mcleod@consumerfocus.org.uk](mailto:zoe.mcleod@consumerfocus.org.uk)

[www.consumerfocus.org.uk](http://www.consumerfocus.org.uk)

Copyright: Consumer Focus

Published: October 2010

If you require this publication in Braille, large print or on audio CD please contact us.

For the deaf, hard of hearing or speech impaired, contact Consumer Focus via Text  
Relay:

From a textphone, call 18001 020 7799 7900

From a telephone, call 18002 020 7799 7900

## Consumer Focus

4th Floor  
Artillery House  
Artillery Row  
London SW1P 1RT

Tel: 020 7799 7900

Fax: 020 7799 7901

Media Team: 020 7799 8004 / 8005 / 8006