International Review of Law, Computers & Technology, 2014
Vol. 28, No. 2, 172–184, http://dx.doi.org/10.1080/13600869.2013.801580

Routledge
Taylor & Francis Group

Britain's smart meter programme: A case study in privacy by design

Ian Brown*

Oxford Internet Institute, University of Oxford, UK

(*Received 18 March 2013*)

Following requirements in the 1996 EU Energy Efficiency Directive, member states are developing programmes to encourage the installation of 'smart' power meters that record much larger quantities of data about power usage than traditional meters. These data can reveal a great deal of information about individual household activity, leading privacy regulators to call for privacy to be 'designed in' to these systems. The British smart metering programme has given some attention to this privacy by design process. This article assesses its effectiveness in this case, using documentary analysis, participant observation, and follow-up interviews with a range of stakeholders. It finds that decisions made early in the British programme had negative privacy impacts that have only been partially remedied by the later development of detailed rules on the processing of smart meter data by energy suppliers and distributors. The article also considers broader lessons for the privacy by design approach.

Keywords: data protection; technology regulation; energy efficiency

Introduction

Smart meters are an important element in government and industry plans to improve the efficiency of energy grids, enable better use of highly variable renewable energy sources, and help consumers to reduce their energy consumption and find more competitive suppliers. They can also be used to investigate fraud and remotely disconnect delinquent customers.

Compared with traditional meters that provide a relatively infrequent reading of total energy used, smart meters allow much more detailed data to be recorded about the energy consumption of individual homes, and shared automatically at varying intervals with energy suppliers, grid operators, and price comparison websites. The energy industry has suggested that this will better allow suppliers to forecast demand, and shape consumer behaviour through time-of-day tariffs and remote instructions to appliances to reduce consumption.

Because of potential cost and energy savings, many governments have legislated to encourage or mandate the large-scale installation of smart meters. The European Union agreed the Energy Efficiency Directive[1] in 2006. Article 13 contains specific requirements for member states to encourage the use of smart electricity, gas, heating, cooling and hot water meters:

> 1. Member States shall ensure that, in so far as it is technically possible, financially reasonable and proportionate in relation to the potential energy savings, final customers for electricity,

*Email: ian.brown@oii.ox.ac.uk

> natural gas, district heating and/or cooling and domestic hot water are provided with competitively priced individual meters that accurately reflect the final customer's actual energy consumption and that provide information on actual time of use.
>
> When an existing meter is replaced, such competitively priced individual meters shall always be provided, unless this is technically impossible or not cost-effective in relation to the estimated potential savings in the long term. When a new connection is made in a new building or a building undergoes major renovations, as set out in Directive 2002/91/EC, such competitively priced individual meters shall always be provided.

An updated Energy Efficiency Directive, which must be transposed by member states before 5 June 2014, includes a more detailed version of this requirement, adding that states 'shall ensure the security of the smart meters and data communication, and the privacy of final customers, in compliance with relevant Union data protection and privacy legislation'. The Directive also requires that 'if final customers request it, metering data on their electricity input and off-take is made available to them or to a third party acting on behalf of the final customer in an easily understandable format that they can use to compare deals on a like-for-like basis'.[2]

In 2009, the Electricity Directive[3] added a requirement that 80% of consumers have smart meters by 2020, subject to a positive cost-benefit analysis for markets and consumers. The Natural Gas Directive[4] requires states to assess 'all the long-term costs and benefits to the market and the individual consumer or which form of intelligent metering is economically reasonable and cost-effective and which timeframe is feasible for their distribution' and subject to that assessment, prepare a timetable for smart gas meter implementation.

Because smart meters can collect and share detailed information about energy use and hence household life, their impact on privacy has become a high-profile matter of interest to energy and privacy regulators, and to privacy campaigners, journalists, and members of the public. In one significant case, the First Chamber of the Dutch parliament rejected two smart metering bills in 2009 because of privacy concerns, forcing the government to add significant privacy protections to revised bills that were passed in 2011.[5]

This article describes the process of implementation of the EU energy directives in Great Britain (England, Scotland and Wales – Northern Ireland has its own Utility Regulator and policies), analysing the evolution of government plans to meet the requirements of European privacy law. One of the main objectives of the British programme was to provide more accurate bills to consumers, which is one specific part of the Energy Efficiency Directive and also a key requirement of the Data Protection Directive ('personal data must be… accurate and, where necessary, kept up to date').[6] In particular, it compares this process with the 'privacy by design' approach that is strongly recommended by European data protection regulators, and made mandatory by the European Commission's proposed Data Protection Regulation.[7] It also compares the British approach to that of the Dutch and German governments, the two EU member states that have had the broadest-ranging public debates over the privacy impact of smart meters.

Data protection and human rights compatibility

Traditional energy meters were not seen to have privacy implications, as the aggregate quarterly energy consumption reading usually collected by suppliers for billing purposes reveals a limited amount of information about customers. Officials and industry experts with the greatest influence on energy policy therefore had little experience with the impact of new technology on privacy.

However, researchers have gradually developed an understanding of the information that can be derived about individuals' day-to-day lives from frequent remote readings of the amount of power consumed at an individual residence, down to the level of minute-by-minute voltage fluctuations. Table 1 shows some examples of some highly sensitive questions that could be answered about an individual using smart meter data.

Requirements of the Data Protection Directive

The main EU law regulating the use of data about individuals is the Data Protection Directive[8] (DPD). The Article 29 Working Party of European data protection authorities confirmed in a 2011 Opinion that smart meters process personal data and that the provisions of the DPD therefore apply.[9] Meter data are associated with a unique identification number linked to an individual associated with the account, used to take decisions directly affecting that individual, and are collected to profile user behaviour for the purpose of reducing energy consumption.

The DPD places a number of responsibilities on 'data controllers' who make decisions about how personal data are processed. For smart meters, this is likely to be the energy supplier or network operator, depending on who installed the meter and collects the data. Communications networks for meters, energy regulators, and third-party service providers may all also assume the role of a data controller. The Opinion emphasised that 'the increased

Table 1. Information revealed by smart meters. Based on Quinn (2009, 30–1).

When are you usually away from home?	Is your household protected with an electronic alarm system? If so, how often do you arm it?
How often do you arrive home around the time the bars close?	How often do you get a full night's sleep v. drive sleep deprived?
How often are you late to work, or rushing to get there on time?	Does the time it takes you to get from your home to your workplace require that you break the speed limit to get there?
On what days and during what times do you watch TV?	How much home time do you spend in front of your computer?
How often do you eat in?	Do you tend to eat hot or cold breakfasts?
What's the relative frequency of microwave dinners to three-pot feasts?	How often do you entertain?
Are any of your appliances failing or operating below optimal efficiency?	Do you own lots of gadgets?
Are you a Laundromat person, or do you have your own washer and drier?	Are you a restless sleeper, getting up frequently throughout the night?
In a custody battle: Have you ever left your child home alone? How often, and for how long?	In a worker's compensation hearing: How is it, with your disabled back, you were able to turn on the TV in the upstairs of your home less than a minute after turning off the lights downstairs?
Alabama recently passed a tax provision requiring obese state employees to pay for their health insurance unless they actively work to reduce their body mass index. So: why haven't you used your treadmill at home any time in the last week? You clearly have not been out of the house and away from a computer or TV long enough for aerobic exercise.	Do clinically depressed or bipolar individuals have distinctive energy profiles? What about people with behavioural disorders? Could you tell if someone hadn't been taking his or her medication?

amount of personal data being processed, the possibility of remote management of connection and the likelihood of energy profiling based on the detailed meter readings make it imperative that proper consideration is given to individuals' fundamental rights to privacy.'[10]

Controllers must have a legitimate basis on which to process personal data. The most commonly used is informed consent from the data subject. Consent must be granular, not a blanket agreement to several divergent or unrelated purposes, and capable of being revoked. Data processing required for the performance of a contract is permissible, but this will often not be the case for detailed smart meter data – for example, a tariff based on total energy usage will not require the processing of detailed hour-by-hour consumption data for billing purposes.

A legal obligation created by EU member states implementing the Energy Efficiency Directive can legitimise processing, as can the public interest and legitimate interests of energy companies in reducing energy consumption. However, energy companies relying on this basis must properly weigh the interests and rights of data subjects. The Article 29 Working Party suggested this would not permit 'the creation of detailed profiles of data subjects that are, in fact, not needed to achieve the purpose, passing details to third parties without the knowledge or consent of the data subject, or the use of personal data to take decisions about remote disconnection without proper regard for an individual's data protection and other rights'.[11]

The European Data Protection Supervisor has suggested that the Electricity and Natural Gas Directives are not specific enough to be considered as a 'legal obligation', and that a clear distinction must be made between objectives that allow processing in the public or other legitimate interests without consent, and those where consent is required. This should be freely given, specific, informed and explicit.[12]

Requirements of the European Convention on Human Rights Article 8

European states must also consider the requirements of the European Convention on Human Rights (ECHR). Article 8 of the Convention provides that 'Everyone has the right to respect for his private and family life, his home and his correspondence.' This is a qualified right, but exceptions must be 'in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Smart meters can clearly record data, revealing patterns about 'private and family life', and individual activity and presence or absence at home. Without effective security controls, functionality such as remote disabling of devices could also enable further invasion of home life.[13]

Member States' implementation of the Energy Efficiency Directive provides a legal basis for this interference with private life and the home. The Directive is introduced under Article 175 of the EC Treaty, meaning that it sets a minimum standard for harmonisation but that member states may go further for the purposes of a high level of environmental protection – so long as such measures are compatible with the Treaty and notified to the European Commission.[14]

Member States have justified privacy interference from smart meters as being in the interests of the 'economic well-being of the country'. Quantification of increased energy efficiency from different types of smart meter configuration and programmes would strengthen this justification. There have been significant questions raised about the costs

and benefits of the British programme, with a review for the government concluding that the scheme's 'ever-increasing complexity' was likely to lead to an 'IT disaster'.[15]

The third requirement of the Convention is that interferences with privacy are 'necessary in a democratic society'. The European Court of Human Rights has defined necessity as 'an urgent social need' where 'the measure is relevant to achieving the aim', 'does not extend further than necessary and is reasonably in proportion to the aim.'[16]

Reducing carbon-intensive energy consumption is clearly an urgent social need, but different types of smart meters and their respective impact on privacy need to be considered to decide what is proportionate for governments to mandate. This makes the concept of 'privacy by design' particularly relevant.

Privacy by design

Privacy regulators in Canada, the US and the EU have become increasingly vocal in calling for privacy to be 'designed-in' to new products and services, rather than added as an afterthought following consumer complaints and regulatory action. This is particularly important in basic infrastructure (such as energy grids and smart meters), which is likely to be extremely expensive to replace (although remote software updates may be able to be applied to some elements). Designed-in privacy is likely to be much more effective if included throughout the product or policy design lifecycle, as a much broader range of options is available to a designer than to an engineer trying to make changes to a product following a privacy incident.[17]

A 'privacy by design' requirement is implied by Data Protection Directive article 17, which requires data controllers to 'implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access'. It is made explicit by the proposed Data Protection Regulation article 23, which requires that controllers implement measures to ensure 'only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage.'

Smart meter designers (and policymakers) considering privacy impact must start by asking some basic questions. What kind of data will the meter collect, under a range of different circumstances? Who has access to that data, for which purposes? Which data will be collected and protected using contractual provisions rather than technical measures? How will consent be gained from consumers, beyond the customer agreement signed at installation, and can it be revoked using meter functionality? How long will data be stored on the meter and at third parties, and what security measures will be in place to protect that data against unauthorised access? What barriers are in place to prevent information collected for one purpose being used for another, without the informed consent of the customer?[18]

Ontario's Information and Privacy Commissioner has suggested a number of principles for making privacy the default 'in all physical, administrative and technological aspects' of smart grids. This would involve the collection of the minimum personal data necessary without reducing the services offered, with options transparently communicated and suitable for a wide range of consumer preferences. Data quality would be assured, while the system was built to be resilient to failures such as data leakage and breaches. This could include measures such as aggregating and reducing the specificity of data before it is provided to third parties for services such as comparisons of neighbourhood averages.[19] The

Article 29 Working Party has added that the use of such an approach makes the 'legitimate interests' justification for data processing under Article 7(f) DPD more plausible.[20]

Sometimes, basic product design decisions can have very significant privacy impacts. For example, a smart meter that displays energy consumption data on an in-home display may provide many of the environmental and consumer benefits with significantly lower privacy risk than sharing detailed consumption data with suppliers and price comparison websites – and would equally satisfy the requirements of the Energy Efficiency Directive.[21]

More sophisticated techniques can be used to provide additional functionality without requiring any further personal data to be shared between smart meters, network operators and energy suppliers. For example, Rial and Danezis described a system that allows time-dependent and other complex tariffs to be applied in a provably correct way without a meter supplying any information to a supplier beyond the total cost incurred. Other privacy-friendly calculations can be performed 'to support forecasting, profiling, settlement, or fraud detection.'[22] Kursawe, Danezis and Kohlweiss extended this system to enable aggregate measurements to be privately computed from multiple meters to allow fraud and leakage detection and network management.[23]

Rubinstein and Good noted that privacy protection can be implemented at both the infrastructural level – 'behind the scenes' at servers that gather and process large quantities of data – and at the user interface that allows individuals to customise software and hardware systems. Infrastructural privacy protection measures are likely to be focused on minimising the quantity of personal data gathered. User interface privacy measures are usually concerned with notifying users of and allowing them to configure personal data collection and use; showing which data has been stored; and allowing the correction of errors.[24] These measures correspond closely to the Data Protection Directive's requirements for data minimisation, notification and consent, and data accuracy.

In the case of smart metering, the focus of privacy regulators will initially be on the overall system design and infrastructural protections, which will later have implications for how much data smart meters must or may collect and share outside residential customers' homes. In assessing the usefulness of the privacy by design framework in the privacy compliance of Britain's emerging smart grid infrastructure, therefore, the key question is: how and why were decisions made by legislators and regulators on the amount of personal data processed outside the direct control of the individual energy consumer?

How personal data processing and access rules evolved

This section describes how far the British smart meter programme did and could have taken account of privacy by design principles, particularly of data minimisation. It is based on document analysis, participant observation, and follow-up semi-structured interviews with six academic experts, civil society campaigners and technologists involved in the programme. All had extensive technical, consumer protection or legal backgrounds. Their views are reported here anonymously to allow commercially and politically sensitive subjects to be discussed.

Initial privacy assessments

A key requirement of privacy by design is that privacy options are considered as early as possible in the development of policies and technologies. However, little attention was paid to privacy in the early phases of Britain's smart metering programme. An initial

227-page assessment of options in 2007 failed to mention 'privacy', and noted only: 'a negative for smart metering is the intrusion that some consumers have said they would feel from having their detailed energy consumption patterns logged and accessible to suppliers. It is unclear how widespread this concern is, and whether it can be easily resolved through recourse to the data protection rules.'[25]

Two years later, a 40-page consultation document from the responsible government Department of Energy and Climate Change (DECC) made one mention of privacy:

> Data access and data protection will be central to the issues to be considered under the preparation programme. Clearly the right level of data access within the industry will be important for the full benefits of smart metering for consumers and ultimately for smart grid management are to be realised. Equally, the right safeguards must be in place to protect consumers from improper access and misuse of data. Among other things, Privacy Impact assessments and Data Protection Act Compliance Checks will be required at appropriate stages of the project, and the detailed design and delivery of the project as a whole will be taken forward in conjunction with the Ministry of Justice and the Information Commissioner as appropriate.[26]

By this stage, DECC had already made a decision – subject to responses to the consultation – to appoint 'a single national communications provider … to provide communications services for all smart meters.' While such a provider could enforce constraints on the flow of data from meters to networks and suppliers, it would also provide a convenient central point at which other interested parties, such as law enforcement agencies, could access meter data given legislative authority.[27]

Following pressure from the statutory consumer group Consumer Focus, DECC started to pay more attention to privacy issues, but took some time even to appoint two (non-specialist) civil servants to work on the issue. Little input was sought at this stage from the Information Commissioner's Office (the independent data protection regulator), and the negative reaction of the Dutch media and parliament to that country's smart meter programme seemed to be the most significant factor behind DECC's attention.

Beginning in January 2010, DECC held three workshops on privacy and data use, although some officials were nervous about providing privacy groups with 'ammunition on something they were blissfully unaware of.'[28] These workshops were the first time that civil society and academic experts were invited to meetings with officials and industry actors. Consumer Focus held their own workshop in June 2010, bringing into the process further stakeholders, particularly a representative of the Dutch consumer organisation Consumentenbond to talk about opposition to Dutch legislation. DECC also formed a Privacy and Security Advisory Group, made up of government officials, the Information Commissioner's Office, suppliers, and Consumer Focus.

Even at this stage, some energy industry representatives took the position that smart meter data was not personal data, and that it belonged entirely to industry actors, to process as they saw fit. Energy suppliers pushed DECC for default access to half-hourly readings. When asked to justify this, one large supplier estimated that £1 billion could be saved annually through better matching of predictions of consumer demand with bids made on Britain's energy spot market.

At the same time, Consumer Focus used its statutory powers to request information from providers that were already conducting smart meter trials. The results showed that most providers were collecting half-hourly data without informing consumers. After Consumer Focus wrote letters of complaint, providers started putting customer information notices onto their websites.

Legislation and standards-setting

DECC then began consultations on the detailed standards and legislation that would be needed to give effect to the government's smart metering programme. The programme's prospectus, published in July 2010, included more information on data security and privacy, setting out an overarching principle that 'consumers should control who has access to their consumption data and the use to which it is put, except where required to fulfil regulatory obligations.' The prospectus affirmed that the government was taking a 'privacy by design' approach, giving as an example a functional requirement that meters should be the 'primary store' of metering data.[29]

In their analysis of consultation responses, the government noted that the programme must comply with the Data Protection Directive principles and the European Convention on Human Rights. They proposed an approach that would limit the flow of meter data via the Data and Communications Company (DCC) linking suppliers and network operators, starting from the presumption that detailed data would be transmitted to an In Home Display, smartphones, and personal computers using a Home Area Network. They also committed to exploring the potential of data minimisation, for example 'where data can be collected from a sample set of meters or aggregated so it would not be possible to identify a "living individual".'[30]

Following a further call for evidence in 2011 and a final consultation in 2012, DECC published final plans on data access and privacy for the programme, and an assessment of human rights compatibility. These took note of opinions from the Article 29 Data Protection Working Party, the European Commission's proposals for reform of the Data Protection Directive and Recommendation on the roll-out of smart meters, recommendations from the European Regulators Group for Electricity and Gas and the European Task Force on Smart Grids, and developments in other member states, the US, Canada and Australia.

The plans include the development of a Privacy Charter by industry, supported by consumer groups, and the finalisation of a Privacy Impact Assessment. They also include the creation of sector-specific rules complementing the Data Protection Act.[31]

DECC has proposed that suppliers be able to access smart meter data at three levels of granularity via the Data and Communications Company:

(1) Monthly or less readings, without customer consent, for billing and the fulfilment of regulated duties;
(2) Daily or less granular readings, with a 'clear opportunity' for customers to opt-out;
(3) Half-hour consumption data, if customers opt-in (or opt-out in the case of approved trials).

'Regulated duties' include prevention of theft, for which DECC decided that daily readings should generally be adequate, with the option of case-by-case investigations to access half-hourly readings. The extent of such duties will be a key factor affecting future data access. Suppliers would need explicit consent to use daily consumption data for marketing, except for information relating to the 'supply of electricity'.

Network operators will be allowed to access half-hourly consumption data for the purpose of developing 'efficient, co-ordinated and economical [distribution] systems,' but first must get approval from DECC or Ofgem for detailed plans that explain what data would be accessed for which purposes, and how privacy concerns will be addressed – including how anonymisation or aggregation of data could be used.

Regulator Ofgem criticised the proposed 'opt-out' daily reading regime, due to the competitive advantage it gave suppliers over third party services, and urged caution 'unless and until it can be established that an opt-out approach will not damage consumers' confidence in the roll-out.' It also noted the importance of giving network companies access to customer data that was 'aggregated or anonymised where possible.'[32] This echoed the general Opinion from the European Data Protection Supervisor (2012, 12): 'in the absence of freely given, specific, explicit, informed consumer consent for a specific time-of-use tariff plan or for the provision of a specific value-added service that requires more frequent readings, individual readings should not be done and transferred more frequently than on a monthly basis.'

DECC has noted 'ongoing developments in the field of privacy-enhancing technologies', but suggested that the field is as-yet too immature to mandate their use.

DECC's proposals will be given statutory force through their inclusion in licence conditions for suppliers and network operators. These must be approved by Parliament, and were originally planned to come into force in June 2013. Ofgem will be responsible for monitoring and enforcing compliance. A Smart Energy Code, following a similar parliamentary process, will regulate third party access to meter data. The latter will be part of a wider government 'midata' programme on consumer access to personal data.[33]

Analysis

The most significant gap between privacy by design principles and the design of Britain's smart metering programme was the lateness of serious consideration of privacy issues in the process. The May 2007 appraisal of options for the Department for Business barely mentioned privacy, and by the time of the DECC May 2009 consultation, key decisions had already been provisionally made on the system architecture, such as the inclusion of a centralised Data and Communication Company. A full Privacy Impact Assessment was only published in December 2012,[34] at the same time as the government announced its final plans and legislative text.[35]

More privacy-friendly options were not given serious consideration – unlike in Germany, which developed specifications for a home gateway that communicates with all parties and aggregates data according to specific recipient profiles. German privacy regulators and the federal standards institute were heavily involved in smart meter discussions by the German parliament 'from the very beginning,' with data minimisation and 'data sovereignty' the starting point.[36]

This highlights the importance of proactive consideration of privacy issues in organisations. The UK government has an unfortunate tendency to assume that data protection issues can safely be left to the Information Commissioner's Office (ICO) – but the ICO often lacks the resources, access, and expertise to shape departmental policy early enough. Even when ICO officials attended smart meter workshops, they were sometimes criticised by civil society groups for taking a 'heavily pro-industry position.' Ironically, the statutory consumer body (Consumer Focus) that stepped into this breach has since been abolished.

The ICO focuses on the provisions of the Data Protection Act, but as the Dutch government found, it can sometimes be broader human rights obligations that cause problems for government programmes. It is extremely costly for regulators to leave such issues to a court process that might take a decade before being decided by the European Court of Human Rights, long after hundreds of millions of euros have been spent on expensive technical infrastructures.[37]

Britain's programme also highlights the importance of multi-stakeholder involvement in policy discussions. One academic expert interviewed complained: 'Ofgem/DECC ran a functional specification workshop … to which they did not even invite the geeks who design and program the meters, let alone troublemakers like us. We just get emailed the PowerPoint afterwards, so that they can pretend they're being "transparent".' Another recalled: 'I emailed Ofgem on behalf of [a professional society] offering the society's help to get the specification right, and weeks later got a patronising email saying that they are pleased that I was interested in their meeting but that, as I would appreciate, there were limited places available, but that they would welcome feedback on the outputs from the meeting. These amounted to transcripts of flipcharts that summarised what seem to have been very superficial break-out groups.'

While these types of comments can be uncomfortable for officials, it is better for all concerned if a broad range of participants can bring a critical eye to policy decisions before they are finalised.

In proposing to set sector-specific data protection rules, overseen by the Office of Gas and Electricity Markets (Ofgem) cooperating with the ICO, DECC is attempting to strengthen regulatory oversight once smart meters have been rolled out. However, the practical details of such joint regulatory oversight have yet to be worked out, and have few precedents. Likely more successful would be pan-European cooperation of national data protection authorities in areas of common interest, as has recently been seen both in the Article 29 Working Party's opinion on smart meters, and the French-led investigation into Google's privacy policy, leading to a decision that was unanimously approved by the members of the Working Party. Such common action is an important part of the proposed Data Protection Regulation.

EU policy was unusually influential for this British energy programme. While DECC initially claimed Britain's industry structure was unique, events in the Netherlands led to a stronger data protection position than expected at the European Commission and the Article 29 Working Party. The recommendations from the EU smart metering task force were much more restrictive than suppliers were pushing for, leading to frantic lobbying in Brussels and a concomitant reaction from the Article 29 Working Party. The resulting policies have had a significant impact on the British programme. The European Data Protection Supervisor has since suggested that further legislative amendments should be made at the EU level, not least requiring data controllers to conduct data protection impact assessments of systems, and to notify any breaches of smart meter databases.[38]

Competition arguments also had a significant effect. Civil society groups warned DECC that if suppliers automatically received detailed half hourly consumption data from customers, they could provide offers and energy-saving advice only to the most profitable customers, as had been seen in the mobile telephony market. Ofgem warned that giving energy suppliers more access to customer data than third-party services would give the former an unfair advantage.[39]

Conclusion

How far did the British government follow 'privacy by design' principles in developing its smart metering programme, as it repeatedly claimed in consultation documents? Civil society experts interviewed were sceptical: 'it became a buzzword, but in practice we have not seen much evidence of it. Suppliers ridiculed [genuine privacy-enhancing approaches] because they were so far away from existing processes. Throughout the process there has been no vision of how privacy by design could have been implemented.

Working groups were dominated by incumbents who are only willing to go one or two steps further than where they are. Therefore, we have a sticking plaster solution on what is fundamentally not the best approach.' Another noted: 'Industry was directly interested in getting personal data and just not interested in privacy enhancing technologies. They also argued [PET designers such as Danezis et al.] didn't understand the industry.'

There has been little involvement from legislators during the programme, since the Secretary of State has wide latitude to set the regulatory framework using secondary legislation. The 'negative resolution' procedure used to amend electricity and gas supplier and distributer licence conditions under s.88 of the Energy Act 2008 provides little opportunity for Parliament to influence the amendments, and comes at the end of the process. Interviewees expressed scepticism that the UK parliament would exercise equivalent oversight to the Dutch and German parliaments. One said: 'we will continue to push issues with the Public Accounts Committee and others, but politicians' expertise is woefully inadequate. We rely on checks and balances in the committee system, but if MPs are not able to get engaged with details of a programme there is no way to hold departments to account – which is what is happening with the smart meter programme.' Privacy issues therefore largely fell between energy regulators, who had limited privacy expertise, and the Information Commissioner's Office, which had limited resources and mandate to shape the regime.

The British programme proposed to Parliament by DECC has ultimately ended up with similar rules to the amended Dutch programme: meter installation is voluntary for customers; energy consumption is measured for billing purposes without specific consent at monthly (Britain) or bimonthly (Netherlands) intervals, and when customers move or change suppliers. More detailed data can be read for specific legal obligations, but explicit consent is needed for half-hourly (Britain) or hourly (Netherlands) readings to be taken for other purposes.[40]

While these compromises seem to meet the basic requirements of the Data Protection Directive and European Convention on Human Rights, earlier consideration of more privacy-friendly options might have produced a more protective (and cheaper) system. For example, Ross Anderson has suggested that governments should simply coordinate the production of industry standards for communication between meters, home devices, and energy companies, and set privacy standards clarifying that data should be controlled by consumers on the meter and shared minimally with other parties.[41] This would allow privacy-sensitive consumers to use privacy-enhancing technologies such as those developed by Danezis et al., while still providing the energy industry with the information it needs to manage networks and supplies. Unfortunately, the British government now appears to have become too attached to their current proposals to reconsider this option.

Acknowledgements

This research has been supported by the European Commission (FP7 Grant Agreement 288021) and the UK Engineering and Physical Sciences Research Council (grant EP/G070687/1). The author thanks the interviewees who generously shared their time and expertise to illuminate several key aspects of the processes described in this article.

Notes

1. Directive 2006/32/EC of the European Parliament and of the Council of the European Union of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC. OJ L 114, 27.4.2006, 64.

2. Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC. OJ L 315, 14.11.2012, 1.
3. Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC. OJ L 211, 14.08.2009, 91.
4. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC. OJ L 211, 14.08.2009, 134.
5. See Cuijpers and Koops (2013).
6. Article 6 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31.
7. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final, 25.1.2012.
8. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31.
9. Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*.
10. Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*, 8.
11. Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*, 14.
12. European Data Protection Supervisor, Opinion on the Commission Recommendation on preparations for the roll-out of smart metering systems, 11.
13. See Cuijpers and Koops (2013, 27).
14. Ibid.
15. Henney and Anderson (2012, 1-2).
16. Cuijpers and Koops (2013, 5).
17. Cavoukian, Polonetsky and Wolf (2010); Spiekermann and Cranor (2009).
18. Cuijpers and Koops (2013, 22-23).
19. Cavoukian, Polonetsky and Wolf (2010, 13-14).
20. Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*, 14.
21. Cuijpers and Koops (2013).
22. Rial and Danezis (2011).
23. Kursawe, Danezis and Kohlweiss (2011).
24. Rubenstein and Good (2012).
25. MacDonald (2007, 52).
26. Department of Energy and Climate Change (2009, 22).
27. Brown (2012).
28. Civil society expert interview, 2012.
29. Department of Energy and Climate Change (2010, 1).
30. Department of Energy and Climate Change (2011a, 4-5).
31. Department of Energy and Climate Change (2012a).
32. Ofgem (2012).
33. Department of Energy and Climate Change (2012b).
34. Department of Energy and Climate Change (2012c).
35. Department of Energy and Climate Change (2012b).
36. Pallas (2012, 14).
37. Anderson et al. (2009).
38. European Data Protection Supervisor (2012, 9).
39. Ofgem (2012).
40. Cuijpers and Koops (2013).
41. Anderson (2010, 4).

References

Anderson, R. 2010. *Consultation response on smart meters*. Cambridge: Foundation for Information Policy Research.

Anderson, R., Brown, I., Dowty, T., Inglesant, P., Heath, W., and Sasse, A. 2009. *Database state*. York: Joseph Rowntree Reform Trust.

Article 29 Data Protection Working Party. 2011. *Opinion 12/2011 on smart metering,* 4 April. WP 183.

Brown, Ian. 2012. Government access to private-sector data in the United Kingdom. *International Data Privacy Law* 2, no. 4: 230–8.

Cavoukian, Ann, Polonetsky, Jules, and Wolf, Christopher. 2010. SmartPrivacy for the Smart Grid: Embedding privacy into the design of electricity conservation. *Identity in the Information Society* no. 3: 275–94.

Cuijpers, Colette, and Koops, Bert-Jaap. 2013. Smart metering and privacy in Europe: Lessons from the Dutch case. In S. Gutwirth et al. (eds.)*, European data protection: coming of age,* Dordrecht: Springer.

Department of Energy and Climate Change. 2009. *A consultation on smart metering for electricity and gas.* 11 May.

Department of Energy and Climate Change. 2010. *Smart Metering Implementation Programme: Data privacy and security.* 27 July.

Department of Energy and Climate Change. 2011a. *Smart Metering Implementation Programme: Response to prospectus consultation – Data access and privacy.* 30 March.

Department of Energy and Climate Change. 2011b. *Smart Metering Implementation Programme: A call for evidence on data access and privacy,* August.

Department of Energy and Climate Change. 2012a. *Smart Metering Implementation Programme: Data access and privacy.* 5 April.

Department of Energy and Climate Change. 2012b. *Smart Metering Implementation Programme: Data access and privacy – Government response to consultation,* December.

Department of Energy and Climate Change. 2012c. *Smart Metering Implementation Programme: Privacy impact assessment,* December.

European Data Protection Supervisor. 2012. *Opinion on the Commission Recommendation on preparations for the roll-out of smart metering systems,* 8 June.

Henney, Alex, and Anderson, Ross. 2012. *Smart Metering – Ed Milliband's poisoned chalice*. Review for Cabinet Office.

Kursawe, Klaus, Danezis, George, and Kohlweiss, Markulf. 2011. Privacy-friendly aggregation for the smart-grid. *Proceedings of Privacy Enhancing Technologies – 11th International Symposium*, 175–91. Dordrecht: Springer-Verlag.

MacDonald, Mott. 2007. *Appraisal of costs & benefits of smart meter roll out options*. London: Department for Business, Enterprise and Regulatory Reform.

Ofgem. 2012. *Ofgem's response to DECC's consultation on data access and privacy.* 30 May.

Pallas, Frank. 2012. Beyond gut level: some critical remarks on the German privacy approach to smart metering. *Computers, Privacy and Data Protection*.

Quinn, E. L. 2009. *Privacy and the new energy infrastructure*. University of Colorado Law School working paper.

Rial, Alfredo, and Danezis, George. 2011. Privacy-preserving smart metering. *Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society*, 49–60. New York: ACM Press.

Rubinstein, Ira S., and Good, Nathaniel. 2012. *Privacy by Design: a counterfactual analysis of Google and Facebook privacy incidents.* New York University School of Law Public Law and Legal Theory Research Paper Series Working Paper no. 12-43.

Spiekermann, Sarah, Cranor, and Lorrie Faith. 2009. Engineering privacy. *IEEE Transactions on Software Engineering* 35, no. 1: 67–82.