Regulating intersectional industries: the feasibility of balancing privacy and energy efficiency

Abbe Brown[a] and Rónán Kennedy[b]

[a]*School of Law, University of Aberdeen, Old Aberdeen AB24 3UB;* [b]*School of Law, National University of Ireland Galway*, *Galway, Ireland*. *(Received 20 June 2017)* [*]

Abstract

Using a case study, this article explores the extent to which one area of law (privacy and data protection) can intersect with, and be challenged by, proposals by delivery of another goal – greater energy efficiency. The article then explores the extent to which these fields are becoming more integrated; and also the risks of relying on technology (notably through Privacy by Design) to do this, particularly given the uncertainties embraced by lawyers and which can be problematic to technologies. Having identified challenges in meeting both energy efficiency and privacy/data protection goals at the same time, the article develops two responses. One looks more widely in law, to competition, to prevent particular activity and to confirm the relevance of greater legal interdisciplinarity. The other is a more multi-faceted collaborative governance approach, involving legal and technical expertise and consumer perspectives, with standards having a valuable role. Addressing climate change should be an appropriate motivation to bring about this second approach, which draws on wider environmental governance developments. With largely a UK and EU focus, but seeking to be of transnational relevance, the article makes key contributions as to the capacity and limits of how law can address societal challenges; explores the risks of assuming that social and legal problems can be readily addressed by technology; confirms the need for lawyers to look to other fields of law; and assists progress in an increasingly intersectional and dynamic field.

Keywords: privacy, smart grids, energy efficiency, data protection, PbD, competition, regulation, intersections, standards

Acknowledgements

The London workshop upon which this article builds was kindly funded by the British and Irish Law Education and Technology Association 2015-16.

[*] Corresponding author Abbe Brown abbe.brown@abdn.ac.uk. Authors are listed in alphabetical order.

Regulating intersectional activity: privacy and energy efficiency, laws and technology

Contextualising a case study

Different fields of law may have different objectives, may conflict in some contexts, and may choose different ways of delivering their objectives. Furthermore, these laws exist alongside other disciplines – for the particular context of this article, most notably information and communications technology (ICT), and its capacity to facilitate the delivery of particular types of policy aims. With a focus on energy efficiency through infrastructure and privacy, this paper explores the intersection between legal fields, the increasingly dynamic intersection between law and sophisticated and complex technologies, and the complex challenges which that intersection creates for arriving at ultimate goals. Using a case study as a framing device, it explores the extent to which different areas of law, and their distinct approaches to technology and to the delivery of privacy, could provide barriers to or enhance the potential use which can be made of technology to deliver a goal. The paper explores legal and regulatory approaches to climate change through energy efficiency and infrastructure, to privacy and data protection, and also to competition law, in the context of the ultimate policy aim of making a positive contribution to reducing greenhouse gas emissions and thus mitigating climate change. There will be consideration of the substantive detail of each area of law and technology, and reference made to the different enforcement frameworks of different areas of law. Having done this, the aim and contribution of the paper is to highlight the necessity and opportunity for lawmakers and regulators to look outside their disciplinary silos to wider laws and to technologies; the risks of assuming the answer can lie in simply turning the problem over to technology; the related risks of not engaging with other laws and of the opportunities which other laws can provide for solving one problem but not all; and of the potential for disconnections between technologists and lawyers, as software developers and engineers struggle to engage with the uncertainty which can sit at the heart of laws and legal intersections in particular contexts. To address this, the paper proposes two ways forward: first, a legal solution to a specific problem identified; and second, a new deliberately fragmented and standards-related dialogue in which lawyers, policymakers and technologists can engage and operate more effectively towards holistic,

workable regulatory solutions. The discussion focuses on the UK countries and the EU, but draws on developments in other countries when appropriate, and seeks to develop a solution which could work transnationally.

Case study

First, an introduction to the (hypothetical) case study:

> A company which owns a small estate in the West Highlands of Scotland is looking to generate a new revenue source. It harvests an established set of trees planted a few decades ago for use in a wood fueled heating business which it recently launched, using well established boilers and other biogas related delivery products. The Scottish Company is then purchased by a large international energy company. The international Company drills in the UK Continental Shelf in the North Sea for oil and gas, and wants to support the Scottish Company to assist the reputation of the wider group in the low carbon energy sector. The Scottish Company also decides to make their boilers 'smarter', so that they can contribute to Smart City initiatives taking place across Scotland. The Scottish Company is excited that it can take advantage of the expertise of the energy company which has developed a subsea smartgrid, in respect of some key smart technology in the UK. The technology enables all information which has ever passed through smart boilers, from which individuals can be identified by name and address with no other details, to be recorded and profiled accorded to criteria and then sold on to other businesses for use in the EU and elsewhere in their product development. The technology quickly became entrenched within efforts to ensure more managed use of energy. The international Company is pleased to have been invited to meet with an energy standards body.

The case study is complex, but not unrealistic; it combines a range of actual events and possibilities. The events and decisions outlined occur within a complex policy and legal environment, which is changing in response to marketplace activity, scientific and technical knowledge, and societal attitudes. Readers from different disciplines (or different regulators) could view the case study from different perspectives, for example with a primary focus on privacy or competition; with a focus on technology; or, like the Scottish company, with a focus on making money from available resources. Wherever one starts, it involves the potential tension between objectives and perspectives and raises the question of the extent to which competing priorities can be addressed effectively through an intersectional approach to legal and technical solutions.

Here, the case study will be discussed from the starting point of delivering greater energy efficiency, so that greenhouse gas emissions from power generation can be reduced. The paper will then discuss the case study from the perspective of privacy (including data protection and information security); and in so doing highlight the challenges involved in implementing “Privacy by Design” (PbD), which may mean that this particular regulatory approach will ultimately fail in its goals. The paper will connect this discussion to the possibility of intervention by competition law regulators in the case study, in seeking to prevent privacy-related abuses of a dominant position through the passing on of information. The paper concludes by building on the standards mentioned in the case study to examine how the problems raised could be addressed, with transnational impact, by a deeper engagement between lawyers and technologists, with much greater two-way dialogue than has been the case in the past.

Firstly, the policy, legal and techno-social context will be introduced.

Policy, legal and techno-social starting point: Climate change and energy efficiency

The case study can be seen as an effort to reduce greenhouse gas emissions through the use of a (fairly) renewable energy source (trees for biomass heating), and the enhancing of energy efficiency through the particular smart grid technology which has become so accepted in the industry. In addressing climate change, a key development was the United Nations Framework Convention on Climate Change (UNFCCC),[1] one of the outputs of the Rio Earth Summit of 1992. The UNFCCC seeks to reduce greenhouse gas emissions. The UNFCCC led to a significant body of outputs and associated meetings, with those at Kyoto in 1997 (leading to reduction of emissions targets being agreed by some countries),[2] Copenhagen in 2009 (which failed to lead to new targets being agreed but created a new pathway),[3] and Paris in 2015[4] (which did lead to new targets, with a deliberately limited approach to enforcement)[5] being the most well-known. Across these meetings, there has been growing attention paid to the importance of technology in addressing climate change, notably through the establishment of the Technology Mechanism; this activity includes smart grids (Patt 2015; Sarnoff 2016; UNFCCC 2017; UNFCCC 2015; also discussion in TRIPS Council 2017).

The UK and the EU are all parties to the UNFCCC. The EU has taken a multifaceted approach to responding to climate change (European Commission 2017a) and one key element is energy efficiency (European Commission 2017b); consider, for example, the EU's third energy package (European Commission 2017c) and the Directive on Energy Efficiency.[6] Within the UK, climate change is an issue which has been devolved, and so the legal context of both Scotland and the UK must be explored. Scotland's 2017 Climate Change Plan seeks to deliver transformative change with a focus on energy efficiency; and again reflecting elements of the case study, the 2017 plan makes repeated references to smart grids and technologies (Scottish Government 2017, paras 2.2.4, 7.2.2, 7.4.1, 8.3, tables 7.2, 8.1, 8-9, 9-21,10-9 and delivery of policy milestones 1 and 2). Indeed, the Scottish Enterprise Smart Grid Sector strategy aims to grow the sector and deliver 12,000 jobs by 2020 (Scottish Enterprise 2017, 7); and industry events stress the opportunities which smart grids can offer for more affordable energy (McKay Hannah 2016). For example, in September 2015 it was reported that Vodafone had signed a £75 million deal with Scottish Power to connect cables to a smart grid (Palmer 2016). There is also to be a new Scottish climate change bill in 2017 (Scottish Government 2017, in particular ch 2 and box 2.1 regarding bill). The call for evidence for this discusses energy efficiency (Scottish Climate Change Bill 2017 - Call for Evidence December 2016)**.** Finally, smart technology is a focus at UK level, as can be seen from the "Smart Power" report of the National Infrastructure Commission (National Infrastructure Commission 2016) and the Queen's Speech of 2017 refers to a Smart Meter Bill to deliver more transparent energy bills and allow use to be monitored.[7]

In addition to the new energy source and the smart technologies, contributing to one means of addressing climate change action through infrastructure to enhance energy efficiency, the case study also raises questions of information security and privacy. These will now be introduced.

Techno-social context: the 'Internet of Things'

To do this, it is necessary to understand what enables new information-based markets and activity. The ability of the Company's smart grid technology to record information and profile its users so that data can be resold, is an example of the application of the so-called 'Internet of Things' (IoT). The IoT creates the potential for very fine-grained tracking and profiling of individual consumers in their most private spaces. As networked micro-processors become smaller and cheaper, and the convenience and capacity for rapid responses which they offer when embedded in everyday items becomes clearer, more and more of the items that we interact with on a daily basis now contain tiny computers, connected together in the IoT. This is difficult to clearly define but includes aspects of information and analysis, and automation and control, with four main elements:

1. sensors, to allow an object to detect its physical environment;
2. communicative chips (such as Radio Frequency Identification Chips), to allow the object to communicate information relating to its senses, and to receive instructions from external or remote sources;
3. computers (or servers), which can aggregate and process the information coming from these objects and return commands; and

4. the Internet, to connect the objects with the servers (Westbrook and Taylor 2013, 244–245, citing Chui, Löffler, and Roberts 2010).

IoT devices have many applications in energy efficiency and smart grids, such as through 'smart' thermostats, 'intelligent' appliances, hybrid and electrical vehicles, distributed electricity generation and storage, security systems, automation, and energy management systems, all with an ultimate goal of dynamic and responsive two-way energy markets in which consumers are also suppliers (Collier 2017). These IoT devices are hubs for information flow in and out of the home, something which consumers will not readily understand and will also quickly forget (Peppet 2014, 108–111, citing Murrill, Liu and Thompson 2012). Further, information on energy use allows for detailed profiling of the lifestyle and habits of an individual (Cavoukian, Polonetsky, and Wolf 2010, 284), as in the case study.

Other policy and techno-social perspectives: information security

Within the IoT, consumer information being profiled, recorded and stored, or accessed without authorisation, can create information security risks. For example, hackers may wish to track the movements of an individual, perhaps in order to determine when they are away from home and thus a good target for burglary (Hoerter, Feyel, and Awad 2015, 296). Indeed, IoT enabled devices are particularly vulnerable because characteristics of the IoT marketplace make them very likely to be insecure: IoT devices are developed by consumer electronics firms, without significant expertise in security at least from the perspective of personal information; the IoT devices are required to be small and use little power (leaving no capacity for security measures); and are not designed to be updated after installation (Peppet 2014, 135). Yet given that they are connected to the Internet, IoT devices can be remotely accessed, modified, and thus hacked. In addition, devices can leak information or be engaging in unauthorised monitoring. Perhaps the most notorious example of this is Samsung's 'Smart TV', whose voice recognition software was, in fact, recording all conversations in its vicinity without notice to users (although there is no evidence that Samsung was doing anything untoward with the information thus collected) (Higgins 2015). In addition, software developers, particularly those working on Web 2.0 applications, apply so-called 'dark patterns' which encourage consumers to provide more information than is necessary to use a particular service for longer than is needed (Bösch et al. 2016) – possibly for the same reasons as those explored in the case study**.**

Accordingly, it has been seen that the scientific and policy context for the case study creates conditions favourable to the development of smart grid technology. The scientific and policy context does not appear, however, adequately to protect the interest of the consumer in protecting information about them. This suggests a need for rapid regulatory responses. Before assessing the form which these might take, it is important to explore more deeply a key issue raised by the IoT and its application for energy efficiency: the challenge to privacy.

"Privacy"

As van Rest and others point out,

> ... the concept is often used without clear definition, and commercial organisations therefore apply it in different ways in practice. … For designers, a checklist would be quite a useful tool, but unfortunately 'privacy' is a complex, multi-faceted topic, which is not very amenable to a reductive approach (van Rest at al 2012, 56–59).

The concept means different things in different legal cultures: Koops et al (2017) survey nine jurisdictions (including the UK) and identify eight basic types of privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioral privacy), together with an overlapping category of informational privacy. Most relevant to the case study activities is the US approach to privacy which traditionally focused on the so-called 'right to be left alone' (Brandeis and Warren 1890); the notion of privacy as based in autonomy and the right to decide for oneself (Bernal 2014); and also that of privacy as empowerment, for example in choosing to commoditise information (Lynskey 2015, 243).

The conceptual confusion relating to privacy increases when law is translated to other disciplines and domains. For example, writing from a legal theory perspective, Carolan and Delaney categorise privacy into three dimensions: *decisional*, *spatial*, or *informational*, each of which operates in specific contexts (Delany and Carolan 2008, 21). This can be compared with the summary of 'prominent approaches to privacy within computer science' which Gürses provides: *confidentiality* (limiting exposure), *control* (managing communication), and *practice* (ongoing social negotiation) (Gürses 2014, 21–23); both approaches, however, can be of relevance to the case study.

Reflecting this connection, these understandings are not completely irreconcilable, but this does not mean that translating legal requirements into IoT standards (as the case study demands) is straightforward. Informational privacy can be connected to privacy as control. However, the ease with which digital information can be duplicated and distributed means that implementing and verifying privacy rules in practice is a significant challenge. Spatial privacy can be connected to privacy as confidentiality. Nonetheless, the law tends to assume that it is managing real, local, and easily defined areas, whereas in the context of electronic communications, privacy must be managed in virtual, geographically disparate, and temporally dynamic environments. Meshing legal and technological research agendas for privacy is therefore difficult. Decisional privacy can be connected to privacy as practice. These are probably the most complex and nuanced approaches to the concept, and it is interesting to note that Delaney and Carolan regard decisional privacy as particularly problematic from a definitional and legal perspective**.**

In response to this confusion, it is interesting to note that Nissenbaum suggests that we should think about privacy in a more contextualised fashion, giving more weight to the different social norms and values that apply in, for example, the work life, home life, and social life, calling this 'privacy as contextual integrity' (Nissenbaum 2010). Further, Toy has synthesised the fundamental ideas from a variety of international frameworks and proposes seven new privacy principles which he claims are more appropriate to the increasingly technological age in which we find ourselves: privacy by design, respect for context, consent, transparency, legitimacy, proportionality, and accountability (Toy 2013, 948). Building on these points and of key

relevance here, Matzner (writing with particular reference to 'ubiquitous' or 'pervasive' computing and smart grids) argues that the widespread use of sensors in an IoT context (as applies in the case study), and challenges fundamental assumptions about the privacy of particular spaces (such as the home or the street) and blurs the distinction between public and private information. He therefore proposes extending Nissenbaum's perspective with an explicitly political and social dimension, while acknowledging that some technical fixes may be possible (Matzner 2014).

Viewing the case study, particularly the extensive capture and repurposing of quite personal data, through this normative lens raises troubling questions: customer information is circulated without regard to individual integrity as explored by Nissenbaum, many of Toy's principles are not complied with, and the orientation of the project is towards what some call 'surveillance capitalism' (Zuboff 2015). Against this complex theoretical base, and in response to the types of technological development outlined in the case study, there are legal frameworks pursuing privacy-related goals (for a deep discussion, with a focus on smart cities and the EU, see Edwards 2016). Firstly, given the geographical focus of this paper, key from the human rights perspective are the EU Charter's right to private and family life and to data protection,[8] and the ECHR right to private life. [9] There is no specific UK legislation on privacy (as opposed to data protection, which is discussed below). Courts have, however, used the obligations imposed on courts pursuant to the Human Rights Act 1998 and the article 8 ECHR right, in conjunction with established case law on breach of confidence, to develop what became an entrenched action for misuse of private information against another individual or company. This cause of action has been used largely in the context of the activities of celebrities and their children.[10] It could apply more widely to the case study activity, depending on the understandings of consumers about what would be done with their information, and with whom they deal in this respect (eg the Scottish Company or another business). For misuse of private information, there must be a reasonable expectation of privacy, which is then balanced against the right to freedom of expression. There is also continuing scope for regard to be had to the public interest in disclosure of information. This draws on breach of confidence decisions (notably *Lion Laboratories*[11] which deal with whether the public interest in knowing whether or not breathalysers were functioning properly was sufficient to defend an action for breach of confidence). Could disclosure of information about an individual be considered a relevant price to pay for greater energy efficiency? The action for misuse of private information can ultimately lead to an injunction and financial compensation arising from the damage suffered through the misuse of information.

Data protection law can also be relevant to privacy, broadly termed. At the time of writing (mid-2017), approaches to it in the UK lie in national data protection legislation[12] implementing the Data Protection Directive of 1996.[13] This imposes obligations on those who control or process (including use, re-use and disclose) information as part of a relevant filing system from which (any) person can be identified. This would cover the activities in the case study – again depending on how uses of the technology progress, in respect of conduct by the Scottish Company and by other businesses. Key provisions in the UK legislation are that the personal information is to be processed in accordance with data protection principles: used fairly and lawfully, for limited specific purposes in a manner which is not excessive, kept for no longer than necessary and safe and secure in the light of the harm which arises from loss or unauthorized dealings with it, and also that personal information should not be passed outside the EU unless the destination country has appropriate data protection provisions; further, personal information is not to be held and processed unless there is consent (explicit consent in respect of sensitive data such as relating to health or religion although the case study indicates that this is not relevant here) – or if processing is necessary for the legitimate interests of the data controller or parties to whom personal information disclosed save if this is unwarranted in the light of the rights of the data subject.[14] The narrow focus of the final base would not likely support an argument that the selling on of the personal information would assist in developing more energy efficient products and assist in general action against climate change, as the impact is likely too remote. Key then is consent and, as with the privacy cause of action, what information was provided, about how personal information would be dealt with. The case study provides no indications that this is being done. Further, the discussion of technology above suggests that there might also be information security questions, which again raise data protection problems.

More issues will arise when the EU General Data Protection Regulation 2016 ("GDPR")[15] applies from May 2018. Themes will continue from the previous regime;[16] however the key difference is that the GDPR requires that dealings with any personal information are (broadly) to be on the basis of clear, affirmative, specific informed and unambiguous indication of consent.[17] There may be processing without consent if it is necessary for the performance of a task carried out in the public interest for purposes of legitimate interests (unless these are overridden by the rights of the data subject).[18] From the information available in the case study and in the light of the points made above, the requirements again this may not be met here. More generally the focus on affirmative and specific consent will require substantial reform to many data management practices in the EU. In the context of Brexit uncertainty, there was the prospect that the GDPR will only have a short period of direct relevance in the UK. It appeared likely, however, because of the commercial importance of being able to deal with the EU for digital economy businesses, and of the EU's requirements regarding the protection provided by other states, that substantive data protection approaches in the UK would remain similar to those in the EU (McCullagh 2017). And indeed, the 2017 Queen's Speech includes a Data Protection Bill which will implement the GDPR in respect of the UK's membership of the EU and also thereafter.[19] Accordingly, all providers of technology, considering activity in any country, should be aware of the deep base required for dealings with personal information. In this respect, the draft 2017 guidance of the UK Information Commissioner regarding consent, and the short consultation on it, are of interest (Information Commissioner's Office 2017a).

Looking outside the case study details, it is also interesting to reflect that even if there is a privacy policy which does provide details of what will be done with personal information and a means of providing consent, an individual may still be faced with a choice between accepting the IoT smart meter or appliance or going without electricity and returning an expensive household device to the vendor. This is arguably not a real choice. More generally, it has been noted that even if there are these policies or agreements to inform consent, consumers may not be able to access them (as IoT devices often do not have good display systems); and if they can read them, they may find them difficult to clearly understand (Peppet 2014, 140–146). The practical reality, in many instances, is that devices will be installed in homes with minimal explanation to users, or with one person consenting for all residents, considerably vitiating any notion of "freely given, specific, informed" consent as will be required under the GDPR.[20] The rollout of smart grids, therefore, are likely to involve possible contraventions of data protection law (see Edwards 2016, for discussion of new approaches to address this such as sticky consent and indeed the appropriateness of a consent based approach with a EU focus).

Of greater relevance to this paper, however, is that the discussion so far suggests that privacy, broadly termed, and energy efficiency through infrastructure, are domains of regulatory activity which are closely connected; in practice, however, they may be being dealt with rather separately. There have been some attempts (in both fields) to explore their intersection. The next section discusses this and considers whether this has been done adequately and effectively.

Energy efficiency and privacy alignments

Firstly, it is surprising, and disappointing, that Scotland's 2017 Climate Change Plan (discussed above in the context of smart grids), does not engage with privacy. Likewise, that the Scottish Enterprise Smart Grid Sector strategy notes that key opportunities include data acquisition, monitoring and analysis, without engaging in depth with how noted privacy issues are to be addressed (Scottish Enterprise 2017, 8, 9,18). This should be contrasted with the approach of the Netherlands Parliament which, when considering smart grid arrangements, found that regard to data protection through an impact assessment was not adequate, and there needed also to be regard to ECHR article 8 rights. This led to the proposed arrangement ultimately being introduced on a voluntary basis (Cuijpers and Koops 2014).[21] Another example of the connection being better addressed is the California Utility Commission, which passed a decision in 2011 to protect privacy of information (using the term widely in a context which would cover both privacy and data protection as discussed above) relating to smart grids (California Utility Commission 2011 and discussion in Edwards 2016).

At UK level, the Smart Power report also does not refer to privacy (National Infrastructure Commission 2016), nor does the Queen's Speech in respect of smart grids – although its other engagement with data protection has been noted. The relevance of privacy to smart grids was recognized, however, by the UK Gas and Energy Markets Authority in 2010. This published a strategy for data privacy and security which provided that the UK data protection legislation will be followed (Office of Gas and Electricity Markets 2010). A data access and privacy framework was established in 2012 (Department of Energy and Climate Change 2012) and in 2013 there

was the Smart Energy Code, an agreement regarding those involved in end to end management of smart metering, which refers to protection of data and security. A Smart Grid Vision and Roadmap was established in 2014 by the Department of Energy and Climate Change[22] (Department of Energy and Climate Change and Office of Gas and Electricity Markets 2014). This includes several references to enabling access to data while respecting consumer privacy, calling for a proportionate approach, data aggregation and working with the EU to pursue standards (Department of Energy and Climate Change and Office of Gas and Electricity Markets 2014, paras 27, 49, 50 and 58); it also refers for example to the work of the Energy Networks Association on data technologies to address privacy requirements (Department of Energy and Climate Change and Office of Gas and Electricity Markets 2014, para 36). This regard continues, for example in the Report of the House of Commons Energy and Climate Change Committee 2016.

At EU level, the 2012 Commission recommendation on roll out of smart meters refers to data protection and privacy legislation, a focus on privacy enhancing technologies (including those which are best available) and a movement to certification marks for these, and a focus on secure communications with regard to privacy and data protection (European Commission 2012, recitals 7 and 13, articles 3(f), 15, 42(h)). The EU's third energy package (European Commission 2017c), particularly the Directive on Energy Efficiency[23] refers to smart and intelligent metering (and to their limited achievements)[24] in previous electricity[25] and natural gas[26] Directives. Importantly this requires that intelligent metering systems have security which complies with data protection and privacy legislation,[27] but also that information is to be disclosed of consumption and profiles.[28] A 2014 Commission staff working document reviews different steps taken by countries on state of play and cost benefit analysis, exploring privacy and data handling (European Commission 2014a, paras 3.3, 3.4, and summary penultimate paragraph). Data protection, privacy and security are strongly visible in the European Commission's 2017 activities regarding smart grids and meters (European Commission 2017d]). It is sobering, however, to note that in the EU Sustainable Energy Week conference 2016 (European Sustainable Energy Week (2017)), there was no session on privacy or data protection.

The connections between energy efficiency and data protection, privacy and security are also reflected in the work of data protection bodies. There is the opinion of the Article 29 Working Party (12/2011) on smart metering (Article 29 Data Protection Working Party 2011) which refers to EU energy efficiency laws, a survey of national data protection authorities and calls for strong engagement between energy providers and data protection authorities. While noting the benefits of the activity for energy efficiency, the opinion considers that smart metering can raise data protection and fundamental privacy questions, and calls for more information to bring about informed consent. Further, and interestingly in the light of the points made above regarding bases for use of data including under the GDPR, the opinion notes the possibility that reduction of electricity use could be in the public interest and a legitimate use of personal information including by those to whom the information is passed on. The opinion considers, however, that this will not invariably be so, and that technologies and assessments will be key to this (Article 29 Data Protection Working Party 2011, 14).

There are also examples of more direct engagement with the connection question from both sides. An Article 29 Working Party opinion was prepared (7/2013) regarding the data protection impact assessment proposal prepared by the European Commission's Smart Grid Task Force (Article 29 Data Protection Working Party 2013). This engages in particular with approaches to privacy targets and to risk management and compliance. The opinion was followed by a Commission Recommendation (European Commission 2014b), which notes that the template for data protection impact assessment should

> not only facilitate the resolution of emerging data protection, privacy and security issues in the smart grid environment, but also contribute to addressing data handling linked to the development of the retail energy market. Indeed, an important part of value in the future retail market will stem from data and wider integration of ICT into the energy system. The collection and organisation of access to the data are key to the creation of business opportunities for newcomers, especially aggregates, energy service companies or the ICT branch. Data protection, privacy and security will therefore become increasingly important issues for utilities to handle. The Template will help ensure, especially in the initial phase of the roll-out of smart meters, that smart metering system developments are monitored and that fundamental rights and freedoms of individuals are respected, by identifying data protection risks in smart grid developments from the start. (recital 19).

The recommendation calls for states to encourage use of the template, to take into account Article 29 Working Party opinions and for multi-stakeholder consultation regarding implementation (arts 3 and 4); for exploration of use of best available techniques as a complement to data protection assessments (art 5); and for there to be a testing phase (Section IV and note also European Commission 2017e).

Likewise at UK level, in 2016 the Department of Energy & Industrial Strategy (which has taken over from the Department of Energy and Climate Change ("DECC")) launched a consultation on a "Smart, Flexible Energy System". This refers to consent, privacy frameworks, the need to have informed consumers and information security (Department of Energy & Industrial Strategy 2016, 15, 68, 69, 83). The UK Information Commissioner responded to this, stressing the importance of specific and transparent consent and the importance of security (Information Commissioner's Office 2017b).

Yet although there are these intersections across energy efficiency and privacy (broadly termed), an opportunity for greater integration was missed. An EU Recommendation (European Commission 2014b) referred to articles 7 and 8 of the EU Charter discussed above (relating to privacy and data protection); it did not, however, reference article 37 of the EU Charter - which provides that a high level of environmental protection is to be integrated into the policies of the Union and ensured in accordance with principles of sustainable development.[29] Although there is a reference to this right in a recital to a 2014 European Parliament resolution on the local and regional consequences of smart grids (European Parliament 2014), engagement with this human rights based justification for smart grids should have a much greater part in legislation and policymaking. This would not of course mean that this would

necessarily prevail over the privacy and data protection rights; but it would provide a deep and present base for legal intersection, including regarding provision of a base for use other than through consent (through the public interest), and a firmer base for the arguments being developed in this paper.

This paper also seeks, however, to look beyond identifying and exploring these two (indeed three including human rights) areas of law and areas for combination. First, if the technology discussed in the case study is creating privacy problems, as is likely with IoT devices, might one also look to technology to solve the problems? This is the approach of "Privacy by Design" (PbD), "Privacy by Default" or "Privacy by Re-Design" (PbRD) (see, for example, Cavoukian, Polonetsky, and Wolf [2010]; Hoerter, Feyel, and Awad [2015]); Kitchin [2016, 7.3.2, and table 8]). Indeed, the GDPR embraces this approach by requiring that data controllers shall use technical and organisational measures to ensure that the data protection goals are met, and also introduces the prospect of delivering the goals through (voluntary and transparent) certification of technologies[30] (see discussions of this, and comparative approaches in the USA, in King and Jessen 2014).

Privacy by Design: an incomplete, inadequate, and impractical solution

Before PbD is interrogated in more detail, a warning from an interdisciplinary study carried out in Ireland. A 2016 report, published by the Department of An Taoiseach (Kitchin 2016) recognised that the four principal Irish cities have all deployed smart technologies and that there are benefits of this 'in producing more efficient, productive, sustainable, resilient, transparent, fair and equitable cities'. It considered, however, that there is also a need to 'carve a path that allows us to harness these benefits while at the same time, ensuring that we do not compromise data privacy, data protection or data security'. Considering this alignment of the two objectives which run through this paper, this report argues that the focus on technologies can 'overly promote top-down technocratic forms of governance, rather than political/social solutions and citizen-centred deliberated democracy' (23), that technologies 'are portrayed as being objective, commonsensical, pragmatic and politically benign, rather than thoroughly political, reflecting the views of their developers and stakeholders' (23), can have social political and ethical effects, extending surveillance and eroding privacy (23, 26 et seq) and can be systemically vulnerable (2).

Moving forward, the use of technology to address the privacy and smart grids question is well recognized, as is indeed indicated by the Irish report, and also by the case study. The EU set up a mandate for investigation of standards for smart grids and its Joint Working Group delivered its final report in 2011 (CEN/CENELEC/ETSI 2011). This made several recommendations in respect of data protection, privacy and information security. There are references to PbD in the Article 29 opinion on smart grids (and also to the work of the European Commission's Smart Grid Task Force Expert Group in respect of it - Article 29 Data Protection Working Party 2011). There are references to PbD in the Commission Recommendation on the Data Protection Impact Assessment Template (European Commission 2014b, art 8). Further, in 2016 the Smart

Grid Task Force Expert Group 2 delivered recommendations for the functionality that technology should be able to deliver in respect of privacy, data protection and cyber-security in the smart grid environment (European Commission 2017f). In particular, this seeks to align itself with the GDPR, notably through the GDPR's engagement with PbD.

At a practical level, however, it is interesting to note that notwithstanding policy and legal recognition of the PbD pathway, there has been a marked lack of attempts to explore the extent to which PbD can actually apply to smart meters. After extensive interviews with those involved in smart grid initiatives in Great Britain, Brown concluded that there was very limited discussion by DECC of privacy in the context of smart meters. He notes that this is so notwithstanding that there were possible useful bases in Ontario, the 2011 report of the Article 29 Working Group, and a very different approach adopted in Germany; indeed, he found that some civil servants seemed reluctant to include privacy issues and campaigners in discussions (Brown 2014). Murphy conducted a similar analysis of the development of a smart grid in Ireland, noting that PbD was not amongst the five key principles underpinning this initiative, and was only added after complaints. She concluded that there was 'a failure on the part of [the Commission for Energy Regulation] to truly appreciate the function of privacy by design' (Murphy 2015, 200–201). Such failures to properly engage with PbD are by no means inevitable, of course; and Brown highlighted how engaged consultation and a willingness to consider alternatives produced a system with strong privacy protections and real options for consumers in Germany (Brown 2014).

There are also more substantive issues. While PbD aligns with arguments that many problems related to privacy are logistical and so a technical solution is required (Lynskey 2015, 262), Rubenstein and Good criticise PbD in the privacy and data protection context which is key to this paper. Applying PbD to the 'Fair Information Processing' data protection principle, Rubenstein and Good attempt to distil or identify design guidelines for systems engineers and user interface and experience designers. They conclude that PbD could have prevented some high-profile privacy controversies but that a great deal more remains to be done by businesses, regulators, and researchers to ensure that PbD is effective in practice. In particular, they claim that if regulators provide clear guidelines (and indeed the GDPR does refer to having a certification process and approved codes of conduct),[31] these can ensure that commercial considerations do not always overcome privacy concerns (Rubinstein and Good 2013). However, their work does not discuss the impact of PbD on delivery of energy efficiency.

Against this backdrop, the reality of implementation of PbD is complex and difficult (van Lieshout at al. 2011, Urquhart, 2016). Some scholars do present PbD as a concept that can easily be integrated into software development methods such as Agile and DevOps (Hirsch and King 2016, 417–18), and work continues on setting standards reflecting energy efficiency and privacy, data protection and cyber security (Urquhart, 2016). Practical software engineering experience with PbD is still, however, quite limited (Gürses, Troncoso, and Diaz 2011). There are no widely accepted tools or methods for PbD's implementation (Mulligan and King 2011). As Massey notes, PbD is 'an excellent example of a policy initiative that does not provide enough specific guidance to be practical for software engineers' (Massey 2014, 697).

Although some computer scientists have put forward design strategies that can be applied in practice (Alshammari and Simpson 2016), Birnhack and others point out, based on a close reading of texts on data warehousing, that 'PbD seems an intuitive and sensible policy tool for lawyers; however, for information systems developers and engineers, it is anything but intuitive as it goes against the grain of several well-established principles of information systems engineering' (Birnhack, Toch, and Hadar 2014, 56). Related research based on interviews with developers found that they regarded privacy as out of their sphere of concern and something to be dealt with by lawyers or security experts (Hadar 2017). There are efforts underway, however, to translate PbD from abstract legal frameworks into clear guidelines which systems developers can apply, such as the PRIPARE project (Notario at al. 2015). Further, design patterns – high-level descriptions of abstract elements of approaches to design – offer considerable potential for PbD (Hoepman (2014, 446)), but require further elaboration by technologists and support from policy-makers (Danezis at al. 2014). On this, it is interesting to note the 2017 response of the UK Information Commissioner, discussed above, that although technical and organisational steps should be taken, this would depend on the technology available; and they did not wish to mandate specific technical measures as technologies could become obsolete and new risks could be identified. (Information Commissioner's Office 2017b).

Further, empirical research conducted by Massey et al (2014, 84) found that regulatory requirements often contain ambiguities, sometimes deliberately, such as the use of terms like 'reasonable', with open, flexible meanings but also because the text is not drafted as tightly as possible. While technologists can identify these, this does not allow them to solve the implementation problems which they create. Indeed, in some cases, even clear requirements are unimplementable in practice as they involve social and legal questions (such as who is an authorised user) which the technology cannot answer by itself (Massey at al. 2014). In this context, implementing the present and quite limited forms of PbD and PbRD in the light of GDPR and similar arrangements, and the EU standards work introduced above and discussed below, do not guarantee that problems will not occur in the future. As has been explored, privacy is a complex and poorly understood concept; translating it from law to systems engineering requires communication between two very different disciplines, and even when this occurs, it is often too little and too late. The open concepts and flexible terminology which the law prefers are difficult to implement in concrete, binary engineering terms; getting this right is often not seen as a priority by engineers; and resources are always limited, so legal compliance can slip down the task list and perhaps be deferred for some future revision.

Therefore given the challenges which have been identified thus far, it seems at least possible that an IoT technology which underlies the smart grid (just like that in the case study), will struggle in general with meeting PbD goals, and specifically will not comply with the GDPR. Responses discussed above such as consultations looking more widely across fields, and through exploration of Best Available Techniques in the European Commission documents, may lead to new approaches to privacy and smart grids in the context of energy efficiency; or at least may lead to more fusion of the importance of energy efficiency with the importance of PbD technology. Yet the technical, and legal, challenges are: what would really be the result of this? Can the PbD challenges actually be avoided through consultation and fusion? Divergences in

outcomes arise not only from a basic lack of engagement but are also the product of different legal and technological cultures in different countries, organisations, and science and engineering disciplines. This indicates that the traditional legal reform toolbox – higher standards of protection, more stringent rules, even better after the event enforcement procedures (be that from privacy as discussed above, data protection[32] or energy efficiency (Spier and Magnus 2014, Macrory 2014, van Calster et al 2015)[33] – may be unlikely to achieve significant change from the technological and practical perspective in either the short or medium term. Rather, given the focus in this paper on relationships between different laws and technologies, two different pathways will be taken here. Firstly, to explore what may be gained from looking to a different form of law: competition. What can this contribute to addressing the problems of a technology which may be inconsistent with privacy and data protection norms while at the same time contributing to energy efficiency and addressing climate change? Secondly, to create a different, more intersectional and hybrid regulatory toolbox, working across laws and technologies to move towards more coherent and integrated outcomes.

The problems with PbD and the power of competition

Competition regulators have been active in the energy sector regarding restrictions on access to the market, capacity and supply (Wilkinson et al. 2016); and in 2015 they began exploring commercial use of consumer data (Competition and Markets Authority 2015). Further, the Department of Energy & Industrial Strategy 2016 consultation call discussed above considered that the

> smart system can go further and faster in breaking down barriers to competition – allowing the widest possible range of innovative products and services to prove themselves in the market place. To make the most of a smart system we need smart policy and smart regulation. Our ultimate objective – clean, secure and affordable energy - is clear, but a number of possibly pathways lie before us (Department of Energy & Industrial Strategy 2016, 1 and see paras 14-6).

Extending this engagement, the avenue explored here is competition law's prohibition of the abuse of a dominant position: how this might be particularly relevant to privacy concerns, and what it can deliver in terms of future pathways?

As the Competition and Markets Authority 2015 report stresses, abuse can be relevant only if the operator is in a dominant position - in a position to act independently of others.[34] This is assessed by reference to the market in which the activity is carried out, and the markets are defined with regard to substitutability and potential competition,[35] and to geography (which could be global).[36] Dominance can be difficult to establish in fast-moving fields such as IoT, although it is not impossible;[37] and the facts of the case study indicate that dominance could be found given the importance of the company's technology, including its possible inclusion in standards. The key issue regarding whether this is so, is would the case study (or other) standard require this particular technology to be used; or whether, reflecting the Smart Grid Task Force Expert

Group 2 recommendations from 2016 discussed above, the standards are much more focused on the general functions which the technology should have. This would leave it open to others to make their own versions such that no one company could act independently.

If there is dominance, the next step is the need for abuse. This often involves pricing, but it is well established that abusive conduct need not always involve raising the price for products or services (Costa-Cabral and Lynskey 2017, 35, anon, to be inserted post review).[38] Taking a different approach to technology to that discussed here, there have been findings of abuse if technology is not shared widely, with the competition regulator requiring that technology is shared on particular terms, likely fair, reasonable and non-discriminatory.[39] This raises the prospect of whether the passing on of information envisaged in the case study could be abuse. And within this, it is interesting to note that when the EU competition regulator (or court) decides these questions, it is well established that they will have regard to the EU Charter rights.[40] These include as discussed the rights to private life and to data protection; and also the right relating to the environment.[41] This provides a framework**,** then, for the three fields which are discussed together in this paper to be combined – an opportunity which was introduced above but which has not been embraced fully so far in existing privacy and energy efficiency intersections.

Further support for an integrated approach can come from the fact that just as competition has been active in relation to energy as noted, data protection has become increasingly accepted in competition analyses – for example, in the Whatsapp/Facebook merger.[42] This can also be seen at scholarly and policy levels. The fields have been argued to have strong underlying themes, of exercising economic activity and enhancing the interests of individuals, ‘at different ends of the same spectrum’ (Costa-Cabral and Lynskey 2017, 13–15, quote 14,18–9). Importantly, a preliminary opinion of the European Data Protection Supervisor called for data protection to be integrated into competition actions as part of the consumer harm and adverse impacts on consumer welfare (European Data Protection Supervisor 2014, para 71) - which is also a key focus in assessing abuse (European Commission 2009, paras 5-7, 86). Costa-Cabral and Lynskey called for links between the two fields (termed “external”) and also for data protection to have an “internal” impact on competition decision making (Costa-Cabral and Lynskey 2015; Costa-Cabral and Lynskey 2017, 19 et seq). And referring to these arguments, the European Data Protection Supervisor has expressed concern at data protection and competition existing in silos, given the cross cutting application of human rights and common underpinning themes of fairness and the Supervisor was broadly in support of the “external” model (European Data Protection Supervisor 2016, 1, 11, 17). It is also interesting to note, consistent with the wider themes underpinning this paper, the argument that the refusal to pass on information to competitors could be justified under data protection law but could also be an abuse - and that this has been said to warrant co-operation between the two sets of regulators (European Data Protection Supervisor 2014, paras 67-8). An issue worthy in itself of further exploration.

To support the linkage sought here (both “internally” and “externally”), one can draw on competition scholarship’s discussion of disclosure of information regarding the perils of apparently free services and, of particular relevance to the case study, discussion of privacy

policies (see Chirita [2016] for a detailed analysis of privacy policies). There have also been calls for a wider approach to be taken to economics from a privacy perspective in competition [Kerber 2016]); and for there to be investigations into discrimination and exploitation, in the light of the lack of information for users who are operating in the digital economy (European Data Protection Supervisor 2014, 11 and 30–31; Costa-Cabral 2016, 498-507). As discussed, within the case study there may not be adequate consent; even if consumers do indicate consent, this could be challenged on the basis that the policies are not readily obtained or visible; or that there were policies but no choice of provider then there is no meaningful consent; or that there is a choice of provider and privacy policies but all are following the same technical standard, so again there is no meaningful consent. The final example may be particularly significant if the standard is seeking – but failing – to meet PbD and data protection rules. Also important here is the German competition regulator's launch of an abuse investigation into Facebook regarding provisions in its privacy policies relating to the use of user data (Kerber 2016, Section II, III).[43]

This discussion provides a base, then, for further enquiry which could lead to a finding that the case study's passing on of the smart grid data can be found to be an abuse of a dominant position; and for this decision to be reached after consideration of competition law, data protection law, and three different human rights. Competition law would bring its own financial sanctions with it to add to the traditional legal toolbox;[44] but it is this highly integrated legal approach and solution which is the key contribution offered here.

This approach still, however, has its limits. It will only apply if the case study Company is in a dominant position, which is not easy to establish, and the competition regulators (whether UK or EU) must decide to allocate some portion of their scarce resources to pursuing an enforcement action. Even if this succeeds, it would simply entrench a pre-eminence on the power of law to offer a particular solution. Yet this widening of the legal toolbox remains vulnerable to the challenges set out above; further, if the activity does come to an end, so does the opportunity for this pathway to energy efficiency to be delivered with its positive impact on climate change. Therefore, as indicated above, a second, more standards based and hybrid approach, requires discussion.

A more integrated, bottom-up, and appropriately complex approach to standards

Towards a new approach

One opportunity is suggested by Hildebrandt (2011), who argues that effective legal protection for privacy (and also due process and non-discrimination) requires creative re-enactment of these rights in the new technologies which are posing challenges to them, such as the IoT which is the basis of the case study. However, this is not straightforward. At this point, it should be clear to the reader that the combination of networked digital devices deployed in contexts such as the smart grids in the case study, and drives towards energy efficiency which they operationalise, create a complex crossover between regulatory and policy domains often

thought of as separate: data protection, energy efficiency through infrastructure, and competition. Protecting the individual and the consumer in these fields, and contributing to addressing climate change in this particular way, will require collaboration and coordination between regulators and policymakers working across industries - as indeed suggested by the European Data Protection Supervisor (European Data Protection Supervisor 2014) and European Data Protection Supervisor 2016) and by the (European Commission 2012, 2014a, 2014b, 2017d).

Actually delivering this will require the application of a range of skillsets, perspectives, and analytical tools. As seen, there is some existing engagement between laws, and within sectors between laws and other fields (notably technology and privacy in data protection, and technical work through the Smart Grid Task Force). There are also key technical challenges to be explored, together with the inherent complexity of balancing the priorities of regard to energy efficiency, privacy and data protection, and to do so by moving beyond the existing engagement. Despite the premise suggested above that this was unlikely to be achieved, hence suggested interventions through competition law in some cases, the privacy-energy efficiency-technology intersection is too important to be abandoned entirely. The very real challenge of addressing climate change by reducing greenhouse gas emissions through a focus on energy efficiency and infrastructure, provides an urgent need and policy momentum to pursue this.

Supporting this, Gellert (2016) points out that efforts to resolve privacy issues with smart grids in The Netherlands (notwithstanding the developments there discussed above) and in Germany have not been adequate, and that current implementations of this technology have a weak approach to sustainability. He argues that a strong sustainable development perspective is required for integration, which must include human rights issues,[45] and that this will allow real progress to be made in tackling both privacy and environmental protection. Although this will make the task more complex, it again underpins the theme of this paper.

A more negative incentive to move forward with this task is that a great deal of IoT technology is designed in the US and manufactured in China, jurisdictions with very different perspectives on privacy (taken broadly) to the EU. There is, therefore, a strong risk of privacy being sidelined at a practical level within the energy and climate change landscape as a minor nuisance, to be ignored until it is too late and then left unsolved as it will be too difficult to retro-fit into the installed base of infrastructure. It is necessary to avoid this. To ensure that protection of privacy and data protection is not a problem or an irritant (however genuinely attempts are being made to address it), when pursuing the energy efficiency goal, but one which is seen as of equal value. A new approach is needed, building on the legal, social, policy and technical developments explored in this paper. This should be inter-disciplinary, and at the intersection between technology, privacy, and energy efficiency issues. Recognition of the social challenges raised in the Irish report; alongside the steps seen to be taken by the EU (in particular) regarding standards, the new data protection template, considering energy benefits in privacy work and vice versa; and the prospect of listening and engaging with industry and technologists, could all combine to bring about something far beyond PbD. On this it is noteworthy that Koops and Leenes conclude that PbD will not be achieved by techno-regulation but by changing communications channels (Koops and Leenes 2014).

New approaches to standards and institutions

A means of bringing this about, which builds on the case study references to (different kinds of) industry standards, is the development of robust open standards. These would be tested by consumers through a collaborative process, and anyone would be able to use the resulting standards. This aligns with self-regulation; Rubinstein has argued that when legal frameworks are fragmented (as in the case study), self-regulation may offer a way forward, however imperfect (Rubinstein 2011). A standards based approach has been applied elsewhere in the environmental landscape; for example as a formal industry initiative such as sustainable timber (for example, the UK Forestry Standard embracing both legal requirements and best practice),[46] and see Maurer 2014, 302-330. Support for this approach from the information security perspective comes in a report published by the European Union Agency for Network and Information Security which recommends the inclusion of privacy in the process of developing standards (Danezis et al 2014, 54). In addition, the International Standards Organisation (ISO) has already undertaken substantial work on privacy standards (De Hert and Papakonstantinou 2013, 295-6)[47] and also on climate change;[48] but it has not combined them. Further standards development is also supported by the International Data Protection and Privacy Commissioners (2007), who drafted a joint proposal (International Data Protection and Privacy Commissioners (2009)), referring to developing technical specifications for information systems and technologies for processing of data to applicable laws (International Data Protection and Privacy Commissioners (22e). Once again, however, this work does not engage with climate change and energy efficiency. Standards for energy efficiency which pay more than lip-service to privacy issues and which drew on legal and technical expertise, could build on the activity of the European Telecommunication Standards Institute (which is involved in the EU standards work discussed above) or indeed the International Telecommunications Institute (ITU).

Of particular interest for possible positive outcomes from the case study, is the potential for European standards to be exported to other jurisdictions. This happened with the adoption of the Reduction of Hazardous Substances regulation by California which was modeled on Directive 2002/95[49] – and is therefore important across the United States and globally (Bradford 2012, 30 and see also Dilling 2012). The possible use of standards as a means of demonstrating compliance with the GDPR, authorized by Article 43, is another means of enabling standards to spread globally (and note also the importance discussed above of the practical importance of non EU countries meeting GDPR standards). However, this will require real engagement not only from industry but from civil society, particularly privacy activists, and from privacy and competition regulators, which (as has been discussed) is still a limited phenomenon.

Indeed new transnational standards proposals would provide a means for constructive dialogue between the legal and technical sphere (Rachovitsa 2016)**.** Further, it could avoid a patchwork of geographically-constrained law and regulation which would also have significant attractions for industry:

> For companies that operate internationally, a set of fundamental principles would also provide guidance. Any personal information that they collect and transfer across borders

> would be subject to the same set of fundamental principles, which would reduce legal complexity and therefore reduce the cost of compliance. Significantly different standards across the world create an impediment to companies that need to comply with the requirements of different information privacy laws (Toy 2013, 957).

Given the starting point of this paper – energy efficiency and addressing climate change through infrastructure – environmental law does, appropriately here and once again, provide a useful further model as to how this could be done. This time, international environmental law has been moving to being more integrated and multi-modal (Long 2015), and adopting more 'hybrid' structures, for example in respect of transnational governance of chemicals and hazardous substances (Dilling 2012). It is time for privacy law and technologies to do the same, particularly for problems (such as in the case study) where there are intersections with other domains.

From a regulatory perspective, such an approach would be more bottom-up than top-down, and in the hands of the wide group of relevant stakeholders – in the case study, this could include two Companies, the standards body and users. Drawing on international environmental law as it strives to rise to the challenges presented by the complex, dynamic nature of the problems which it seeks to solve, four key features emerge which are relevant to ensuring the success of any moves in this direction. Firstly, flexible and integrated institutions, which operate in a "soft regulation" mode (such as the best practice in the forestry standard) rather than applying "hard rules" such as a requirement that a smart grid is used (Long 2015, 180-190). Secondly, due to the range of entities, issues, and natural phenomena which international environmental law addresses, it meets complex problems with appropriately complex institutional inter-relationships (Long 2015, 190-196). Thirdly, institutions adapt to changing physical and policy contexts in an iterative and resilient fashion (Long 2015, 196-200). Fourthly, international environmental law pays particular attention to linkages between issues and institutions, particularly by ensuring that human rights questions are included in discussions about environmental law (Long 2015, 200-201) – the relevance of this to the case study has been explored. It is also noteworthy that the development of standards that are more than "green-washing" may require including Non Governmental Organizations. This was done in the Mobile Phone Partnership Initiative (Dilling 2012, 406), which addresses the environmentally sound management of end-of-life mobile phones (Secretariat of the Basel Convention undated, Morgera and Kulovesi 2013, from 140). In respect of the case study, privacy and climate change activists could both be involved in standards development.

Delivering these new standards through a wider and more inclusive governance process may not be straightforward. It is valuable here to explore some of the wider issues which could be encountered. In respect of institutions the first key feature identified above, standard-setting (particularly when it is an alternative to more conventional law-making) and being to an extent bottom up nature and leading to power held by the institution, can suffer from a perception of lack of legitimacy (Biermann and Gupta 2011). This is highlighted in the case study by the rise in importance of the Company's products in the marketplace; they may become a standard while not respecting fundamentals of data protection law. How, then, can the standards' legitimacy be ensured? Scharpf (writing about European law-making, but making a point which

extends to other domains) argues that legitimacy relies on trust in institutional arrangements, which provides *input legitimacy* ("that governing processes are generally responsive to the manifest preferences of the governed") and *output legitimacy* ("that the policies adopted will generally represent effective solutions to common problems of the governed") (Scharpf 2003, 4).

Can the institutions discussed above be trusted now, or made trustable through reform? This will also require some effort. Gerson (2016) argues forcefully that the ITU is "broken" as it fails to engage constructively with civil society. He proposes a number of reforms which he claims are necessary in order to increase transparency: broader channels for participation and lower barriers to access to internal documents (Gerson 2016, 1470–1488). This echoes what has already been successfully implemented by a different type of institution, the World Wide Web Consortium. In its privacy standard setting processes, the World Wide Web Consortium has incorporated elements of delegation to multi-stakeholder groups, public discussions and debates, deliberately diversifying participation to include civil society and government experts (through waiving fees, geographically distributed meetings, funding support, and other capacity-building measures) (Doty and Mulligan 2013, 155–165). This approach is also once again in keeping with international environmental law, for example Principle 10 of the 1992 Rio Declaration on Environment and Development[50] calls for more participatory governance. It is also possible: strong civil society participation in ITU processes has been achieved in the past, particularly in the World Summit on the Information Society in 2003 (Yu 2009, 538).

Getting the most from this process will require "orchestration" (Abbott 2012, 587) by an institution and intersecting, and linking with other institutions (reflecting the second and fourth key feature) such as those with a climate change and energy efficiency focus. It is important, however, that this process also avoids the possible dysfunctions of decentralized governance, such as fragmentation and high transaction costs (Abbott 2012, 587). The end result is likely to be a "regime complex" of overlapping regimes (Raustiala and Victor 2004). Several approaches can be used in turn to assess the legitimacy of an energy efficiency and privacy complex as it develops. There are the six criteria put forward by Keohane and Victor (2011): coherence, accountability, determinacy, sustainability, epistemic quality, and fairness; Bäckstrand (2008, 82)'s three-dimensional model of accountability (participatory, transparency, and availability of monitoring mechanisms); and Arnstein (1969)'s "ladder of citizen participation", with rungs that elevate stakeholder engagement from manipulation through consultation to delegated power and control.

Finally, at a practical level within the functional requirements within the standard one could have regard to some diverse proposals regarding how best to manage privacy and security risks arising from networked digital devices. Peppet suggests tighter controls on the re-use of information; more clarity for consumers regarding policies, sensors, and sharing; and vesting ownership in information in individuals rather than businesses, all of which are highly relevant to the case study (Peppet 2014, 150–164). Similarly, the UK National Association of Citizens Advice Bureaux has recommended empowering consumers with greater transparency around the use of their data and ultimate control of its use according to their preferences rather than the

convenience of businesses (Coll 2015). Ohm and Reid propose the creation of a state agency with responsibility for regulating code, with the role of coordinating between and convening other agencies, together with a bottom-up focus on injecting technical and technological expertise in the policy process (Ohm and Reid 2016, 1700–1702). In a similar vein, it has been argued that important applications of software require its making available on an open source basis (Sandler et al. 2010); and Moglen (focusing on software in medical devices, but presenting an analysis that can be extended to many other fields) claims that black-boxed software without source code is an "unsafe building material", something which would not be permitted in the construction industry (Moglen 2010). Therefore, in order for citizens and consumers to have confidence in IoT devices, source code for key components may need to be made available, either on an open source basis or (if trade secrets concerns require) perhaps by deposit with trusted third parties. This would create opportunities for privacy and security audits, either by government agencies or through crowd-sourcing.

Conclusions

Within the context of a multi-faceted case study, this paper began with a focus on delivering one policy and legal goal – energy efficiency through infrastructure to assist in addressing climate change to meet international treaty commitments. The paper explored the policy and legal challenges that one means of delivering this, smart grids which provide personal information, can pose to privacy and data protection law. It then noted the risks for privacy if installed infrastructure and accepted approaches to smart grids and information do not conform to legal requirements taken broadly. This is so notwithstanding some significant recognition of the issue within the energy landscape, and indeed within the information landscape. The paper argued that these risks continue notably because of the inadequacy of the technology; the challenges of relying on technology; and in the overly limited instances of regulators of energy and climate change, and of privacy and data protection, fully embracing and intertwining the other field.

The paper outlined two solutions which could respond to this: one which turns to more law, and one which is interdisciplinary with a focus on standards, involving institutions, wider participation and self regulation**.** Legally, it was argued that the EU framework of competition law prohibiting abuse of a dominant position, human rights (covering privacy, data protection and also rights in respect of the environment) and data protection law could combine to prevent sharing of data by those with significant control of a market. The possibility of integration of data protection law, with its strong impact on non-EU activity, with competition law increase the prospect of this model having wider transnational appeal. This legal approach could, however, be a rather blunt approach. It could lead to the energy efficiency and ultimate climate change benefits of smart grids being lost through a prohibition of the abusive activity. It would not provide solutions for the information regulator, or those involved in policy leadership and regulation in energy efficiency, to deliver energy efficiency through infrastructure while also acting consistently with other legal fields.

So although legal interdisciplinary dialogue and more can assist, something else is required. The powerful Irish report concluded that "there is a need to chart a path that is neither so luddite

that no developments can occur, nor too boosterist or scare-mongering that fundamental values of privacy, liberty and freedom are sacrificed for a data economy or a surveillant securitised state" (Kitchin 2016, 60). There must be deep and ongoing engagement between law and technology, much more integrated and ongoing than has been seen in the past. Open standards, built through wide communication including across institutions (themselves across discipline), through a self-regulatory approach and involving lawyers, technologists and users, are a hybrid means of delivering this. Indeed, appropriately given the focus on energy efficiency for addressing climate change, the related field of international environmental law has been seen to provide a useful base for more multi-modal, self regulatory frameworks, and new communication across legal and technical fields. This, with some effort towards reforming institutions and involving civil society, has been argued to provide a base for new standards which can be used by energy efficiency and by information regulators, together and apart, to support their existing openness to engaging with the challenges of the other field. It has been recognised that this raises wider questions of regulatory legitimacy and proposals have been made as to how this could be pursued.

Accordingly, in a refined version of the case study, the smart technology developed through wide engagement with lawyers and technologies across fields could meet PbD and EU data protection requirements and would be of transnational appeal. It would not involve an abuse of a dominant position on the basis posited here. Through adoption by a standards body it could enable three areas of law (privacy in the broad sense, and addressing climate change through energy efficiency and infrastructure, and human rights) to be effectively and informedly integrated. More widely, this approach could address the challenges of seeing technology as having the answers to legal problems; of technology being confused by legal uncertainties; and of some lawyers seeing the answers as lying in another field or the other field as being irrelevant to them. It also avoids the prospect of the passing of more laws (general or specific) and the reliance on existing laws, which are often mis-understood, mis-applied, or simply ignored by that key group - technologists.

Two strands of solutions exist, therefore, to increase the prospects of solutions being delivered which reflect and integrate competing fields which are in fact relevant to single goals. What is required is intersectional willingness to bring them about. The roots of this have been identified in this paper. Now it is time for action.

Notes

[1] United Nations Framework Convention on Climate Change (opened for signature 9 May 1992, entered into force 21 March 1994) 31 International Legal Materials 849.
[2] Kyoto Protocol to the United Nations Framework Convention on Climate Change (opened for signature 11 December 1997, entered into force 16 February 2005) 37 International Legal Materials 22, articles 2-4, Annex A.
[3] UN Doc FCCC/CP/2009/L.7. There is agreement on enhancing actions, see articles 1, 2, 4, 5.

[4] UN Doc FCCC/CP/2015/L.9/Rev.1.
[5] Paris Agreement, articles 2, 3, 4, 5, 7, 11, and 12; regarding compliance articles 13-15.
[6] Council Directive (EU) 27/2012 on energy efficiency [2012] OJ L315/1, recitals 27 and 31 ("Energy Efficiency Directive").
[7] The Queen's Speech and Associated Background Briefing, on the Occasion of the Opening of Parliament on Wednesday 21 June 2017. hhttps://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf (Queen's Speech), pages 13, 32
[8] Charter of Fundamental Rights of the European Union (Charter) arts 7 and 8.
[9] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) ("ECHR") art 8.
[10] *Campbell v MGN* [2004] 2 AC 457, *Weller v Associated Newspapers* [2015] EWCA Civ 1176.
[11] *Lion Laboratories Ltd v Evans* [1985] QB 526 (CA).
[12] Data Protection Act 1998.
[13] Council Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
[14] UK Data Protection Act 1998 s1, s 2, s36, schedule 1, schedule 2
[15] Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1 ("GDPR").
[16] GDPR arts 3, 4, 5, 7, 13 ,14, 32, 44 – note also the right to be forgotten art 17 and provisions regarding automated decision making in arts 21 and 22
[17] GDPR, art 4, 6(1)(a), 7, 13 and 14 (regarding provision of information)
[18] GDPR, art 6(1) (e) and (f), 13(a)(d) and 14 (regarding provision of information),
[19] Queen's Speech, p16, 46.
[20] GDPR, art 4(11)
[21] This is in contrast to 2016 attitudes in the UK, leading to the Investigatory Powers Act 2016 and the Digital Economy Bill 2016.
[22] Note that in the UK, climate change is since 2016 part of the Department for Business, Energy and Industrial Strategy.
[23] Again, Energy Efficiency Directive recitals 27 and 31.
[24] Energy Efficiency Directive, recital 32.
[25] Council Directive (EC) 2009/72 concerning common rules for the internal market in electricity [2009] OJ L211/55
[26] Council Directive (EC) 2009/73 on common rules for the internal market in natural gas [2009] OJ L211/94.
[27] Energy Efficiency Directive, art 9(2)(b).
[28] Energy Efficiency Directive, art 7(8)(b) – with confidential information to remain as such.
[29] Charter, art 37.
[30] GDPR, arts 25 and 42.
[31]GDPR, arts 40, 41
[32] See eg new approaches to data protection enforcement, in the UK through section 13 and also 55A-E Data Protection Act 1998 and GDPR arts 77-84; see also *Google Inc v Vidal-Hall* [2015] EWCA Civ 311.
[33]See discussion above regarding international pathways notes 1-5. Enforcement in respect of climate change, energy and the environment more generally is very fragmented and can sit at the border of private/public questions, as well as involving questions of eg nuisance and disputes relating to specific regulatory regimes such as trading schemes - see cited sources for discussion across jurisdictions and eg *Urgenda* (Rechtbank Den Haag (2015) C/09/456689) and R (on application *ClientEarth v Secretary of State for the Environment, Food and Rural Affairs* [2016] EWHC 2740 (Admin).
[34] Case 27/76 *United Brands v Commission* [1978] ECR 208.

[35] European Commission (1997).
[36] *Microsoft Corp v Commissio*n [2007] ECR II-3601 (note 146). And note that for EU competition law to apply there must be an effect on trade across member states, although this is likely to be met when data might be crossing borders, as seems possible given the case study – see European Commission (2014c).
[37] See findings of dominance and abuse in technology sectors, see for example *Microsoft Corp v Commissio*n [2007] ECR II-3601 (note 53, 151).
[38] Building on for example Case C-418/01 *IMS Health v NDC Health* [2004] ECR I-5039; Case T-201/04 *Microsoft Corp v Commissio*n [2007] ECR II-3601.
[39] Building on Case C-6/73 *Commercial Solvents v Commissio*n [1974] ECR 233, Case C-418/01 *IMS Health v NDC Health* [2004] ECR I-5039 (note 53), Case T-201/04 *Microsoft Corp v Commissio*n [2007] ECR II-3601 (note 53).
[40]and as was done by the EU Court of Justice in considering when it was abuse to seek an injunction after an undertaking had been given to licence a standard essential invention on a fair, reasonable and non discriminatory basis Case C-170/13 *Huawei v ZTE* [2015] Bus LR 1261**,** AT.39985 - Motorola - enforcement of GPRS Standard Essential Patents (29 April 2014), http://ec.europa.eu/competition/antitrust/cases/dec_docs/39985/39985_928_16.pdf. See also balancing of different human rights by the EU Court of Justice in cases involving privacy and data protection eg Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971; Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271; Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*; and Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831
http://ec.europa.eu/competition/antitrust/cases/dec_docs/39985/39985_928_16.pdf. See also balancing of different human rights by the EU Court of Justice in cases involving privacy and data protection eg Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971; Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271; Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*; and Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831
[41] Charter arts 7, 8 and 37.
[42] Case COMP/M.7217 Commission Decision [2014] OJ C 417/2. (although not in relation to Google/Doubleclick) Case COMP/M.4731 Commission Decision [2008] OJ C 184/10.
[43] For details of a Bundeskartellamt proceeding 2 March 2016.
[44] No longer quite so different from those now in the GDPR, see note 30, but the large prospect of a fine of up to 10% of global turnover Article 23(2) Council Regulation 1/2003 of 16 December 2002 on implementation of rules on competition OJ L 4 January 2003, 1-25.
[45] See also on this eg 1986 UN Declaration on the Right to Development A/RES/41/128 and the UN Sustainable Development Goals https://sustainabledevelopment.un.org/?menu=1300
[46] See https://www.forestry.gov.uk/theukforestrystandard
[47] A particular example might be ISO/IEC 29100:2011.
[48] For example, ISO 14001, ISO 50001 regarding good practice in energy management and quantifying and communicating greenhouse gas emissions ISO 14064 and 14065, and dedicated web page https://committee.iso.org/tc207sc7
[49] California Department of Substance Control, Restrictions on Use of Hazardous Substances "http://www.dtsc.ca.gov/HazardousWaste/RoHS.cfm
[50] UN Doc A/CONF.151/26 (Vol. I).

References

Abbott, Kenneth W. 2012. "The transnational regime complex for climate change." *Environment and Planning C: Government and Policy* 3 0(4): 571–590.

Alshammari, Majed and Andrew Simpson. 2016. “Towards a Principled Approach for Engineering Privacy by Design.” *Department of Computer Science Oxford University*. http://www.cs.ox.ac.uk/publications/publication10480-abstract.html

Sherry R. Arnstein. 1969. “A Ladder Of Citizen Participation.” *Journal of the American Institute of Planners*, 35 (4): 216–224.

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

Article 29 Data Protection Working Party. 2013. *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (“DPIA Template”) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force*, 4 December. WP 209.

Bäckstrand, Karin. 2008. "Accountability of networked climate governance: The rise of transnational climate partnerships." *Global Environmental Politics* 8 (3): 74–102.

Bernal, Paul. 2014. *Internet Privacy Rights: Rights to Protect Autonomy.* Cambridge: Cambridge University Press.

Brandeis, Louis and Samuel Warren. 1890. “The Right to Privacy.” *Harvard Law Review* 4 (5): 193–220.

Biermann, Frank, and Aarti Gupta. 2011. "Accountability and Legitimacy in Earth System Governance: A Research Framework." *Ecological Economics* 70 (11): 1856–1864.

Birnhack, Michael, Eran Toch, and Irit Hadar. 2014. “Privacy Mindset, Technological Mindset” *Jurimetrics* 55 (1): 55–114.

Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. “Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns.” *Proceedings on Privacy Enhancing Technologies* 4: 237–254.

Bradford, Anu. 2012. “The Brussels Effect.” *Northwestern University Law Review* 107 (1): 1–68.

Anon to be inserted post review

Anon to be inserted post review

Brown, Ian. 2014. “Britain’s Smart Meter Programme: A Case Study in Privacy by Design.” *International Review of Law, Computers and Technology* 28 (2): 172–184.

California Utility Commission. 2011. “Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company,

Southern California Edison Company, and San Diego Gas & Electric Company". Decision 11-07-056.

Cavoukian, Ann, Jules Polonetsky, and Christopher Wolf. 2010. "Smartprivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation." *Identity in the Information Society* 3 (2): 275–294.

CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids (2011) ftp://ftp.cencenelec.eu/CENELEC/Smartgrid/SmartGridFinalReport.pdf

Chirita, Anca D. 2016. "The Rise of Big Data and the Loss of Privacy." *Durham Law School Research Paper*, August 22. https://ssrn.com/abstract=2795992

Chui, Michael, Markus Löffler, and Roger Roberts. 2010. "The Internet of Things" *McKinsey Quarterly* 2010 (2): 1-9.

Collier, Steven E. 2017. "The Emerging Enernet: Convergence of the Smart Grid with the Internet of Things." *IEEE Industry Applications Magazine* 23 (2): 12–16.

Competition and Markets Authority. 2015. "The commercial use of consumer data. Report on the CMA's call for information" https://www.gov.uk/cma-cases/commercial-use-of-consumer-data

Costa-Cabral, Francisco. 2016. "The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law." *Maastricht Journal* 23 (3): 495–513**.**

Costa-Cabral, Francisco and Orla Lynskey. 2015. "The Internal and External Constraints of Data Protection on Competition Law in the EU". *LSE Working Paper 25/2015*.

Costa-Cabral, Francisco and Orla Lynskey. 2017. "Family Ties: The Intersection Between Data Protection and Competition in EU Law." *Common Market Law Review* 54 (1): 11–50.

Cuijpers, Colette, and Bert-Jaap Koops. 2014 "Smart Metering and Privacy in Europe: Lessons from the Dutch Case." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet. 269–293. Dordrecht: Springer Netherlands.

Danezis, George, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. 2014. "Privacy and Data Protection by Design – from Policy to Engineering." European Union Agency for Network and Information Security.

De Hert, Paul and Vagelis Papakonstantinou. 2013. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?" *I/S: A Journal of Law and Policy for the Information Society* 9 (2): 271–324.

Delany, Hilary and Eoin Carolan. 2008. *The Right to Privacy: A Doctrinal and Comparative Analysis* Dublin: Thomson Round Hall.

Department of Energy and Climate Change. 2012. "Smart Metering and Implementation Programme. Data access and privacy"

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

Department of Energy and Climate Change and Office of Gas and Electricity Markets. 2014. *Smart Grid Vision and Roadmap*. London: Department of Energy and Climate Change.

Department of Energy & Industrial Strategy and Office of Gas and Electricity Markets. 2016. "Call for Evidence on a 'Smart, Flexible Energy System"' *Department of Energy and Climate Change and Office of Gas and Electricity Markets*. Accessed 1 June 2017 https://www.gov.uk/government/consultations/call-for-evidence-a-smart-flexible-energy-system

Department of Energy and Climate Change and Office of Gas and Electricity Markets. 2017. "UK Smart Grid Portal." *Department of Energy and Climate Change and Office of Gas and Electricity Markets*. Accessed 14 February 2017. http://uksmartgrid.org

Dilling, Olaf. 2012. "From Compliance to Rulemaking: How Global Corporate Norms Emerge From Interplay With States and Stakeholders." *German Law Journal* 13 (5): 381–418.

Doty, Nick, and Deirdre K. Mulligan. 2013. "Internet Multistakeholder Processes and Techno-Policy Standards: Initial Reflections on Privacy at the World Wide Web Consortium." Journal on Telecommunications and High Technology Law 11: 135–182.

Edwards, L. 2016 "Privacy, security and data protection in smart cities: a critical EU law perspective" European Data Protection Law Review vol 2 28-58

European Commission. 1997. "Notice on the Definition of Relevant Market for the Purposes of Community Competition Law." [1997] OJ C 372/5.

European Commission. 2006. "Guidelines on the Methods of Setting Fines." [2006] OJ C210/2.

European Commission. 2009. "Guidance on Its Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings." [2009] OJ C 45/7.

European Commission. 2012. "Recommendation on preparations for the roll-out of smart metering systems." 2012/148/EU.

European Commission. 2014a. "Commission Staff Working Document Cost Benefit Analyses and State of Play on Smart Metering Deployment." SWD/2014/0189/final.

European Commission. 2014b. "Recommendation on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems." 2014/724/EU.

European Commission. 2017a. "Climate Action" *European Commission*. Accessed 30 May 2017 https://ec.europa.eu/clima/citizens/eu_enhttps://ec.europa.eu/clima/citizens/eu_enhttps://ec.europa.eu/clima/citizens/eu_enhttps://ec.europa.eu/clima/citizens/eu_en

European Commission. 2017b “Energy Efficiency” *European Commission*. Accessed 30 May 2017 http://ec.europa.eu/energy/en/topics/energy-efficiency

European Commission. 2017c. “Market Legislation.” *European Commission*. Accessed 14 February 2017. http://ec.europa.eu/energy/en/topics/markets-and-consumers/market-legislation

European Commission. 2017d. “Smart Grids and Meters.” *European Commission*. Accessed 14 February 2017. http://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters

European Commission. 2017e. “Test phase of the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering Systems.” *European Commission*. Accessed 14 February 2017. https://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systemshttps://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systemshttps://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systemshttps://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems

European Commission. 2017f. Smart Grids Task Force accessed 24 May 2017 https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force

European Data Protection Supervisor, 2014. “Preliminary Opinion of the European Data Protection Supervisor. Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy.”

European Data Protection Supervisor, 2016. “Coherent Enforcement of Fundamental Rights in the Age of Big Data.” Opinion 8/2016.

European Parliament resolution of 4 February 2014 on the local and regional consequences of the development of smart grids (2013/2128 (INI) OJ C 93 24 March 2014 34-41

European Sustainable Energy Week. 2017. “Web Streaming 2016.” *European Sustainable Energy Week*. Accessed 14 February 2017. http://eusew.eu/livestreaming

European Telecommunication Standards Institute. 2016. “ETSI Intellectual Property Rights Policy.” *European Telecommunication Standards Institute*, April 20. http://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf

Gellert, Raphael. 2016. “Redefining the Smart Grids' Smartness. Or Why it is Impossible to Adequately Address Their Risks to Privacy and Data Protection if Their Environmental Dimension is Overlooked.” *Journal of Law, Information and Science* 24 (1): 34.

Gerson, Jason. (2015): “A Grand Bargain among the International Telecommunication Union's Skeptics and Proponents: Building a Third Way toward Internet Freedom.” Georgetown Journal of International Law 47: 1459–1496.

Gürses, Seda, Carmela Troncoso, and Claudia Diaz. 2011. “Engineering Privacy by Design." *Computers, Privacy and Data Protection* 14 (3).

Gürses, Seda. 2014. “Can you Engineer Privacy?” *Communications of the ACM* 57 (8): 20–23.

Hadar, Irit, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. “Privacy By Designers: Software Developers’ Privacy Mindset.” *Empirical Software Engineering* (2017): 665.

Higgins, Parker. 2015. “Big Brother Is Listening: Users Need the Ability To Teach Smart TVs New Lessons.” *Electronic Frontier Foundation*, February 11. http://www.eff.org/deeplinks/2015/02/big-brother-listening-users-need-ability-teach-smart-tvs-new-lessons

Hildebrandt, Mireille. “Legal Protection By Design: Objections and Refutations.” *Legisprudence* 5 (2) (2011): 223–48.

Hirsch, Dennis D. and Jonathan H. King. 2016. “Big Data Sustainability: An Environmental Management Systems Analogy.” *Washington and Lee Law Review Online* 72 (3): 406–419.

Hoepman, Jaap-Henk. 2014. “Privacy Design Strategies.” In *ICT Systems Security and Privacy Protection*, edited by Nora Cuppens-Boulahia, Frédéric Cuppens, Sushil Jajodia, Anas Abou El Kalam, and Thierry Sans. 446–459. Heidelberg: Springer.

Hoerter, Christian M., Nils Feyel and Alexandria Awad. 2015. “The Smart Grid: Energy Network of Tomorrow – Legal Barriers and Solutions to Implementing the Smart Grid in the EU and the US.” *International Energy Law Review* 8: 291–300.

House of Commons Energy and Climate Change Committee. “The energy revolution and future challenge for UK energy and climate change policy. Third Report of Session 2016-7 https://www.publications.parliament.uk/pa/cm201617/cmselect/cmenergy/705/705.pdf

Information Commissioner’s Office. 2017a “GDPR consent draft guidance and consultation” https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Information Commissioners’ Office. 2017b. “Response to the Department of Energy & Industrial Strategy and Ofgem’s Call for Evidence on a “Smart, Flexible Energy System”’ https://ico.org.uk/media/about-the-ico/consultation-responses/2017/1625738/ico-response-beis-smart-energy-20170112.pdf

International Data Protection and Privacy Commissioners. 2007. “Resolution on Development of International Standards.” *International Data Protection and Privacy Commissioners*, September 26–28. https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Development-of-International-Standards.pdf

International Data Protection and Privacy Commissioners. 2009. “Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data.” *International Data Protection and Privacy Commissioners*, November 5. http://www.privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

Keohane, Robert O., and David G. Victor. 2011. “The regime complex for climate change.” *Perspectives on Politics* 9 (1): 7–23.

Kerber, Wolfgang. 2016. “Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection.” *Journal of Intellectual Property Law and Practice* 11 (11): 856–866.

King, Nancy J., and Pernille W. Jessen. 2014. “Smart Metering Systems and Data Sharing: Why Getting a Smart Meter Should Also Mean Getting Strong Information Privacy Controls to Manage Data Sharing.” *International Journal of Law and Information Technology* 22 (3): 215–253.

Kitchin, Rob. 2016. *Getting Smarter about Smart Cities: Improving Data Privacy and Data Security*. Dublin: Data Protection Unit, Department of the Taoiseach.

Koops, Bert-Jaap and Ronald Leenes. 2014. ‘Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the ‘Privacy by Design’ Provision in Data-Protection Law.” *International Review of Law, Computers and Technology* 28 (2): 159–171.

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tom Chokrevski, and Maša Galič. 2017. “A Typology of Privacy.” *University of Pennsylvania Journal of International Law* 38: 483.

Long, Andrew. 2015. “Global Integrationist Multimodality: Global Environmental Governance and Fourth Generation Environmental Law.” *Journal of Environmental and Sustainability Law* 21 (1): 169–208.

Lynskey, Orla. 2015. *The Foundations of EU Data Protection Law.* Oxford: Oxford University Press.

Macrory, Richard. 2014. 2nd edn *Regulation and Enforcement and Governance in Environmental Law* Oxford: Hart.

Massey, Aaron. 2014. “Getting to October: Why Understanding Technology Is Essential for Privacy Law.” *Idaho Law Review* 51 (3): 695–710.

Massey, Aaron K., Richard L. Rutledge, Annie I. Antón and Peter P. Swire. 2014. “Identifying and Classifying Ambiguity for Regulatory Requirements.” *22nd International Requirements Engineering Conference (RE)*, edited by Robyn Lutz, Tony Gorschek, Sarah Gregory, Marjo Kauppinen, 83–92. IEEE.

Matzner, Tobias. 2014. “Why Privacy Is Not Enough Privacy in the Context of ‘Ubiquitous Computing’ and ‘Big Data’.” *Journal of Information, Communication and Ethics in Society* 12 (3): 93–106.

Maurer, Stephen M. 2014. “Public Problems, Private Answers: Reforming Industry Self-governance Law for the 21st Century.” *DePaul Business and Commercial Law Journal* 12 (3): 297–360.

McCormick, Melanie. 2015. “Conflicting Theories at Play: Chemical Disclosure and Trade Secrets in the New Federal Fracking Regulation.” *Golden Gate University Environmental Law Journal* 9(2): 217–237.

McCullagh, K. 2017. “Brexit: potential trade and data implications for digital and ‘fintech’ industries” International Data Privacy Law 7(1): 3-21

McKay Hannah. 2016. “Making Energy in Scotland Affordable: Smart Grids - Smart Energy - Smart Consumers.” McKay Hannah, September 20. http://www.mackayhannah.com/conferences/smart-grids-smart-energy-smart-consumers

Moglen, Eben. 2010. “When Software Is in Everything: Future Liability Nightmares Free Software Helps Avoid.” *Software Freedom Law Center*, June 30. http://www.softwarefreedom.org/events/2010/sscl/moglen-software_in_everything-transcript.html

Morgera, Elisa and Kati Kulovesi. 2013. “Public-private partnerships for equitable access to climate technologies” in *Environmental technologies, intellectual property and climate change*, edited by Abbe E. L. Brown 128-151. Cheltenham: Edward Elgar, UK

Mulligan, Deirdre K and Jennifer King. 2011. “Bridging the Gap Between Privacy and Design.” *University of Pennsylvania Journal of Constitutional Law* 14: 989.

Murrill, Brandon J., Edward C. Liu and Richard M. Thompson II. 2012. *Smart Meter Data: Privacy and Cybersecurity*. Washington: Congressional Research Service.

Murphy, Maria H. 2015. “The Introduction of Smart Meters in Ireland: Privacy Implications and the Role of Privacy by Design” *Dublin University Law Journal* 38 (1): 191–207.

National Infrastructure Commission. 2016. “Smart Power” https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/505218/IC_Energy_Report_web.pdf

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books.

Notario, Nicolás, Alberto Crespo, Yod-Samuel Martín, Jose M. Del Alamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener, and David Wright. 2015. “PRIPARE: Integrating Privacy Best Practices Into a Privacy Engineering Methodology.” In *IEEE Security and Privacy Workshops (SPW), 2015*, 151–158.

Office of Gas and Electricity Markets. 2010. “Smart Metering Implementation Programme: Data Privacy and Security.” Office of Gas and Electricity Markets. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/42730/232-smart-metering-imp-data-privacy-security.pdf

Ohm, Paul and Blake Reid. 2016. “Regulating Software When Everything Has Software.” *George Washington Law Review* 84 (6): 1672–1702.

Palmer, Kate. 2016. “Vodafone signs £75m deal with Scottish Power to connect cables to a ‘smart grid’.” *Telegraph*, January 12.

Patt, Anthony. 2015. *Transforming Energy: Solving Climate Change with Technology Policy*. Cambridge: Cambridge University Press.

Peppet, Scott R. 2014. “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent” *Texas Law Review* 93 (1): 85–176

Rachovitsa, Adamantia. 2016. “Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue.” *International Journal of Law and Information Technology* 24 (4): 374–399.

Raustiala, Kal, and David G. Victor. 2004. "The regime complex for plant genetic resources." *International Organization* 58 (2): 277–309.

Rubinstein, Ira S. 2011. “Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes.” *I/S: A Journal of Law and Policy for the Information Society* 6 (3): 355–423.

Rubinstein, Ira S. and Nathaniel Good. 2013. “Privacy by Design: a Counterfactual Analysis of Google and Facebook Privacy Incidents.” *Berkeley Technology Law Journal* 28 (2): 1333–1414.

Sandler, Karen, Lysandra Ohrstrom, Laura Moy, and Robert McVay. 2010. “Killed by Code: Software Transparency in Implantable Medical Devices." *Software Freedom Law Center*, July 21. https://www.softwarefreedom.org/resources/2010/transparent-medical-devices.pdf

Sarnoff, Joshua D. 2016. “Intellectual Property and Climate Change, with an Emphasis on Patents and Technology Transfer.” In *The Oxford Handbook of International Climate Change Law*, edited by Kevin R. Gray, Richard Tarasofsky, and Cinnamon P. Carlarne, 391-346. Oxford: Oxford University Press.

Scharpf, Fritz W. 2003. “Problem-solving Effectiveness and Democratic Accountability in the EU”. Max Planck Institute for the Study of Societies working paper, No. 03/1.

“Scottish Climate Change Bill - Call for Evidence” Accessed 30 May 2017 https://www.theccc.org.uk/wp-content/uploads/2017/03/WWF-Scotland-consultation-response.pdf

Scottish Enterprise, 2017. “Scottish Smart Grid Sector Strategy: Enabling the Low-Carbon Economy, Creating Wealth.” *Scottish Enterprise*. Accessed 14 February 2017. http://www.scottish-enterprise.com/~/media/se/resources/documents/stuv/smart%20grids%20brochure.pdf

Scottish Government. 2017. *Draft Climate Change Plan: The Draft Third Report On Policies And Proposals 2017-2032*. Edinburgh: Scottish Government.

Secretariat of the Basel Convention. Undated. “The Basel Convention MPPI.” http://archive.basel.int/industry/mppi.html

Smart Energy Code https://www.smartenergycodecompany.co.uk/ (2013)

Spier, Jaap. and Magnus, Ulrich. 2014. (eds) *Climate Change Remedies. Injunctive Relief and Criminal Law Responses* Eleven Netherlands: International Publishing.

Sutherland, Ewan. 2009. “Regulating the Energy Efficiency of ICT Equipment” *Computer and Telecommunications Law Review* 9 (8): 179–181.

Toy, Alan. 2013. “Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy” *New Zealand Universities Law Review* 25 (5): 938–959.

TRIPS Council. 2017 “Climate change and the WTO intellectual property (TRIPS) agreement”. TRIPS Council. Accessed 14 February 2017. https://www.wto.org/english/tratop_e/trips_e/cchange_e.htm

UNFCCC. 2015. Technology Executive Committee “Facilitating Technology Deployment in Distributed Renewable Electricity Generation” Accessed 30 May 2017 http://unfccc.int/ttclear/misc_/StaticFiles/gnwoerk_static/TEC_documents/5be1bf880cc34d52a4315206d54a711b/6134b1f4c4db4356999aa64c9c6fdcc8.pdf

UNFCCC. 2017. “Technology Mechanism.” UNFCCC. Accessed 14 February 2017. http://unfccc.int/ttclear/support/technology-mechanism.html

Urquhart, Lachlan. “White Noise From the White Goods? Conceptual & Empirical Perspectives on Ambient Domestic Computing.” (2016): Accessed 06 June 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865738

van Calster, Geert, Vandenberghe,. Reins, Leonie. (eds) 2015 *Research Handbook on Climate Change Mitigation Law* Cheltenham: Edward Elgar.

van Lieshout, Marc, Linda Kool, Bas van Schoonhoven, and Marjan de Jonge. 2011. “Privacy by Design: An Alternative to Existing Practice in Safeguarding Privacy.” *info* 13 (6): 55–68.

van Rest, Jeroen, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen. 2012. “Designing Privacy-by-Design.” In *Privacy Technologies and Policy*, edited by Bart Preneel and Demosthenes Ikonomou, 55–72. Heidelberg: Springer.

Westbrook, Nick and Mark Taylor. 2013. “The Internet of Things” *Computer and Telecommunications Law Review* 19(8): 244–246.

Wilkinson, Charu, Tomaso Duso, Jo Seldeslachts, Elena Argentesi, Florian W. Szücs, Albert Banal-Estanol, Veit Böckers, and Meagan Andrews. 2016. *The Economic Impact of the Enforcement of Competition Policies on the Functioning of EU Energy Markets.* Brussels: European Commission.

Yu, Peter K. 2009. "A tale of two development agendas." *Ohio Northern University Law Review* 35: 465–572.

Zuboff, Shoshana. 2015. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.” *Journal of Information Technology* 30 (1): 75–89.