*International Review of Law, Computers & Technology*, 2013
Vol. 27, Nos. 1–2, 161–186, http://dx.doi.org/10.1080/13600869.2013.764140

Routledge
Taylor & Francis Group

# Smart meters and the information panopticon: beyond the rhetoric of compliance

J. Savirimuthu*

*Liverpool Law School, University of Liverpool, Eleanor Rathbone Building, Bedford Street South, Liverpool, L69 7ZA, UK*

(*Received 4 December 2012*)

The Smart Meter Implementation Programme is the Government's flagship energy policy. In its search for solutions to address privacy dilemmas raised by smart meters, the Government has been content with using data protection principles as a policy framework to regulate the processing of consumers' personal information. This is worrying since the question of *who* has access to *what* type of information and *how* it is used cannot simply be regarded as raising information security, authenticity and integrity issues. If we are to go beyond the rhetoric of protecting the privacy rights of energy consumers we must scrutinise the context in which legitimate interests and reasonable expectations of privacy subsist. To remedy this apparent policy oversight, the paper undertakes two tasks: first, to clarify the content and application of data protection and privacy rights to smart meters; and second, it outlines a policy framework that will address the lack of specificity on how best innovation and privacy issues can be better calibrated. More importantly, it calls for targeted substantive reforms, development of accessible privacy policies and information management practices that promote transparency and accountability and deployment of technological solutions that will help reduce emerging fault lines between innovation and privacy in this sphere of energy policymaking.

**Keywords:** Privacy; data protection; smart meters

## 1. Introduction

The energy industry is on the cusp of an information revolution.[1] It is expected that over 28 million homes in the UK will have smart meters installed in them by 2020 as part of the Government's Smart Meter Implementation Programme (the Programme).[2] This affordance will not only enhance energy generation and distribution capabilities but it will also enable real-time energy consumption data of individuals to be collected and used.[3] Balancing the benefits of access to consumers' energy usage data for productivity, innovation and competition with privacy concerns continues to pose considerable challenges.[4] By installing smart meters in their homes, individuals will effectively be exposed to three specific information pathologies: use of energy usage activity to construct personal profiles; sharing of aggregated de-identified energy usage data with commercial organisations for marketing and advertising purposes; and evolution of smart meters into surveillance technologies to be used by local authorities and law enforcement.[5] Context-aware innovations such as smart meters are outpacing the ability of policymakers to implement

*Email: jsaviri@liverpool.ac.uk

effective and democratic regulatory frameworks.[6] The Government, in its search for solutions to address privacy dilemmas raised by smart meters, has been content with using data protection principles as a policy framework to regulate the processing of consumers' personal information.[7] This is regrettable since the intrusive nature of smart metering technology also requires provision of safeguards against the invisible processes of digital curation, which can impair an individual's right 'to respect for his or her private and family life, home and communications' as stipulated by Article 8 European Convention on Human Rights (ECHR) (*Pretty v United Kingdom* (2002) §61).[8] This paper charts a possible way forward to remedy the policy oversight. It begins with an examination of the Programme and explains its role and outcomes. The paper then goes beyond familiar debates on privacy compliance within the smart metering environment in two respects. It first situates smart meters within the information generative environment where individuals willingly share information, yearn for new technologies and innovations but seem equally anxious about converging public and private spaces.[9] Second, it frames privacy policy regulatory objectives for smart metering in terms of managing the transition and balancing innovation benefits and privacy values. It clarifies the content and application of data protection and privacy rights and outlines a policy framework that will address the lack of specificity on how best innovation and privacy issues can be better calibrated. More importantly, it calls for targeted substantive reforms, development of accessible privacy policies and information management practices that promote transparency and accountability and deployment of technological solutions that will help reduce emerging fault lines between innovation and privacy in this sphere of energy policymaking.

## 2. The smart meter implementation programme: the rhetoric of compliance

### 2.1. *The Smart Meter Implementation Programme*

The Government has five policy strands in its energy reform agenda: first, demonstrating compliance with regional and international commitments in tackling climate change; second, supporting the EU's 2020 emission reduction target; third, developing domestic strategies that enhance energy security and competition; fourth, providing political leadership in moving towards greater use of renewable sources for energy; and finally, of relevance to the present paper, establishing smart grids and implementing a Programme for deploying smart meters.[10] Market ideology is an important driver of the Programme.[11] It has also played an important role in framing policy debates and regulatory strategies for privacy. The workshops, consultations and meetings with all affected stakeholders emphasise a 'light touch' strategy. Self-regulation is aimed at providing the energy sector with incentives to invest in smart grid infrastructures and drive innovation while assuming primary responsibility for addressing consumers' needs and expectations (e.g. data protection and security, interoperability, controlling energy usage and reducing bills). The Programme provides a transparent process documenting the views and experiences of energy utilities, consumers and organisations from the public and private sector on a range of technical, operational and implementation issues, which also includes establishing privacy management frameworks. During the Prospectus Consultation in March 2011, efforts were made to elicit responses from industry regulators, the Information Commissioners Office (ICO), representatives from the energy sector and consumer watchdogs.[12] The discussions were wide ranging and covered matters relating to information management policies, information sharing and design protocols and product development and installation plans.[13] The Government, encouraged by the consensus building and collective

vision generating exercise subsequently published its conclusions to the Programme in April 2012.[14] It also commenced consultations on its proposals for data access and privacy, mindful that more work was needed to persuade the industry to develop privacy management programs that were transparent and accountable.[15] According to the Government, a consumer-centric approach would go some way towards allaying any public misgivings about the cost of the Programme and the benefits of smart meters for consumers.[16] While some may regard the strategy for placing consumers at the centre of smart metering policy as a rhetorical device, we should not ignore the economic imperatives driving the Programme and which could ultimately prejudge how privacy management programs are to be operationalised. It is true that industry has made some concessions. For example, with the exception of collecting monthly data, consumer consent will now be required before utilities can access additional energy usage data. Rules will be developed to facilitate consumer access to their energy records. Arrangements are now to be made to provide a framework for network distributors and suppliers to address data access and security issues.

The Government has also built on 279 responses from 197 stakeholder groups and these are reflected in the consultation document and comprise a number of proposals for managing consumer's expectations and privacy concerns.[17] Four are worth noting. First, there was broad support for educating consumers and raising their awareness of privacy issues.[18] The industry assured the DECC that it would develop accessible codes that place customers at the centre of policymaking. The Government in its Response to the Prospectus Consultation urged the Energy Retail Association (ERA) to develop a Privacy Charter, which would reassure customers that their personal information and privacy would not be compromised. A draft Privacy Charter has since been produced, which sets out a number of information management commitments regarding the way energy usage information was to be accessed and used.[19] Second, the linkage between licence conditions and risk assessment audits could be regarded as encouraging the energy industry to view information security as a continuing process. Suppliers and network operators would now be required as part of the licensing arrangement to ensure that processes for creating, storing and accessing of energy usage information were in line with industry benchmarks. Third, the Energy Networks Association (ENA) recently conducted a Privacy Impact Assessment (PIA) to assess members' readiness in dealing with privacy issues raised by the use of energy usage data.[20] Smart meters with their enhanced collection and transmission of data functionalities raise concerns about security and potential misuse of information. Impact assessments offer the prospect of addressing specific privacy concerns and provide opportunities for developing prudent information management practices within the organisation.[21] Third, stakeholders agreed that Privacy by Design (PbD) should be integrated into the design of smart meters since the algorithms were originally conceived with accessing raw energy data rather than discriminating between non-privacy and privacy invasive data.[22] This strategy for addressing privacy issues pursues the programme initiated by the ICO in 2008.[23] The value of PbD is founded on the premise that addressing privacy concerns after the installation of smart meters would be time consuming, expensive and erode consumer trust and confidence.[24]

At one level, the concessions could be viewed as demonstrating clear commitment to the cause of consumers. While it is encouraging that industry attaches great importance to engaging directly with consumers, the likely effectiveness of these measures may prove to be exaggerated. We can provide a context for these concerns through a consideration of the nature of smart meter technology.

### 2.2. *The relational dimension: visualising smart metering data and privacy dilemmas*

It is uncontroversial to say that context-aware technologies embedded in smartphones such as iOS, Android and Windows enable businesses to leverage vast amounts of consumer data. Smart meters reflect an extension of this trend into the energy sector. According to IBM's recent study, utilities stand to leverage data from 96 million reads per day for every million meters.[25] Smart meters are equipped with sensory affordances that collect, store, process and transmit energy usage data to suppliers and network distributors. Care should however be taken in not demonising smart meters on the basis of its functionalities. Smart meters offer operational, consumer and societal benefits. Optimising the economic value of energy usage data will no doubt ensure returns to shareholders on considerable investments poured into innovation, advanced metering infrastructures (AMI) and energy grids. Assuming the economies of scale are realised, the energy sector as a whole stands to benefit from using volumes of data to drive productivity and innovation in the generation, distribution and transmission of electricity. Data relating to consumption needs and preferences could be used to improve demand response, detect theft or power outages and address any problems in the distribution and supply chain. Suppliers should be able to provide consumers with flexible pricing options based on actual energy consumption. Information derived from raw energy data could also be used to deliver innovative products and services to consumers. In the longer term, with the deployment of smart grids, smart meters will enable alternative energy sources to be integrated into networks. Energy usage information will be provided in human readable format and gleaned from in-home displays.[26] Consumers could also monitor their energy consumption activity and use smartphone apps to control heating levels and lighting devices. Finally, payments would be based on energy actually consumed rather than estimates. Consumers would not be reliant on human meter readers or estimated energy consumptions bills.

It is important to recognise that privacy dilemmas confronting energy policymakers have been encountered in other realms (e.g. online profiling, behavioural advertising, data mining in e-Health and tracking on social networking sites and websites).[27] The questions, *what* type of data can be accessed, by *whom*, for *what* purposes and for *how* long are frequently encountered in policy debates concerning information privacy.[28] It is worth recounting the reasons smart meters raise privacy anxieties in the first instance. First, there is a legacy of mistrust, which implicates the Programme. As the Special Eurobarometer survey revealed, there is general public mistrust in the way industry discharges its obligations towards safeguarding consumers' privacy and personal data.[29] Another reason could be that individuals still regard electricity as a commodity to be consumed when switching on an appliance or device. Smart metering innovations such as non-intrusive load monitoring software do more than bridge the previous gulf between transmission and consumption of energy. Context-aware technologies, unlike the human meter reader, interweave social, digital and communication spaces seamlessly and often with consumers being totally unaware of their functionalities. Most consumers do not readily associate convergence between social, energy and technological contexts with the potential exposure of their location details, the duration and frequency of their use of communication devices and monitoring of activities they would regard as being within the zones of private lifestyle choices, expressions and intimate interactions. This is troubling: as Quinn suggests, data from energy consumption activity could even be used to identify periods when occupants are sleeping, watching television or eating.[30] Depending on the frequency of the collection (e.g. daily, hourly or quarter hourly), the life cycle of energy usage data could be capable of

being extended indefinitely to serve business needs and made available to third parties outside the energy industry (e.g. law enforcement, insurance companies and landlords). The lack of clarity regarding applicable standards and mechanisms that ensure transparency in information management programs could only heighten public mistrust.[31] Finally, even though we have a patchwork of privacy regulations, it should also be borne in mind that cultural attitudes toward electricity have not kept pace with evolving business models, which regard monetisation of energy usage data as a legitimate commercial opportunity. Rheingold is right when he recalls that pervasive computing cultures are characterised by the way new smart technologies become embedded into the daily lives of individuals.[32] Data protection rules do not adequately address the dilemma confronting individuals as social media platform providers and energy suppliers encourage consumers through design and technological functionalities to disclose a wide range of information about themselves, their preferences and lifestyles.[33] Cavoukian's continued references to technological solutions such as PbD might in large part be due to the scale and pace of privacy-invasive developments culminating in industry utilising software algorithms to profile individuals and its use of innocuous pieces of information from public and private sources to create multiple identities for individuals. Individuals are not only oblivious to the scale of profiling taking place but are effectively powerless to stem this rising tide of 'big data'.[34] The granular data derived from smart meters could therefore be regarded as possessing a generative element, in the sense that new knowledge generated from the data could be shared and used in contexts other than billing – mobile app developers and electrical appliances manufacturers for example would have particular interest in aggregated de-identified consumer data to help them understand how their devices and services are being used. Profiling and data mining have clear implications for individuals who regularly use smart devices to connect to the Internet and consumer social media.[35] It is an aspect of cultural and technological convergence that has not been fully accommodated within the measures proposed in the recent Programme Update.

### 2.3. *Assessment*

The Programme provides us with the first opportunity to reflect on the energy industry's response to the impact of smart meters on its privacy management strategies, policies and organisational practices. It also gives us an insight into the principles that currently inform the Government's privacy strategy. Both Government and industry regard the Programme as achieving the goal of identifying key strategies and priorities: Government commitments to mass-scale roll-out on the proviso that consumers can opt-out from the installation, industry's responsibility for identifying and implementing information management measures that safeguard consumers personal information, a balanced approach towards innovation and privacy concerns and greater engagement with consumers. If we take the outcomes to the Programme at face value, the rhetoric of compliance with data processing rules would appear to be sufficient. In view of the earlier discussion, it is understandable why consumer organisations and privacy advocates question whether benefits to consumers will be outweighed by overriding gains to the energy sector following installation of smart meters throughout the country. Doubts for example have been expressed at the outset whether the interests of consumers could be robustly protected given the close relationship between Ofgem, DECC and the energy industry. Anderson expressed his dismay that the Government had not learnt from its failed attempts to balance utility and privacy values in creating centralised databases for personal information.[36] The watchdog, Consumer Focus, while supportive of the technology, stressed that Government and

industry had some way to go in persuading the public of the value of smart meters.[37] Consumer mistrust of the energy sector continues to be prevalent and suspicions surround the value of installing smart meters in homes. The sporadic media campaigns undertaken by individual energy suppliers may partially explain why consumers do not appear to have an understanding of smart metering technology or suppliers' information management practices. The lack of effective engagement does not bode well for the future, particularly as the Programme places great store by consumers making meaningful choices.

There are more fundamental concerns. For example, the absence of a clearly defined privacy safeguard baseline will have implications for consumers' expectations and the regulator's ability to assess industry compliance with its privacy obligations. During the Programme, representatives from the industry pointed to value added services that could be generated from access to granular data. Industry reaction to the generative potential of energy usage data is particularly significant from a self-regulation perspective.[38] Linkage between privacy management and industry self-regulation conceals a paradox: what incentives are there for the energy sector to further the privacy interests of consumers when the business model is designed to leverage the economic value of energy usage data? This important question aside, the impression gleaned from the recent Programme Update is that compliance with data protection legislation would be sufficient to discharge the energy sectors' privacy obligations towards consumers. There is no suggestion in the Programme or from the information made available on energy suppliers websites that indicates an awareness of the need to ensure that smart metering operations and practices are also consistent with individuals' Convention rights, in particular Article 8 ECHR. As will be illustrated later, it is never a foregone conclusion that compliance with data protection legislation avoids any violation of an individual's human rights under the ECHR (*Z v Finland* (2008), *Pretty v UK* (2008)). This brings us to another area of concern – the value of privacy policies.

There is general consensus that privacy policies are impenetrable and lack clarity – it comes as no surprise to find that privacy policies relating to suppliers' collection and use of consumers' energy usage data offer nothing more than generic commitments and lack specificity.[39] One would have expected that with the imminent cultural shift in the way consumers would interact with energy and the industry that privacy policies will be used to embed transparency and accountability values. Bennett's pessimism regarding the effectiveness of self-regulation generally may hold true in this context.[40] The real concern with self-regulation is that often little is done by the industry to identify credible mechanisms for promoting transparency and accountability in its privacy management practices. It is in this sense that Bennett's comments could be regarded as being relevant to the present discussion. The idea of accountability does not appear to go beyond producing best practice policies, developing Privacy Charters and restating commitments to PbD. What is more disconcerting perhaps is the fact that Article 8 ECHR issues appropriate to the residential context (e.g. respect for life, family and quiet enjoyment) were not considered or explicitly addressed during the Programme in view of well-established Strasbourg jurisprudence (*Peck v UK* (2003) §57, *Evans v UK* (2006) §59). This policy oversight is regrettable as privacy violations in these contexts are rarely visible and its adverse consequences are likely to be far reaching (*Smith and Grady v UK* (1999) §87). Consumers' lack of awareness of the range of privacy risks also undermines the value of privacy policies.[41] There is also the risk that, should consumers take notice of these documents, many will assume that the presence of a Privacy Charter will invariably protect all their privacy rights.[42] Following an examination of the Privacy Charter and energy suppliers' current privacy policies, it seems that this confidence might yet prove to be misplaced. Critical issues relating to

*who* has responsibility for dealing with complaints regarding *third party use* of consumer's energy usage data, for *what purposes* and for *how long* personal information is to be held cannot be artificially separated from those comprising an individual's physical and social identity. The consumption activities are very much indivisible and which include the individual's "right to personal development, and the right to establish and develop relationships with other human beings and the outside world" (*Pretty v UK* (2008) § 61).

Gellert and Gutwith make another observation that lends weight to the concerns expressed above.[43] They suggest that in an environment where technology, social media and culture intersect, the premise that data protection laws are sufficient to provide effective safeguards for individuals is erroneous.[44] This is a timely comment and it also highlights the relevance of context in decision making by consumers. A smart meter generates one CD worth of data every 15 minutes per year.[45] If we multiply this volume of data with real-time collection activity that will take place within the curtilage of homes, the implications for individuals' reasonable expectations of privacy are likely to be immense. It is not entirely clear how policymakers and the energy industry will eventually address these thorny issues, given that they seem to arise from a failure to acknowledge the need to preserve the individual's right to privacy within the home. Consequently, the failure to consider the rationale and conceptual foundations of the rights to privacy will deprive the Programme of much of its value in creating accountable and responsive privacy management processes.[46]

The overreliance on data protection not only suggests the market imperatives driving policymaking but also illustrates how far policymakers have lagged behind in their appreciation of the social value of privacy in the age of 'big data'. Indeed, in this environment of pervasive computing and the likely harms resulting from leakage of personal information, the role of Article 8 ECHR in ensuring that individuals retain some autonomy in managing boundaries between public and private spheres becomes all the more critical.[47] It may be unfair to quickly dismiss these observations. For example, how does one assess the appropriateness of smart metering privacy policies or information management practices, when data points are capable of creating visual representations of activities taking place within the private space of the home? Accountability is seriously undermined by the absence of any narrative or text in the Privacy Charter or PIA, which suggests that energy suppliers, network operators and value added services providers recognise the full extent of their obligations under Article 8 ECHR.[48] As the Leveson Inquiry makes plain, respect for privacy rights must be extended to everyone. This is a point worth keeping in mind since it is now well-known that software algorithms, can reveal 'at what hour each night the lady of the house takes her daily sauna and bath – a detail that many would consider "intimate"' (*Kyllo v US* (2001) 38). The upshot is that there may be sound reasons why individuals may not wish to have their consumption activities, communications, sites visited and online interactions made visible.[49] Admittedly this may be seen as an extreme example but it serves the purpose of highlighting the need for Government to make clear that while society benefits from innovation it must not be at the expense of eroding fundamental privacy protections such as the individual's right to private life and family. Second, the conflation of data protection and privacy issues may suggest that regulators and industry view the standards for enforcing both sets of rights as being similar – this is patently wrong as the normative foundations, mechanisms for enforcement and outcomes for breaches are fundamentally different.

Finally, the failure to use the consultation phase of the Programme to articulate specific Article 8 ECHR issues, work through privacy management strategies and highlight operational compliance challenges at the outset would seem to place far too much faith in future pilot projects as a test bed for problem solving. Given that the precise relationship between data protection and privacy in the smart metering context has never been clearly

articulated, both Government and industry have missed an opportunity to provide much needed clarification regarding the circumstances when Article 8 ECHR rights might trump energy suppliers' contractual claims to access, use and distribute granular energy usage data. From a constitutional standpoint, the Programme can be seen as having initiated a significant policy shift from a baseline of principles of *opacity* to those of *transparency* without detailed scrutiny or public debate.

The discussion demonstrates the need to overcome these deficiencies. To this end, a hypothetical scenario will be provided to help frame the debate and lay the foundations for a hybrid model that may enable stakeholders embrace a responsive approach towards data protection and privacy values.

## 3. Data protection and privacy: legal and policy issues

### 3.1. *Contextualising the hybrid model for policymaking*

Judy lives in a five-bedroom detached house in Cosgrove Way (CW) with her partner Alex and two children, Janet and Mark, aged 17 and 23 respectively. There is a room on the ground floor that has been converted for Mark to use his home dialysis equipment. Mark is also a member of the NHS and National Kidney Federation support networks on Facebook. Judy and her family have smartphones, which allow them to connect to social networking sites. They have also installed a wide range of software applications on their computers, laptops and smartphones. The house has a home area network, which allows Judy and her family to access their computers and entertainment devices through password protected Wi-Fi. Judy recently installed a smart meter in the house and purchased a hub-based platform, which connects her smartphone and PC to the smart boiler and digital thermostat via the Internet. The app she downloaded from the energy supplier allows her to view real-time energy consumption remotely.[50] The other members of the family have since downloaded the app onto their smart devices. Judy frequently posts queries to the energy supplier's customer support site on Twitter.

Most reasonable individuals would accept that the collection of energy usage data for billing purposes is both legitimate and necessary. Safeguards are also needed to ensure that personal sensitive information is not processed without consent. Additionally, measures need to be put in place to support occupants whose health and well-being are dependent on continued and reliable energy supply. There will also be little disagreement that homeowners should be able to take full advantage of innovations that reflect their lifestyles and help them better manage their energy consumption choices and activities. Much of the policy debates during the Programme regarding the protection of consumers' privacy in the smart metering environment have tended to be framed narrowly in these terms. It may explain why the protection of an individual's privacy has been viewed through data protection rules and mechanisms. Given that many consumers use multiple communication devices and platforms (e.g. tablets, smartphones, laptops, social networking and micro-blogging sites) within the home to engage in a range of activities of a private or intimate nature, the narrow focus on data protection safeguards underestimates the real social costs to an individual's privacy and respect to private and family life.[51] One aim of the hypothetical is to draw attention to the fact that data protection and privacy laws can coexist in a smart metering environment.

Technological and cultural convergence has not only disrupted assumptions about information pathologies, but the pace of developments may suggest that the Government has perhaps erred on the side of caution and adopted a 'wait and see' approach rather than actively steering the industry towards developing accountable privacy management frameworks that balance utility and privacy concerns. Industry inertia in integrating transparent

and accountable privacy mechanisms continues to concentrate the minds of policymakers on both sides of the Atlantic.[52] Cohen is not exaggerating when she highlights the illusory nature of consumer consent in an age where personal information is seen as a resource to be leveraged.[53] Raab draws our attention towards the elusive nature of the concept of accountability – he suggests that its rhetoric should not distract us from the need to evaluate the basis upon which organisations can be said to have discharged their stewardship responsibilities over consumers' personal information.[54] Both observations not only highlight ongoing privacy dilemmas but they also illustrate the complexity of governance and the uncertain nature of how accountability is to be measured.[55] These governance dilemmas are further exacerbated by consumers' ambivalence to privacy policies being inaccessible or their fear that insisting on privacy invasive terms being removed will result in access to desired services and products being terminated. These concerns, including those now being witnessed at EU level relating to the Data Protection Reform Package, are also symptomatic of an attitudinal shift in two major respects: first the recognition of the need to transcend orthodox conceptions of personal information and, second, a willingness to scrutinise the reasons policymakers seem reluctant or unable to persuade industry to develop effective privacy compliance frameworks.[56]

We can help illuminate the issues raised by the hypothetical and offer a variant. Consider in a stark way if a human meter reader ('Bill') appeared in Judy's household and proceeded to record energy consumption activity and patterns of appliance use by its occupants over a period of 12 weeks. Imagine if he then compiled the information with data generated from texts, forms and online posts. This process, let us assume, allowed Bill to draw conclusions and inferences from the occupants' communication choices, appliance preferences, routines, beliefs and lifestyles: (i) Judy spent a lot of time online viewing poker gaming sites; (ii) Mark made extensive use of the dialysis machine between 6pm and 9pm during weekends; and (iii) Janet spent each morning chatting with her LGBT friends on social networking sites. Information from online football forums and Alex's tweets led to conclusions drawn about his leisure activities and times when he was likely to be away attending football matches. Bill uploaded all the information on his laptop and sent it directly to his employer via a secure protocol mediated by the network distributor. This information was collated and distributed to businesses that had information sharing arrangements with the energy supplier. Even though Judy consented to the sharing of information collected from the smart meter when entering into the service agreement with her energy supplier, should she be permitted, by way of analogy, to object to the monitoring activities of the human meter reader? How should revocation of consent be facilitated?[57] It is reasonably clear that policymakers and courts will be reluctant to supervise contractual relationships in the absence of clear evidence of exploitative behaviour or reliance on unconscionable terms.[58] Could these negative externalities and social costs be better addressed through targeted reforms to data protection? The culture of transparency that convergence and new technologies encourage, while amenable to data protection rules, does not sit easily with individuals' reasonable expectations of privacy. Why would data protection policies be found to be wanting in addressing the concerns of Judy and her family? Is it adequate for an energy supplier to rely on its contract terms in regard to information sharing arrangements?[59] What should be the default principle – opacity or transparency? Trenchant commitment to either principle has its drawbacks.

One problem with the Government's preferred policy option is that the market ideology of *laissez-faire* principles, which if relied upon exclusively, effectively places the onus on consumers to anticipate pathologies of information misuse. It is true that industry is subjected to

data protection rules – but the lack of effective enforcement mechanisms continues to hamper efforts to increase business responsiveness to consumers' privacy concerns. The focus on the process of collection and distribution does not, for example, address the effects of digital curation, which is an emerging phenomenon in the networked environment. Alex and Janet's expressions of their identity also remind us about the discriminatory potential of 'big data' when smart metering policymaking is not firmly grounded in norms that emphasise respect for fundamental rights to privacy. 'Big data' opens up a new dimension regarding the ethics of curation: the lack of autonomy and self-determination over how various items of personal information collected in public and private online environments are aggregated, the contexts in which they are subsequently used and the longevity of such data.

We can now offer three main reasons why a broader 'privacy logic' approach (rather than a 'data protection logic') towards governance, advocated by privacy scholars and the EDPS, is a preferable policy option for the Programme. First, the risks to choices about privacy and boundary management are likely to be significant. If the home is not a 'breathing space' where else can individuals find a space that prevents 'the seamless imposition of patterns predetermined by others'?[60] Second, individuals should be able to have peaceable enjoyment in their homes without fear of unauthorised access to energy usage data, which may expose them or their belongings to risk of violence or theft. Third, there is very little evidence available, which shows that the public has a good understanding of the safeguards and protections available to them under privacy and data protection regulations.

To conclude, the vignette alerts us to a more complex picture of convergence, data linkage and multiple access points to personal information flows within the home. Identity and privacy management are not purely data processing issues (*Commission v Bavarian Lager* (2009) §§100-103). By focusing on data processing safeguards the Programme misses an important dimension to privacy governance − it is not control over the data *per se* but the significance of the loss of autonomy in being able to define one's identities, preferences and lifestyles following the installation of smart meters. To non-privacy experts – the consequences of failing to respond to the significant paradigm shift in the way personal information is curated may be irreversible. Is it still possible to reorientate the smart metering privacy management strategy? Or must we choose between data protection and privacy? In the remainder of the discussion an outline will be provided of how we can reconcile both data protection and privacy principles, which avoids the crude market-led thinking that presently frames policy issues associated with privacy management practices in the Programme. Data protection principles are not so static as to be incapable of being accommodated within the framework of Article 8 ECHR (*Commission v Bavarian Lager* [2007] §§114 − 115, (2009) Opinion of the Advocate General §§214 − 217). We can approach smart metering privacy management policy from a stance that is slightly different, namely, highlighting how their integration will guide transparent and accountable process and effects-based outcomes.

### 3.2. *The legal framework*

#### 3.2.1. *Data Protection Directive 95/46/EC ('the transparency model')*

Personal information provides the resource for many economic, political and cultural arrangements. Historically, the creation of a regulatory framework for collection, storage and use of personal information was informed by the need to facilitate data processing activities of institutions while providing safeguards to the individual.[61] How does Directive 95/46/EC view its role?

Directive 95/46/EC, in encouraging transparency rather than secrecy, is founded on the idea that access to personal information facilitates proper functioning of institutions, organisations and economies (*Murray v Express Newspapers plc* (2007) §92). Balancing the interaction between these entities and information markets is very much a feature of this Directive. The ruling in *Durant v Financial Services Authority* (2003) is often regarded as a starting point for understanding the constraints imposed by data protection rules. It was held in this case that for information to be regarded as 'personal data', it had to consist of data that was 'biographical', had as its principal focus the data subject and that the context of its processing affected the individual in his personal, business or professional capacity.[62] Data that is anonymised, although not being completely free from the risk of being de-identified would not in the light of *Durant* be regarded as personal data (*R (on the application of the Department of Health) v Information Commissioner* (2011)). We have seen in the hypothetical scenario involving the individuals in CW that *Durant* does not help us address the issue regarding the use of information from multiple sources to create individual biographies despite compliance with data protection rules. Legal attempts in grappling with the evolving nature of personal data conceal tensions that result from reconciling complex cultural and technological values. Although *Durant* is regarded as precedent in this jurisdiction, we need to consider its reach alongside more recent developments, in particular the role of the influential Article 29 Data Protection Working Party (A29WP).[63] The A29WP most recently stated that smart metering processing activity will be engaged if the data collected 'relates to any information relating to an identified or identifiable natural person' and a person will be regarded as identifiable either directly or indirectly 'by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[64] Other 'data processors' that access or process metering data on behalf of energy utilities would also be brought within the scope of Directive 95/46/EC (e.g. network and transmission operators).[65] Data protection principles also obligate data controllers to ensure the security, integrity and authenticity of information processing activities. The rationale is to arrest information pathologies and define a broad set of principles to identify and curb potential threats to personal data (*Campbell v Mirror Group Newspapers* (2002) §§104-107).[66] These principles (e.g. legitimacy, fairness, purpose limitation, minimal data, access, integrity, security and disclosure), as De Hert and Gutwith suggest, provide the benchmark for data processing activities.[67] The principles also provide default standards for the energy sector. For example, Article 6 prescribes a set of principles that balance the needs of utilities and consumers. Smart metering data must, for example, be processed fairly and lawfully; collected and processed in a way that is compatible with the original purpose; must not be excessive in relation to the purpose for which the data are being collected or processed; accurate and not kept for a period that exceeds the purposes for which the data were originally collected.[68] Without these principles, there would have been very little institutional oversight over processing of individuals' personal data. It is, however, difficult to envisage a situation in the future when the ICO can lay claim to energy suppliers being in breach of the Directive, except in blatant cases of security lapses and loss of consumer data. In the main, energy suppliers are likely to be 'technically' compliant with Directive 95/46/EC as the principles are sufficiently nebulous to permit subjective assessments. More specifically, Judy may be representative of a number of consumers who discover too late that their ability to exercise their rights under Articles 12 (access right) and 14 (objection right) is redundant if contractual terms circumscribe their ability to retain effective control or if they are oblivious to their right to revoke consent to secondary use of consumption data (Articles 10 − 11). Finally, Article 7 recognises limited exceptions

where the unambiguous consent of the data is subject to the lawful collection and processing of energy usage data (e.g. where it is necessary for the utility to discharge its statutory or contractual obligations) (Articles 7(b) − (f)). However, processing of information that can lead to disclosure of health or sex life would not be lawful unless the 'data subject has given his explicit consent' (Article 8(2)(a)). As the A29WP noted, principles of consent and accountability must be operationalised and these must evident at the collection and processing phase.[69] The issues raised by the principles (e.g. what is necessary, when the amount of data collected is excessive and what period of retention exceeds the scope of the original purpose) are easy to comprehend in the abstract but as the hypothetical case illustrates, it is far from straightforward when applying them to an environment of converging mobile communication interfaces and hence not easy to resolve. The Programme does not provide any clarity on these matters.

Finally, metering data, which are used to identify the individual for billing purposes, would be regarded as personal data. Will energy data resulting from consumption activities of occupants in a particular household outside the scope of Directive 95/46/EC and hence not 'personal data' as such? This is a different question from that concerning technical data in the form of aggregated data taken from houses in the vicinity of CW to assess the performance level of the grid and assist in mapping peak response periods. The lack of clarity here must be addressed since Directive 95/46/EC only subjects the processing of 'personal data' relating to the data subject.

Data protection regulations have been placed under enormous strain in having to cope with technological convergence and information pathologies associated with smart metering in the age of 'big data'. It may be appropriate to recall that when Directive 95/46/EC was first enacted, surveillance technologies and arrangements for information sharing between the private sector that enabled individuals to be profiled and anonymous data to be de-identified were not as ubiquitous as they are today.[70] Even though the adoption of an opt-in/opt-out framework may be a solution of last resort it is not an ideal response from a public policy perspective, as noted by the A29WP:

> Consent is sometimes a weak basis for justifying the processing of personal data and it loses its value when it is stretched or curtailed to make it fit to situations that it was never intended to be used in. The use of consent 'in the right context' is crucial. If it is used in circumstances where it is not appropriate, because the elements that constitute valid consent are unlikely to be present, this would lead to great vulnerability and, in practice, this would weaken the position of data subjects in practice. (A2PWP 2011a: 10)

### 3.2.2 *Article 8 ECHR ('the opacity model')*

Article 8 EU Charter of Fundamental Rights now states that the protection of personal data is a right that imposes correlative obligations on the part of data controllers and data processors. Article 7 of this Charter also accommodates Article 8 ECHR. Article 8 ECHR is significantly wider in terms of contexts where privacy rights can be protected. Unlike Directive 95/46/EC, which relies on transparency in processing operations, Article 8 ECHR preserves the privacy of individuals and only permits disclosure under clearly defined grounds (*Halford v UK* (1997)). Of immediate relevance to the present discussion is that unlike Directive 95/46/EC, the scope of Article 8 ECHR covers all activities regarded as constituting private and family life. We can, for example, identify an established jurisprudence articulated by judgements from the European Court of Justice and national courts.[71] It extends for example, beyond the biographical information of a data subject and provides an extra layer of safeguards for physical, personal and psychological development,

namely gender, religious and political beliefs, sexual choices and identity. Before the rights under Article 8 ECHR can be engaged, the following elements must be satisfied: first, there must be an interference with the right to respect for the individual's 'private and family life, his home and his correspondence'; second, the interference must be in accordance with the law; and third, the interference is one that is regarded as necessary in a democratic society on the grounds provided (*Botta v Italy* (1998)).[72] Like all human rights, Article 8 ECHR does not create absolute rights but crucially places the onus on organisations to demonstrate that publication of the information is legitimate. In other words, the presumptive *opacity* rule can only be displaced if the intrusion is *in accordance with the law*, is *proportionate* to the purpose for which the intrusion was needed in the first place, is clearly *necessary* and comes within the *grounds set out in Article 8(2)* ECHR (*Huang* (2007) §20). The collection of aggregated energy usage data of occupants in a home, even though satisfying data processing rules could amount to a breach of the right to respect for family life if profiles are subsequently constructed to make visible, activities taking place within this space. As discussed earlier, aggregated data can subsequently be linked with various items of innocuous data and optimised to create a digital trail that constructs 'the self' of each occupant in a home. The boundaries between data protection and privacy law are uncertain and it is not entirely clear whether aggregated energy data that is de-identified and optimised in a manner described in the hypothetical would avoid breaching Article 8 ECHR. While there is some uncertainty regarding the ability of data protection laws to regulate the effects of profiling (either directly or indirectly) it is an activity that could be brought within the scope of the rulings in *S & Marper v UK* (2007) and *Z v Finland* (1997). The former could be regarded as one example of the care taken by courts when determining the types of information and contexts that give rise to Article 8 ECHR and data protection rights. The focus of the court's attention appears to centre very much on delineating 'a zone of interaction of a person with others . . . which may fall within the scope of "private life"' (*Peck v UK* (2003) §57). In other words, energy usage data is indivisible and cannot be neatly segregated into 'data processing' and 'privacy' spheres of activity (*Von Hannover v Germany* (2004) §59). The ruling in *Z v Finland* (1997) adds another layer of governance responsibilities, in particular the role of policymakers in framing privacy management strategies. The judgment recognises that the privacy of the individual is a fundamental right and makes clear that organisations (including the State) could be held to account if measures taken to ensure the security of personal information were found to be unreasonable. If States and organisations are to demonstrate compliance with their positive obligations towards individuals, it is imperative that privacy management frameworks are shown to complement the rights safeguarded by the Convention. There is one area that requires immediate attention of policymakers and industry. Positive measures are needed to demonstrate that the aggregation of items of information that ultimately lead to profiling of individual's preferences or lifestyles in his private space do not undermine the protections available under Article 8 ECHR (*Peck v UK* (2003) §63). Data processing rules do not however capture the myriad ways data mining and monitoring activities take place and consequently expose individuals to discrimination and arbitrariness (*Kruslin v France* (1990), *S and Marper v UK* (2007), Article 14 ECHR). *Perry v UK* (2004) serves as a reminder that disregarding the constitutional safeguards of citizens would not be tolerated. Finally, where monitoring takes place in the absence of consent, there is a clear expectation that evidence be provided to show that such a course is necessary in a democratic society, is proportionate and supported by the law (*Liberty v United Kingdom* (2009), *Heglas v Czech Republic* (2009)). If there is some doubt regarding the 'pressing social need' warranting the collection of additional information, Cuijpers and Koops suggest that industry undertakes an

assessment of smart meter functionalities, the nature and extent of its use and, finally, determine whether less privacy invasive methods are available.[73] This is correct but it should also be noted that Article 8 ECHR also envisages that a fair balance needs to be maintained between utility and privacy concerns on the one hand and potential conflicting public and private interests on the other. It may very well be that the 'margin of appreciation' threshold requires an assessment to be made in respect of the interests at stake and the degree of interference deemed to be unacceptable. For example, the collection and processing of information used to identify consumption activity, appliance choice and duration could potentially constitute an overreaching of Article 8 ECHR rights, if less privacy invasive steps which were regarded as a proportionate measure were not taken (*Amann v Switzerland* (2000), *Z v Finland* (1997)). Similarly, collection and processing activity on the grounds of expediency is unlikely to be regarded as satisfying the threshold of necessity or being in the interests of the economic well-being of the country (*Peck v UK* (2003) §77). Cases such as *Malone v UK* (1984) may also provide some guidance to policymakers in assessing the 'margin of appreciation' threshold. The court suggested that if breaches of Article 8 ECHR were to be avoided, the measures adopted must not be shown to be disproportionate and unnecessary in the particular context. Even the collection, retention and processing of personal information not preceded by measures which alert the data subject to the type of and purposes for which information was collected and the period for which it was being stored, could amount to a breach of privacy rights (*Shimovolos v Russia* (2011)). In *Douglas v Hello!* (2005) the Court of Appeal provided some insights into the 'margin of appreciation' threshold. It concluded that the public interest in disclosing information could be a relevant consideration when determining the scope of an individual's claim to have a reasonable expectation of privacy. As the Court of Appeal remarked in *Murray v Express Newspapers Limited* '[t]he question of whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case' (2009) Ch 481 §36.

Article 8 ECHR can therefore be regarded as a cluster concept and its application to information flows in CW is not bounded. By way of analogy *Copland v UK* (2007) should be taken into account when evaluating the policy issues highlighted in CW. An important limb to the concept of a 'reasonable expectation of privacy' is the view that surveillance technologies create a 'chilling effect' on the peaceful enjoyment and the well being of individuals in their home, since they create an environment that could lead to individuals monitoring their own activities. This view and the extract cited above, illustrates the mischief of Article 8 ECHR, namely to curb the imbalance in the power relations resulting from the deployment of context-aware technologies. The power of the panopticon lies in the way individuals end up modifying their activities in accordance with the expectations of their observers (*Lopes-Ostra v Spain* A 303-C (1994), *Keegan and another v UK* (2006)). As discussed previously, context-aware technologies create information asymmetries and power imbalances between the industry and the consumer. The selected cases considered here not only illustrate the scope of privacy regulation but they also illustrate the context dependent attribute of the settings when a consumer is likely to be vested with a reasonable expectation of privacy (*Campbell v Mirror Group Newspapers Ltd* (2004) §21).

### 3.3. *Conclusion*

The two regulatory frameworks considered could be seen as adopting different strategies for promoting accountability. Directive 95/46/EC could be regarded as using transparency and fair information principles to promote accountability, while Article 8 ECHR presumes that

certain information should be made transparent under strict conditions. The introduction stated that the regulatory challenge facing policymakers and the energy industry was to manage the transition into installing smart meters in homes. Responses to the Programme make it evident that the energy sector appreciated the privacy concerns – but perhaps not to the extent described in this paper. We can move the debates regarding the implementation of smart meters forward by framing the governance challenge in this way: how should we begin to reconcile the norms of opacity with those of transparency?

## 4. A hybrid model for policymaking: towards an accountable privacy management framework

### 4.1. *Overview*

Increasingly, national data protection authorities and scholars have called for industry to make its knowledge and information management practices transparent to consumers. As the CW hypothetical case illustrates, the policy framework favoured by the Government is likely to provide less rather than more safeguards to consumers' reasonable expectations of privacy. The uncertainties regarding the application of Directive 95/46/EC to biographical information that is curated through data mining techniques and the differing rationales of data protection and privacy norms are likely to raise challenges for developing industry-wide privacy management standards and securing compliance. Given that the proposals for reform in the EU Data Protection Package are unlikely to be in place before the mass-scale roll-out of smart meters, the proposed hybrid model for policymaking offers two key advantages.[74] First, it will help overcome some of the deficiencies identified in this paper through a better integration of data protection and privacy principles.[75] Second, it highlights the benefits of a responsive regulatory framework, which may help manage the transition from 'dumb meters' to 'smart meters'.[76]

### 4.2. *Hardwiring privacy principles into anticipated regulatory outcomes.*

#### 4.2.1. *Targeted substantive clarifications*

Given the scope of this paper it would not be possible to undertake a comprehensive analysis of the EU Data Protection Package proposals. It is, however, fair to say that the proposals do provide guidance in terms of likely future trends in the development of responsive privacy management protocols within businesses. There are two proposals, which will be noted, as they are relevant to the issues considered in this paper. First, Article 23 advocates the integration of PbD into governance strategies. Second, Article 33 obligates the undertaking of PIA. To ensure that data protection provisions can supplement safeguards provided by Article 8 ECHR, a number of clarifications may also be needed. First, a 'data subject' should now incorporate persons who can be identified either directly or indirectly through technological trails created from visiting websites, communication platforms or use of devices. The definition of 'personal data' needs to be widened to cover *any* information relating to a data subject. This is akin to the wide definition of 'private life' adopted by the court in *Amann v Switzerland* (2000 at §65). Processing of personal data in the age of technological convergence and 'big data', particularly in view of the growth of online profiling and behavioural tracking must be subject to regulatory oversight to prevent misuse (*Lindqvist (Approximation of laws)* (2003)). This will ensure greater complementarity in the contexts brought within the purview of data protection and privacy regulations.[77] Second, the issue of meaningful consent, which has constantly troubled policymakers and privacy

advocates, must be confronted.[78] Consent is only one of six criteria for lawful processing under Article 6(1). Under the new Regulations, processing will be lawful even if consent is not obtained, if it is in furtherance of the data controller's 'legitimate interest'. To reduce debates on what may or may not constitute a 'legitimate interest' one suggestion would be to encourage energy suppliers to adopt measures that promote accountability rather than simply require transparency. For example, the industry should be encouraged to draw attention to specific commercial interests, which override the need for prior consumer consent. Divergences in interpretations surrounding the nature of consent could be minimised by adhering to the relevant A29WP guidance on this issue, which highlights measures that should be adopted to demonstrate unambiguous consent with built-in mechanisms for highlighting accountability for the type of information being processed, their use and the process for 'opt outs'.[79] Finally, 'soft law' should be used to encourage the adoption of binding corporate rules and their incorporation into data sharing arrangements similar to those now available as between data controllers and data processors.[80]

#### 4.2.2. *A hybrid model*

It is suggested that Article 8 ECHR rather than data protection law should provide a default framework. For example, Article 8 ECHR provisions could be used to identify smart metering practices that may breach values such as respect for private life and family. Human rights provisions are sufficiently well established to enable legislators and courts to balance the interplay between Directive 95/46/EC and fundamental rights principles. A hybrid model also needs to be proactive. Rather than leave it to policymakers and legislators to resolve the privacy issues incrementally, concerns could, for example, be anticipated in advance by responsive strategies. Over the years, scholars have turned to responsive regulatory strategies as a way of building trust and ensuring accountability.[81] Responsive rather than reactive strategies may for example be relevant in guiding parties through the adoption of measures, which increase the likelihood of compliance, integrate privacy principles and do not overreach Article 8 ECHR rights. What follows is an account of those measures that should enhance greater accountability in the smart metering environment.

#### 4.2.3. *Application*

The term 'responsive' is used in the sense that institutional settings and standards can be used to advocate a process-orientated mind-set towards addressing information sensitivities and development of appropriate forms of communication and informational management frameworks. The following aspects illustrate their value in reconciling energy and privacy goals: (i) information gathering; (ii) standard setting; (iii) behaviour modification; and (iv) privacy by design. Although not exhaustive, these aspects help bridge smart meter policymaking and privacy law principles within complex organisational environments such as the energy sector.

(a) *Information gathering***.** The Consultation on data access and privacy, as noted previously, was based on the premise that disclosure of relevant information would increase transparency of industry's smart metering processes and practices. If a critical assessment of the impact of smart meters on privacy matters is to be facilitated, parties' responses must (at a bare minimum) cohere with positive rights and obligations enshrined by Article 8 ECHR principles. The ICO and A29WP could also continue to facilitate industry's practical understanding of its privacy obligations. Measures such as those put forward by

the Government, which identify circumstances when consumers' consent is mandatory is a step in the right direction.[82] Increasing transparency of smart meter information management processes will enable an objective assessment to be made by consumer organisations and policymakers if industry has obtained meaningful consent.

(b) *Standard setting*. By emphasising Directive 95/46/EC and Article 8 ECHR, businesses in the energy sector will have their attention drawn to the importance of aligning their business models with both sets of legal standards.[83] Examples of emerging opportunities for standard setting within the industry will require measures for identifying the scope of 'regulated duties', 'necessary data' and 'consent'. Unlike Directive 95/46/EC, the Programme also requires the energy sector to undertake PIAs, which will help establish appropriate base lines for mapping risks to personal information in smart metering systems (ICO 2009). We need to build on the PIA undertaken by the ENA and produce a framework for auditing privacy risks against the background of Article 8 ECHR and not simply Directive 95/46/EC.[84] Energy companies should also be required to undertake an internal audit to ensure that either consumer consent can be verified or that use of personal information is clearly prescribed by statutory authority or relevant privacy policies. In its response to the Call for Evidence, the Government provided some practical guidance outlining circumstances when collection of energy usage data will require consumer consent. In practice however, further clarification of substantive obligations (as discussed in the preceding section) will be needed, in particular the precise mechanics for 'opting out' and secondary usage.[85] Table 1 provides an illustration of how Directive 95/46/EC and Article 8 ECHR values could be integrated into an organisation's information management policies and PbD protocols.

In essence, the protocol is consistent with human right values of autonomy and self-determination, namely providing oversight in relation to data minimisation, controllability, data quality, confidentiality, transparency and use limitation (*Commission v Bavarian Lager* 2009).[86]

Table 1. A responsive hybrid regulatory model for smart meters.

| Directive 95/46/EC Art 8 & 10 ECHR, Article 29 Working Party | Regulatory role | | | |
|---|---|---|---|---|
| | Information gathering | Standard setting | Behaviour modification | Privacy by design |
| Industry | Consumer Concerns Short Trials Feedback Consent Mechanisms | Privacy Charter Smart Energy Code for Third Parties and Energy Suppliers | Energy Retail Association, Privacy Commitments that emphasise both Directive 95/46/EC and Article 8 | Programme's Data Access Group and Security Technical Expert Group |
| Civil Society | Feedback Consumer Organisations | Feedback Consumer Organisations | Feedback Consumer Organisations | Feedback Consumer Organisations |

PIAs have an important role in establishing benchmarks for assessing the scale of privacy risks when processing vast volumes of consumers' energy consumption data. Article 8 ECHR norms should provide the benchmark – the greater the intrusion, the higher the justification threshold. This is an aspect that underpinned the reasoning of the court in *Österreichischer Rundfunk & Ors (Approximation of laws* (2003) at §§68–71). Securing compliance in this context will ensure that energy suppliers continue to be responsive to the needs and concerns of their customers. One observation to be made is that standardisation of technologies and systems is regarded as invaluable to the deployment of smart metering. Standardisation initiatives and communication protocols are already being undertaken at the EU level, with ESMIG working towards the development of European standards.[87]

(c) *Behaviour modification***.** Information gathering, standard setting and consumer engagement in the shadow of the law could also be viewed as creating a process for social learning, where consumers have the opportunity to review their options; the energy sector is provided with an opportunity to adapt, experiment or develop privacy compliant measures; co-regulatory strategies could emerge with the development of industry codes of practice and ensure monitoring and identification of breaches of legal standards. It would be premature to claim that the process-orientated organisational shifts initiated by the Call for Evidence are now firmly embedded. What this discussion has illustrated is that Article 8 ECHR could provide steering mechanisms for identifying and implementing privacy and security responsive measures. This culture of reflexivity is already evident if we were to consider one outcome of the Foundation Phase – the development of a Privacy Charter as part of the overall consumer engagement and data protection consultation exercise. However Article 8 ECHR values and norms should now be used as a framework for internal reflection and external assessment of compliance through audits and consumer feedback. The industry could make explicit two additional items of information: the basis upon which interferences satisfy the strict grounds set out in Article 8 ECHR and that information collection practices do not impair the constitutional and privacy safeguards.

(d) *Privacy by Design (PbD)***.** As the hypothetical involving CW illustrates, information flows are invisible and privacy risks are pervasive. The European Commission and A29WP continue to advocate the use of PbD.[88] PbD can be viewed in a number of ways. It may be seen as a necessary response to the fact that privacy breaches may go unnoticed, that consumers may be unaware of their legal rights, lack privacy management skills and the costs of litigation. PbD can be described as a strategy for embedding 'social translucence' in technological artefacts.[89] It is an invaluable regulatory technique particularly as energy usage data can now be accessed through multiple venues, applications and devices. The Government has acknowledged that any design and licensing solution must cover not only network operators and energy suppliers but also platforms through which data can be accessed. In view of the foregoing discussion, the regulatory value of PbD lies in its role in integrating process-orientated privacy values into smart metering systems. It could also provide consumer organisations with an invaluable opportunity to visualise the information flows and industry compliance with privacy regulations.

The preceding account demonstrates the normative and institutional flexibility of privacy regulation in addressing the regulatory challenges encountered in implementing smart metering systems. This is, however, not the end of the matter. Three further comments can be made. First, much is made of consumer engagement and consumers' interests being paramount. At a practical level, there is a need to clarify the precise nature and extent of


Figure 1. An information management protocol for consumers energy usage data.

consumers' control over their energy usage data. To ensure that consumers can make informed decisions about their usage data, it is also critical that further information is provided with regard to the domains of authorised third parties who may already have extensive databases containing personal information of individuals (see Figure 1). Second, if privacy rules and norms are to continue to keep abreast of information pathologies, policymakers cannot be content in relying solely on the deliberations of stakeholders. As Schomberg correctly observes, whilst deliberative participation can lead to improved decision making, an uncritical acceptance of its value may overlook the fact that stakeholders may emphasise those elements that suit their interests and objectives.[90] Privacy Charters and Codes of Practice will need to be supplemented by detailed accounts of privacy and security risks, levels of industry compliance, and outcomes of independent audits of privacy impact assessments. The Government can provide some guidance on how best to frame privacy risks and the safeguards to be put in place before smart meters are rolled out in 2014. It is incumbent on the Government to use 'carrots' and 'sticks' to ensure that industry adheres to its privacy commitments.[91] The particular challenge for reflexive policymaking is to incentivise industry so that it will adopt responsible innovation and privacy respecting practices.[92] Finally, the adoption of some of these reflexive measures will ensure that privacy regulations can ultimately be used to steer the energy industry towards responding to societal concerns and even extend to involving the public in the product design, implementation and monitoring process so as to minimise their actual or perceived negative impact. Carefully designed compliance mechanisms and practical guidance can for example, provide anchor points for impact assessment, mutual feedback and transparent decision making processes. Fortunately for the Government it does not have to draft new standards and benchmarks for smart metering. As the Consultation on data access and privacy acknowledges, policymakers now have access to developments from other jurisdictions when determining the trade offs between facilitating innovation in electric grids on the one hand and implementing adequate safeguards protecting consumers' energy usage data on the other.

## 5. Conclusion

We cannot claim to protect the privacy rights of energy consumers without scrutinising the context in which legitimate interests and reasonable expectations of privacy subsist.

Despite the Government and industry's failure to integrate privacy respecting norms into the Programme, it is imperative that steps are now taken to minimise the adverse implications of smart meters for individuals' Convention rights. This paper has argued for a managed transition and proposed a sensible compromise that integrates both data protection and privacy norms. Looking ahead, the Programme should not be approached purely through the limited frame of data protection, contractual consent and enhanced customer support. In the long term, addressing the complex challenges posed by converging context-aware technologies through the lens of data protection principles is unlikely to address real privacy intrusions resulting from the exponential growth of 'big data'. The integration of privacy principles, coupled with effective engagement between suppliers and consumers, constant vigilance by regulators will provide a robust framework that calibrates utility and privacy issues. It should now be apparent that the governance challenge of who has access to what type of information and how it is used and for how long, is deceptively simple. Framing the right policy question and identifying strategies may help embed processes that will promote greater compliance and which will engender trust amongst the public. This paper has provided some suggestions on how the oversights in the Programme could be remedied. It also identified what could be regarded as a key privacy management issue posed by smart meters: how should Directive 95/46/EC and Article 8 ECHR confront the challenges posed by smart meters in the age of convergence and 'big data'? In both instances the answer must be that collection and use of personal identifiable data, obtained either directly or indirectly, must be made subject to unambiguous regulatory oversight. In failing to ask the right privacy management question, we should not be too surprised if Government and industry continue to remain befuddled by Judy and her family's claim that their Convention rights to privacy might have been breached. One does not need to be a privacy expert to acknowledge that protecting the social value of privacy in the smart metering environment is more than a bureaucratic process – even though Judy consented to the use of her family's data, she did not envisage decisions will continue to be taken in relation to her possible creditworthiness or that the rights of her family to peaceable enjoyment and private life would be subject to endless algorithmic profiling.

## Notes

1. Ernst & Young. 2012. Smart grid: a race worth winning? Available at http://www.ey.com/Publication/vwLUAssets/Smart_Grid-_a_race_worth_winning/$FILE/Smart%20Grid%20-%20a%20race%20worth%20winning.pdf. Pp.18-24.
2. Department of Energy and Climate Change. 2012a. Smart metering implementation programme (April update). Available at http://www.decc.gov.uk/assets/decc/11/consultation/smart-metering-imp-prog/4938-smart-metering-imp-prog-update-apr2012.pdf: para. 3.3.
3. Brynjolfsson, E., Hitt, L., and Kim, H. (2011). Strength in numbers: how does data-driven decision- making affect firm performance? Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.
4. McKinsey Global Institute. 2011. Big data: the next frontier for innovation, competition, and productivity. Available at http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation, pp. 4–11.
5. Federal Trade Commission. 2012. Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers. Available at http://www.ftc.gov/opa/2012/03/privacyframework.shtm, Bradwell, P. 2010. Private lives: a people's inquiry into personal information, p. 38 Available at http://www.demos.co.uk/files/Private_Lives_-_web.pdf; Accenture. 2011. Revealing the values of the new energy consumer, p. 32 Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Resources/Accenture_Revealing_Values_New_Energy_C onsumer.pdf.

6. Schmidt, A. 2012. Context-aware computing: context-awareness, context-aware user interfaces, and implicit interaction. In: Soegaard, M. and Dam, R.F. (eds), *Encyclopedia of human-computer interaction*. Aarhus, Denmark: The Interaction Design Foundation. Available online at http://www.interaction-design.org/encyclopedia/context-aware_computing.html.
7. Engage Consulting. 2011. Engage Consulting briefing note: smart metering implementation programme: government response to prospectus consultation.
8. Consumer Focus. 2010a. Consumer Focus response to smart metering implementation programme: data privacy and security. Available at http://www.consumerfocus.org.uk/files/2009/06/Consumer-Focus-response-to-Smart-Metering-Implementation-Programme-Data-Privacy-and-Security.pdf, pp. 4–6. House of Lords. 2009. Surveillance: citizens and the state. Select Committee on the Constitution, 2nd Report of Session 2008-09, HL Paper 18-I. London: The Stationery Office. Paragraphs 10-14. Reference should however be made to the explicit mention of Article 8 ECHR concerns in Department of Energy and Climate Change. 2011. Impact assessment: Smart Meter rollout for the domestic sector. Available at http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/1485-impact-assessment-smart-metering-implementation-p.pdf, p. 82. However, this dimension is not followed through in any meaningful detail in subsequent documents.
9. European Commission. 2012. Safeguarding privacy in a connected world – a European data protection framework for the 21st century. COM(2012) 9 final, 9.
10. European Commission. 2010. Energy 2020 a strategy for competitive, sustainable and secure energy (Communication). COM (2010) 639 final Action 3.
11. Oxford Economics. 2012. The value of smart metering to Great Britain – draft report for British Gas, p. 7.
12. Department of Energy and Climate Change. 2011a. Smart metering implementation programme: response to prospectus consultation: overview document. Available at http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/1475-smart-metering-imp-response-overview.pdf; Data access & privacy – Smart Metering Implementation Programme. 2011b. Available at http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/1477-data-access-privacy.pdf;. Impact assessment: Smart Meter rollout for the domestic sector. 2011c. Available at http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/1485-impact-assessment-smart-metering-implementation-p.pdf
13. Department of Energy and Climate Change. 2010. Smart Metering implementation programme: data privacy and security (supporting document). Available at http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/232-smart-metering-imp-data-privacy-security.pdf, pp. 6–10.
14. DECC, note 2, 2012.
15. DECC, note 12, 2011b.
16. Department of Energy and Climate Change. 2012. Smart meter rollout for the domestic sector (GB): Impact Assessment (Government response stage). Available at https://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/221-ia-smart-roll-out-domestic.pdf.
17. DECC, note 12, 2011a. 41–47. Stakeholder groups include energy suppliers (12); communications sector (10); energy services companies (8); network operators (4); consumer and campaign organizations (3); trade associations (3); academics and professional institutions (3); and regulators (2).
18. *Ibid*., p. 6, Van Elburg, H. 2008. Report on effective customer feedback mechanisms, deliverable 6, work package 2, task 2 and 3 of ESMA-Project, supported by IEE, July 2008.
19. The Data and Communications Company will now provide secure communications between energy suppliers, network operators and authorised third parties on the one hand, and compliant smart metering equipment in UK domestic premises on the other. Licensees are required to 'take all reasonable steps to ensure that it is able to comply' with ISO 27001:2005. Energy UK. 2012. Energy UK's Privacy Commitments for Smart Metering: Version 1.0. Available at http://staging.energy-uk.org.uk/publication/finish/37-smart-meter-policies/448-energy-uk-privacy-commitments-for-smart-metering.html.
20. Energy Networks Association. 2011. Privacy impact assessment: use of smart metering data by network operators. http://www.energynetworks.org/electricity/futures/smart-meters.html. Wright, D. 2011. Should privacy impact assessments be mandatory? *Communications of the ACM* 54, no. 8: 123–124; Clarke, R. 2009. Privacy impact assessment: its origins and development. *Computer Law and Security Review* 25, no. 2: 123–135.

21. Bennett, C., Charlesworth, A., Clarke, R., and Oppenheim, C. 2008. Privacy impact assessments: international experience as a basis for UK guidance. *Computer Law and Security Report* 24, no. 3: 233–242.
22. DECC, note 16, 2012: 88.
23. Information Commissioner's Office (ICO). 2009. *Privacy impact assessment handbook*, Version 2.0 (June 2009). Available at http://www.ico.gov.uk/for_organisations/topic_specific_guides/ pia_handbook.aspx.
24. McDaniel, P., and McLaughlin, S. 2009. Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, May/June 2009, p. 73.
25. IBM. 2012. Managing big data for smart grids and smart meters. 25 May, 2012: 2, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=IMW14628USEN.
26. Knyrim, R., and Trieb, G. 2011. Smart metering under EU data protection law. *International Data Privacy Law*, March 1, 2011: 121, Klopfert, F., and Wallenborn, G. 2011. Empowering consumers through smart metering. Report for BEUC. Available at http://docshare.beuc.org/Common/GetFile.asp?ID=43184&mfd=off&LogonName=GuestEN; Hargreaves, T., Nye, M., & Burgess, J. 2010. Making energy visible: a qualitative field study of how householders interact with feedback from smart energy monitors. *Energy Policy* 38: 6111–6119, Darby, S. 2006. The effectiveness of feedback on energy consumption: a review for DEFRA of the literature on metering, billing and direct displays. Available at http://www.eci.ox.ac.uk/people/darbysarah.php.
27. Turow, J. 2011. *The daily you: how the new advertising industry is defining your identity and your worth*, 18–31. New Haven, CT: Yale University Press.
28. Cohen, J. 2012. *Configuring the networked self*, 115–121. New Haven, CT: Yale University Press.
29. Eurobarometer. 2011. Special Eurobarometer 359 Survey attitudes on data protection and electronic identity in the European Union. Available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, p. 137.
30. Quinn, E. 2009. smart metering & privacy: existing law and competing policies. Report for the Colorado Public Utilities Commission, Spring 2009. Available at http://cospl.coalliance.org/fez/eserv/co:7930/reg72m562009internet.pdf, p.11.
31. European Data Protection Supervisor. 2012. Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering systems. Available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf, Para. 14-20 and 72.
32. Rheingold, H. 2002. *Smart mobs, the next social revolution*. Cambridge, MA: Perseus, pp. 84–85. This view is echoed very much by scholars such as Ling and Dourish when they point to the way embodiment not only leads to consumers failing to recognise the significance of blurring contexts and spaces but sensory capabilities possessed by technologies permit access to personal information in settings when actual physical intervention would have been previously needed: Ling, R. 2008. *New tech, new ties: how mobile communication is reshaping social cohesion*, 3. Cambridge: MA: MIT; Dourish, P. 2001. *Where the action is: the foundations of embodied interaction*, 101. Cambridge, MA: MIT.
33. Brandimarte, L., Acquisti, A., and Loewenstein, G., 2010. Misplaced confidences: privacy and the control paradox. Ninth Annual Workshop on the Economics of Information Security (WEIS). Available at http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf. Many consumers are unaware that apps installed on their smartphones and devices can access address book and other personal information automatically: Smith, E. 2010. iPhone applications & privacy issues: an analysis of application transmission of iPhone Unique Device Identifiers (UDIDs). Available at http://pskl.us/wp/wp-content/uploads/2010/09/iPhone-Applications-Privacy-Issues.pdf.
34. Office of Fair Trading. 2012. OFT calls for information about online personalised pricing practices. Published 15 November 2012. Available at http://www.oft.gov.uk/news-and-updates/press/2012/104-12#.ULi3Q4VkgXw. See also Cavoukian, A., Polonetsky, J., and Wolf, C. 2010. SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society* 3, no. 2: 275–294. Lupton, D. 2000. The embodied computer/user. In D. Bell and B. Kennedy (eds), *Cybercultures reader*, 477–488. New York: Routledge Press.

35. OfCom, Communications Market Report. 2011. Available at http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK_CMR_2011_FINAL.pdf, pp. 193–195. European Commission. 2012b. 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. European Data Protection Supervisor. 2012b. Opinion on the Communication: A comprehensive approach on personal data in the European Union. Available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.
36. Anderson, R. 2010. Consultation response on smart metering. Published 28 September 2010. Available at ww.cl.cam.ac.uk/ ~ rja14/Papers/fipr-smartmeters2010.pdf.
37. Consumer Focus. 2010b. Consumer Focus response to smart metering implementation programme: implementation strategy. Available at http://www.consumerfocus.org.uk/files/2009/06/Consumer-Focus-response-to-Smart-Metering-Implementation-Programme-Implementation-Strategy.pdf, pp. 7–9.
38. World Economic Forum. 2011. Personal data: the emergence of a new asset class. Available at http://www.weforum.org/reports/personal-data-emergence-new-asset-class, p.5, FTC, note 5 at 26.
39. Turow, note 27 at: 179–181.
40. Bennett, C. 2010. International privacy standards: can accountability ever be adequate? *Privacy Laws & Business International Newsletter* 106: 21, 21–22.
41. McDonald, M., and Cranor, L. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4: 564.
42. Nissenbaum, N. 2009. *Privacy in context: technology, policy and the integrity of social life*, 105. Stanford, CA: Stanford University Press.
43. Gellert, R., and Gutwirth, S. 2012. Beyond accountability, the return to privacy? In D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland and H. Postigo (eds), *Managing privacy through accountability*, 261–283. London: Palgrave Macmillan.
44. *Ibid*., 274. They suggest that Article 8 ECHR, unlike data protection provisions and the Privacy Charter, emphasizes opacity rather than transparency, which is the operative default rule in data protection frameworks, p. 271.
45. Danahy, J. 2009. The coming smart grid data surge. Published October 5, 2009. Available at http://www.smartgridnews.com/artman/publish/News_Blogs_News/The-Coming-Smart-Grid-Data-Surge-1247.html.
46. Rabb, C. 2012. The meaning of 'accountability' in the information privacy context. In D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland and H. Postigo (eds). *Managing privacy through accountability*, 15–17. London: Palgrave Macmillan; Regan, P. 1995. *Legislating privacy: technology, public values, and public policy*, 221. Chapel Hill: University of North Carolina Press.
47. Office of the Privacy Commissioner of Canada. 2012. Web Leakage Research Test Results. Available at http://www.priv.gc.ca/information/pub/wl_201209_e.asp.
48. EDPS, note 31, 2012: para. 27-31.
49. Austin, L. 2012. Privacy, shame, and the anxieties of identity. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2061748.
50. Hutnik, A. 2011. 3 FTC cases that could affect your mobile app. Published October 21, 2011. Available at http://mashable.com/2011/10/21/apps-ftc-settlements/. O'Reilly, L. 2012. Mobile operators agree to new app privacy rules. Published 20 February, 2012. Available at http://www.marketingweek.co.uk/news/mobile-operators-agree-to-new-app-privacy-rules/4000327.article.
51. See for example DECC 2012c: 24.
52. European Data Protection Supervisor. 2010. Opinion on promoting trust in the Information Society by fostering data protection and privacy. Available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10- 03-19_Trust_Information_Society_EN.pdf : 11-15, note 35, 2012b: para. 181, FTC, note 5 at 7-15.
53. Cohen, note 28 at 144–146.
54. Raab, note 46 at 24-29.
55. Bovens, M. 2007. Analysing and assessing accountability: a conceptual framework. *European Law Journal* 13: 447–468, 447–449.

56. European Data Protection Supervisor. 2010. Opinion on promoting trust in the Information Society by fostering data protection and privacy. Available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10- 03-19_Trust_Information_Society_EN.pdf. : para.11-15, EDPS 2011: para. 68-82.
57. It is not uncommon for contract terms to stipulate that the supplier does not have responsibility over subsequent use of information or their secondary usage. Energy suppliers may not be the only organisations who will utilise data optimising systems to integrate energy consumption history, choice of appliances and plug-in devices, visits to websites, phone calls and emails to customer services with databanks of publicly available information to profile consumers and monetise the information. See ICO, What Price Privacy Now? http://www.ico.gov.uk/news/current_topics/~/media/documents/library/Corporate/Research_and_reports/WHAT_PRICE_PRIVACY_NOW.pdf. See also the announcement by Telefónica to monetise value from its aggregated and anonymous mobile network data: http://blog.digital.telefonica.com/?press-release=telefonica-digital-thinking-things-concept-can-create-smart-m2m-connectivity-for-any-object.
58. Hon, K., Hoȑnle, J., & Millard, C. 2012. Data protection jurisdiction and cloud computing – when are cloud users and providers subject to EU data protection law? The cloud of unknowing. *International Review of Law, Computers & Technology* 26: 2–3, 134–136.
59. The ethics of digital curation may very well emerge as a principle, which ensures that certain privacy rights are non-negotiable. At present however, the application of this principle may be a difficult argument to run, given that consumers can 'opt-out' from installing smart meters in their homes. British Gas, Customer Charter (Summary version). The occupants living in Cosgrove Way may claim their 'right to be left alone' but at present the Programme provides no credible response the questions raised above. Customers are advised to read the full terms at britishgas.co.uk/termsandconditions. A good example would portals like Oopower that encourage consumers to provide information regarding the energy practices and appliances used in the home.
60. Cohen, note 28 at 150.
61. Organisation for Economic Cooperation and Development. 1980. OECD guidelines governing the protection of privacy and transborder flows of personal data. Available at http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
62. Article 29 Data Protection Working Party. 2011a. Opinion 15/2011 Consent WP187. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. It widens the scope of the concept.
63. For ease of reading the relevant Opinion issued by A29WP will be stated in numerals.
64. Directive 95/46/EC Article 2(a), A29WP. 2011b. Opinion 12/2011 on smart metering WP 183. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf 183: 6–8.
65. *Ibid*,. A29WP. 2011b. 8–10.
66. See also A29WP. 2009. The future of privacy: joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data WP168. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.
67. De Hert, P. and Gutwirth, S. 2009. Data protection in the Case Law of Strasbourg and Luxembourg: constitutionalization in action. In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne and S. Nouwt (eds), *Reinventing data protection*?, 8. Berlin: Springer.
68. A29WP. 2007. Opinion No 4/2007 on the concept of personal data WP 136. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf A29WP (2010).Opinion 3/2010 on the principle of accountability WP173. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.
69. See for example A29WP, *ibid*,. 2010 173: 10-15 and note 62, 2011a 187: 11–12.
70. See A29WP 2010: 3–4 and Vyas, D. 2011. On the record: energy suppliers and credit reference information. Consumer Focus. Available at http://www.consumerfocus.org.uk/files/2011/10/Consumer-Focus-On-the-record.pdf.
71. De Hert and Gutwith, note 67 at 15–20.
72. Article 8(2) ECHR provides 'There shall be no interference by a public authority with the exercise of this right except such as is 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'.

73. Cuijpers, C., and Koops, B-J. 2013. Smart metering and privacy in Europe: lessons from the Dutch case. In S. Gutwirth, R. Leenes, P. de Hert, and Y. Poullet (eds). *European data protection: coming of age*, 269–293. Berlin: Springer.
74. See UK government's recent Impact Assessment of the draft European data protection regulation published on 22 November 2012. Available at https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf
75. Even though 'command and control' regulations possess virtues of high dependability and predictability, this technique lacks the subtlety in managing polycentric public policy issues. The shortcomings of a centralised approach to rule enforcement and compliance are particularly acute in areas of public policy that are challenged by the scale and rapid nature of technological advances. Complex systems and networks continue to challenge traditional command and control strategies – smart meters now join the list of the 'Internet of things' that present society with a Faustian bargain.
76. Responsive governance may help address 'regulatory deficits' in situations where consumers do not take advantage of the protections provided by the law owing to their lack of information or understanding of how best to manage their exposure to particular risks or exploitative practices. Responsive governance has also been seen as a strategy designed to offset the problems of market failure, 'regulatory creep', the State's lack of resources and expertise and the need to keep pace with technological developments. Consequently, as Foucault reminds us, holding on to the trenchant ideology of 'constraining' or 'controlling' architectures is deceptive and an oversimplification of policymaking.
77. See EDRI '(3a) "profiling" means any form of automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour: http://protectmydata.eu/articles/articles-1-10/article-4/.
78. Eurobarometer 2012, A29WP, note 62 (2011a): 7.
79. See A29WP, note 62 (2011a).
80. A29WP. (2012). Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules 00930/12/EN WP 195. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.
81. Responsive governance can be described as a strategy where organisational behaviour and policies are steered towards ensuring that technology push measures do not undermine consumers' privacy and safeguards to their energy usage data. Some of its key elements include collaboration in problem-solving, engagement and responding to public opinion and concerns.
82. DECC, note 2, 2012a para. 3.3.
83. *Ibid*., para. 4.7–4.15, 4.20–4.25.
84. A PIA does not necessarily mean that the parties have complied with their privacy obligations.
85. DECC, note 2, 2012a: para. 4.17
86. A29WP, note 66, 2009, 168: 14–15, De Hert and Gutwirth, note 67 at 39–42.
87. See the mandate initiated by European Commission and accepted by CEN, CENELEC and ETSI, available at http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf.
88. A29WP, note 66, 2009, 168: 53.
89. Erickson, T., and Kellogg, W. 2000. Social translucence: an approach to designing systems that support social processes. *Transactions on Computer-Human Interaction* 7: 59–83.
90. Von Schomberg, R. 2011. Prospects for technology assessment in a framework of responsible research and innovation. In M. Dusseldorp and R. Beecroft (Eds). *Technikfolgen abscha?tzen lehren: Bildungspotenziale transdisziplina?rer Methoden*, 39–61. Wiesbaden: Vs Verlag.
91. Culnan, M. 2000. Protecting privacy online: is self-regulation working? *Journal of Public Policy & Marketing* 19: 20–26.
92. The European Data Protection Supervisor has recently provided policymakers and Governments with recommendations, which lend specificity to the measures that enable industry to address and implement its privacy obligations: EDPS, note 31, 2012a. See also its emphasis on practical governance: EDPS, note 35, 2012b and EDPS, note 52. European Data Protection Supervisor. 2010.

Opinion on promoting trust in the Information Society by fostering data protection and privacy. Available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10- 03-19_Trust_Information_Society_EN.pdf.

## Bibliography

*Amann v Switzerland* [2000] ECHR 88.
*Botta v Italy* (1998) 26 EHRR 241.
*Campbell v Mirror Group Newspapers* [2002] EWHC 499 (QB).
*Commission v Bavarian Lager* [2007] EUECJ T-194/04, [2009] EUECJ C-28/08_O.
*Copland v United Kingdom* [2007] IP & T 600.
*Douglas v Hello Ltd* [2005] EWCA Civ 595.
*Durant v FSA* [2003] EWCA Civ 1746.
European Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. 2010. A comprehensive approach on personal data protection in the European Union. COM(2010) 609 final.
*Evans v UK* (2006) 43 EHRR 21.
GMSA. 2012. Privacy design guidelines for mobile application development. Available at http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf.
*Halford v United Kingdom* [1997] ECHR 32.
*Heglas v Czech Republic* (2009) 48 EHRR 1018.
Huang [2007] UKHL 11.
IEE. 2011. The costs and benefits of smart meters for residential customers. Available at http://www.smartgridnews.com/artman/uploads/1/IEE_Benefits_of_Smart_Meters_Final.pdf.
*Keegan and another v United Kingdom* [2006] All ER 235.
*Kruslin v France* (1990) 12 EHRR 546.
*Kyllo v. United States* (2001) 533 US 27, 38.
*Liberty v United Kingdom* (2009) 48 EHRR 1.
Lindqvist (Approximation of laws) [2003] ECR I-12971.
*Lopes-Ostra v Spain* A 303-C (1994), EctHR.
*Malone v United Kingdom* (1984) 7 EHRR 14.
*Murray v Express Newspapers plc* [2007] EWHC 1908 (Ch).
Österreichischer Rundfunk & Ors (Approximation of laws) [2003] EUECJ C-138/01.
*Peck v UK* (2003) 36 EHRR 41.
*Perry v UK* (2004) 39 EHRR 76.
*Pretty v UK* [2002] ECHR 427.
*R (on the application of the Department of Health) v Information Commissioner* [2011] EWHC 1430 (Admin).
*S and Marper v United Kingdom* 30562/04 and 30566/04 [[2008] ECHR 1581.
*Shimovolos v Russia* (Application no 30194/09) (2011) ECHR First Section.
*Smith and Grady v UK* (1999) 29 EHRR 493.
*Von Hannover v Germany* [2004] ECHR 294.
*Z v Finland*, judgment of 25 February 1997, Reports of judgments and Decisions 1997-I 10.