Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

For privacy's sake: Consumer "opt outs" for smart meters

Nancy J. King [a,*], Pernille Wegener Jessen [b]

[a] College of Business, Oregon State University, USA
[b] School of Business and Social Sciences, Aarhus University, Denmark

Keywords:
Smart meters
Data sharing
Privacy law
Data protection
Opt out mechanisms

ABSTRACT

When balancing consumer privacy and data protection rights with the important societal benefits to be obtained from smart meters, should consumers be allowed to opt out? If so, what should a smart meter opt out mechanism look like? Further, may consumers be charged additional fees for the privilege of opting out without violating their privacy and data protection rights? The EU/U.S. comparative law analysis provided in this paper aims to help energy suppliers and regulators craft opt out mechanisms to protect individual privacy and data protection rights while also achieving important societal benefits from smart meters.

1. Introduction

"Smart metering systems enable massive collection of personal information from European [and U.S.] households with the potential intrusiveness increased by the ability to infer information from the data about what members of a household do within the privacy of their own homes."[1] Privacy concerns about smart metering systems are exacerbated because these systems typically use cloud computing, which raises its own set of privacy and data protection concerns, including the possibility of unauthorized access and use of data, improper surveillance and security breaches.[2] Additionally, it is anticipated that consumers will access their smart meter data and help manage their energy uses through mobile phone applications, which raises concerns about privacy and security in mobile contexts.[3] In both Europe and the United States, concerns about consumer privacy and data protection and concerns about other potential harms,

* *Corresponding author*. Professor of Business Law, College of Business, Oregon State University, 200 Bexell Hall, Corvallis, OR 97331, USA.
E-mail addresses: nancy.king@bus.oregonstate.edu (N.J. King), pwj@law.au.dk (P.W. Jessen).

[1] See Commission, 'Opinion of the European Data Protection Supervisor (EDPS) on the Commission Recommendation on preparations for the roll-out of smart metering systems (EDPS Opinion on Smart Metering Systems)' COM (2008) 4–6; NISTIR, 'Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, National Institute of Standards and Technology Interagency Report', NISTIR 7628 (August 2010) (NISTIR 7628); *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, Executive Office of the President of the United States, p. 60 (June 2011) (U.S. Energy Framework for the 21st Century).

[2] See, e.g., Jeff St. John, *Siemens, eMeter Push Smart Meter Data and Analytics to the Cloud*, (Greentech Media 24 October, 2013), at: <http://www.greentechmedia.com/articles/read/siemens-emeter-push-smart-meter-data-and-analytics-to-the-cloud> accessed 30 April 2014.

[3] See, e.g., Weiss et al., *Handy feedback: Connecting smart meters with mobile phones*, (in proc. MUM 2009, ACM), at: <http://www.im.ethz.ch/publications/weiss_handyFeedback_MUM09.pdf> accessed 30 April 2014; M. Weiss et al., 'Evaluating Mobile Phones as Energy Consumption Feedback Devices' in P. Sénac, M. Ott, A. Seneviratne (eds), *Mobile and Ubiquitous Systems: Computing, Networking, and Services*, (Vol. 73, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012) 63–77.

http://dx.doi.org/10.1016/j.clsr.2014.07.001

including health concerns, have caused delays in programs to roll out smart meters. In particular, questions are arising about whether consumers should be given options to keep analog meters or provided with other options that would mitigate the potential privacy-intrusiveness of smart meters.[4]

This paper addresses consumer privacy and data protection issues for smart metering implementation programs that relate to requests by customers to opt out of having a smart meter for electricity service installed in their homes.[5] Section 2 provides an overview of the technology of smart metering systems. Section 3 explores the privacy and data protection concerns related to smart meters that may justify opt out mechanisms.[6] It also discusses significant societal benefits advanced by smart metering implementation programs that may be undermined by opt out programs.[7] Section 4 compares the privacy and data protection laws of the European Union and the United States that relate to smart metering implementation programs and discusses how regulators are responding to consumer opt out requests. Finally, Section 5 recommends a balanced model opt out mechanism that will protect consumers' privacy and data protection without sacrifice of important societal benefits to be gained from using smart meters.

2. Overview of smart meter technology

Installation of residential smart meters is a key component of implementing smart metering systems. Smart metering systems feature two-way communication between the smart meter and the energy supplier and also between the smart meter and other potential third parties, a communication capability that distinguishes smart meters from more conventional meters.[8] Smart metering systems use Advanced Metering Infrastructure (AMI).[9] Smart metering systems equipped with AMI have the capacity "to collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes via two-way communications."[10] Finally, a capability that is important for privacy and data protection analysis, smart meters provide the information data and communications (ICT) capacity to measure, record and transmit very granular (meaning highly detailed, in terms of frequency of measurement and types of data) energy consumption data.[11]

3. Smart meters, individual rights and societal interests

Significant consumer privacy and data protection concerns are associated with implementation of smart metering systems that relate to a traditionally highly private arena, the home. These interests include the legal rights of people to be free from unreasonable surveillance and other intrusions into their homes and their personal and family lives.[12] Once smart metering systems are installed, such surveillance could be either overt or covert, depending on whether the consumers who are under surveillance are aware of the surveillance. For example, overt surveillance would occur if consumers have opted in to having a smart meter that monitors their household's energy use (at least to the extent that consumers' are aware of smart meter data collection and communication),

[4] For example, in the Netherlands, consumer privacy concerns led to a significant delay in the roll-out for smart meters after the Dutch Senate rejected a proposal for mandatory smart metering deployment. European Smart Metering Landscape Report 2012, SmartRegions Deliverable 2.1, Vienna, pp. 58–60 (October 2012) (European Smart Metering Landscape Report 2012). See also, Angela Beniwal, 'Utilities Are Getting Ahead Of Smart Meter Opt-Out Demands', (Renew Grid 28 February 2012) (reporting on the California Public Utility Commission's mandate of opt outs and the opt out programs put in place by utilities in California that charge customers who elect to retain or return to an analog meter an initial fee of $75 and a monthly charge of $10; low-income customers who opt out are charged an initial fee of $10 and a monthly charge of $5).

[5] A comprehensive analysis of the broad range of privacy concerns related to data sharing in smart metering implementation programs is provided in our first paper. See Nancy J. King and Pernille W. Jessen, 'Smart Metering Systems and Data Sharing: Why Getting a Smart Meter Should Also Mean Getting Strong Information Privacy Controls to Manage Data Sharing', (2014) International Journal of Law and Information Technology (http://dx.doi.org/10.1093/ijlit/eau001). In contrast, this paper focuses on the desirability of consumer opt outs for purposes of privacy and data protection and proposes a balanced opt out mechanism.

[6] See, e.g., Commission, 'Commission's Recommendation of 9 March 2012 on preparation for the roll-out of smart metering systems' (Commission's Recommendation on Smart Metering Systems) COM (2012/148/EU), OJ 2012 L 73/11, note 1; Article 29 Data Protection Working Party's Opinion 12/2011 on smart metering, p. 2, 00671/11/EN/WP 183 (4 April 2011) (Art. 29 Opinion 12/2011); EDPS Opinion on Smart Metering Systems, (fn 1), 2. For discussion of the distinction between data protection and broader personal privacy notions that include personal liberty and autonomy, see Luiz Costa and Yves Poullet, 'Privacy and Regulation of 2012', (2012) 28 3 Computer Law & Security Review 254.

[7] See Joseph Savirimuthu, 'Smart meters and the information panopticon: beyond the rhetoric of compliance', (2013) 27 1–2 International Review of Law, Computers & Technology 161.

[8] Commission's Recommendation on Smart Metering Systems, (fn 6) para. 3(b).

[9] Communications Requirements of Smart Grid Technologies, U.S. Department of Energy, 12 (5 October 2012). The U.S. Federal Energy Regulatory Commission (FERC) defines AMI as "meters that measure and record usage data at hourly intervals or more frequently, and provide usage data to both consumers and energy companies at least once daily".

[10] Communications Requirements of Smart Grid Technologies, (fn 9) 9.

[11] Data Access and Privacy Issues Related to Smart Grid Technologies, U.S. Department of Energy, pp. 6, 9 (5 October 2010) (DOE Data Access and Privacy Report).

[12] EDPS Opinion on Smart Metering Systems, (fn 1) 4–6; David Wright and others, 'Sorting out smart surveillance' (2010) 26 Computer Law & Security Review 343. Where there is surveillance, there will be leaks and there is a need for more research about the security issues related to smart meters including data breaches. An EU proposed directive on cyber security covers data breach reporting of utility companies such as electric and gas companies. See Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48 final, p. 14.

while covert surveillance would presumably include surveillance that occurs after consumers have opted out of having a smart meter.[13]

There are also significant personal data concerns because "smart metering systems produce highly detailed energy usage data at the household level,"[14] including the ability to measure, record and transmit granular individual energy consumption data on a near real-time basis.[15] For example, depending on the granularity of energy use data collected and communicated by particular smart metering systems, these devices may enable persons outside the home to remotely monitor activities in the home, potentially revealing when the home is occupied, what specific appliances are used in the residence, when an individual household appliance is turned on or off, and providing a detailed picture of energy usage in the home over a long period of time that reveals patterns of energy use from which human behavior in the home can be inferred.[16] Further, implementation of smart metering systems raises important privacy and data protection concerns that are exacerbated by the availability of other sources of personal data that could be combined with energy-use data to produce highly-detailed consumer profiles. Smart meter data and related consumer energy-use profiles could be used for secondary purposes not directly related to delivery of electricity, including direct marketing and unfair price discrimination (charging some consumers more than other consumers for the same goods and services without justification).[17]

Citing privacy and other concerns, some consumers have objected to having smart meters installed in their homes.[18] When consumers object to smart meters and are allowed to opt out (in some cases, opt out may mean modifying or disabling the meter's monitoring and communication capabilities, or it may mean choosing a meter that has not been equipped with AMI), they are taking action to prevent potential privacy and data protection intrusions associated with having a smart meter by excluding the device that is capable of monitoring and communicating energy use data from their homes. However, such opt outs do not come without societal costs as consumer opt outs may also hinder achieving societal benefits from smart meters, as next described.

It is anticipated that significant societal benefits will flow from implementation of smart metering systems that relate to protecting the environment, improving energy management and promoting new economic opportunities for businesses. For example, installation of smart meters may facilitate better management of the energy supply and lessen society's dependence on fossil fuels by making it possible to improve: operational efficiency, reliability of delivery, energy conservation and use of renewable power.[19] Consumers with smart meters may be able to take advantage of dynamic pricing models that adjust the price of energy for peak and off peak periods, thus reducing their energy costs.[20] Additionally, smart meter installation programs may create new economic opportunities for energy suppliers or third party businesses that are likely to be based on selling access to smart meter data or providing services related to the availability of smart meter data. Such opportunities are likely to include helping consumers to better manage their households' energy consumption and delivering targeted behavioral advertising to consumers.[21]

A wide variety of third parties may be interested in accessing smart-metering data and they may claim to be negatively impacted by allowing consumers to opt out of having a smart meter installed in their homes. Potentially interested third-parties include: law enforcement agencies, tax authorities, insurance companies, landlords, employers, commercial data banks, appliance and equipment makers, participants in the online behavioral advertising industry and companies offering consumer energy management related services.[22] For example, allowing consumers to opt out may prevent collection of data that would facilitate delivery of targeted advertising solicitations to those consumers. It may also prevent use of energy use data by: landlords to identify potential lease violations, such as occupancy by an unauthorized guest; life insurance companies to assess higher premiums based on negative evaluation of the insured's energy

[13] See generally, Charles A. Sennewald and John Tsukayama, *The Process of Investigation*, (3rd edn, Butterworth–Heinemann 2006), Chapter 6: (describing covert versus overt surveillance).

[14] DOE Data Access and Privacy Report, (fn 11) 9. This type of data is consumer-specific energy-usage data (CEUD). Ibid.

[15] DOE Data Access and Privacy Report, (fn 11) 20; Art. 29 Opinion 12/2011, (fn 6) 9.

[16] EDPS Opinion on Smart Metering Systems, (fn 1) 5.

[17] EDPS Opinion on Smart Metering Systems, (fn 1) 6 (profiling may also increase the information imbalance between consumers and energy suppliers or other third parties who wish to market goods and services to consumers); Art. 29 Opinion 12/2011, (fn 6) 21 (use in criminal investigations, etc.). See also, Parmy Olson, 'This Landmark Study Could Reveal How the Web Discriminates Against You' (2013) Forbes (discussing a study by researchers at Princeton University and Belgium's KU Leuven that will enable comparison of search results, prices, ads, offers and emails in response to fake online profiles to look for patterns and measure what kind of discrimination is happening across different sites).

[18] European Smart Metering Landscape Report 2012, (fn 4) 58–60. Analysis of potential health risks associated with smart meters is beyond the scope of this paper, but government regulators have found no significant health risks associated with smart meters. See Jeff Evans, 'The Opt-Out Challenge' (2012) Black & Veatch issue of Electric Light & Power.

[19] Simone Pront-van Bommel, 'Smart Energy Grids within the Framework of the Third Energy Package' (2011) European Energy and Environmental Law Review 32; Paul Lewis Joskow, 'Creating a Smarter U.S. Electricity Grid' (2012) 26 1 Journal of Economic Perspectives 29.

[20] EDPS Opinion on Smart Metering Systems, (fn 1) 4 (describing 'demand-response,' 'dynamic' or 'time of use' pricing for electricity that allows customers to buy electricity at constantly changing prices, thereby cutting demand at peak times and facilitating better integration of renewable energy sources).

[21] EDPS Opinion on Smart Metering Systems, (fn 1) 5–6 (smart meter data may be used for consumer profiling including generation of targeted and personalized advertising).

[22] EDPS Opinion on Smart Metering Systems, (fn 1) 5–6. Third-party requests to utilities for data about their customers' energy usage have come from many sources: energy services providers, law enforcement, regulators, attorneys, researchers, municipalities and real estate agents. Angelique Carson, 'Consumer data privacy concerns persist in smart grid plans' (2011) The Privacy Advisor.

use patterns; and law enforcement to identify energy use patterns that indicate growing marijuana in the home.

4. Comparing EU and U.S. laws regarding privacy and data protection

The installation of smart meters is a necessary prerequisite to implementation of smart grids.[23] In fact, unless one of the exceptions applies, EU Member States are required by the Energy Services Directive to ensure implementation of smart metering systems that help consumers actively participate in the electricity supply market.[24] There is no analogous federal legislation in the United States that mandates installation of smart meters in customers' homes. Instead, these decisions are left to the public or privately-owned energy suppliers ("utilities"), which are regulated by public utility commissions (PUCs) in the fifty states.[25] Leaving regulation of the smart grid to the states is consistent with the U.S. view that state public utility commissions, as opposed to federal regulatory agencies, should have regulatory authority over public utilities including energy suppliers.[26] Although the smart grid and smart metering systems are primarily regulated at the state level by PUCs, the U.S. government has an important policy-making and oversight role and the federal government has provided substantial financial incentives to encourage smart grid development that have helped fund smart meter installation programs.[27]

Currently there is no EU or U.S. legislation that expressly addresses privacy or data protection issues related to implementation of smart metering systems or that mandates offering smart meter opt out mechanisms to consumers. As described below, some Member States and some state PUCs have created opt out mechanisms for energy consumers within their jurisdictions, but not all consumers in all jurisdictions have been provided opt out mechanisms. Further, where opt out mechanisms have been made available to consumers in the EU and the U.S., there is a wide disparity in these mechanisms and any applicable fees for opting out. EU and U.S. regulators need to address whether an opt out mechanism for smart meters should be made available to consumers given their privacy and data protection concerns and the corresponding societal benefits for implementing smart meter programs, and if so, at what cost, if any, to those who opt out.

4.1. *The EU perspective*

The starting point in the EU is Article 8 of the European Convention on Human Rights (ECHR), which protects an individual's "right to respect for his or her private and family life, home and correspondence".[28] Personal data protection is also explicitly mandated by the EU's Data Protection Directive (Directive) and Member States' implementing legislation in the form of general data protection principles that apply to all processing of EU residents' personal data.[29] Further, the E-Privacy Directive ensures privacy and data protection in the electronics communication sector.[30]

Although EU privacy and data protection legislation does not explicitly address smart meter implementation programs and opt out mechanisms, it is clear that this comprehensive legislative and regulatory framework for personal privacy and data protection is applicable to the collection and processing of energy use data in smart metering systems. The applicability of EU law to smart metering systems is supported by various sources of EU soft law, including opinions by the EU's Data Protection Supervisor and the Article 29 Working Party, which offer specific guidance on how the Data Protection Directive should apply in the context of smart metering systems, and a Recommendation from the European Commission

[23] EDPS Opinion on Smart Metering Systems, (fn 1) 4.

[24] Art. 13 of the Directive 2006/32 of 5 April 2006 on the energy end-use efficiency and energy services and repealing council Directive 93/76, OJ 2006 L 114/64, (Energy Services Directive). See also, Ann-Sofie Vanwinsen, 'Smart Grids: Legal Growing Pains' (2012) 21 European Energy and Environmental Law Review 142 (the Energy Services Directive requires Member States to ensure final customers are provided with affordable individual meters, but installation of smart meters is not mandatory in all circumstances as there are three justifications for not requiring installation: technical impossibility, financial unreasonability and disproportionate benefit in relation to the potential energy savings).

[25] There are estimated to be over 3000 electrical energy suppliers in the U.S.; over 25 U.S. states have already adopted policies regarding smart grid technology. U.S. Energy Framework for the 21st Century, (fn 1) 2.

[26] John R. Forbush, 'Regulating the Use and Sharing of Energy Consumption Data: Assessing California's SB 1476 Smart Meter Privacy Statute' (2011/2012) 75 Albany Law Review 341; NISTIR 7628, (fn 1).

[27] The National Science and Technology Council (NSTC) Subcommittee on Smart Grid has taken the lead to outline the federal policy framework on the smart grid. U.S. Energy Framework for the 21st Century, (fn 1) 2. See also, Russell Frisby and Jonathan Trotta, 'The Smart Grid: The Complexities and Importance of Data Privacy and Security' (2011) 19 CommLaw Conspectus 297.

[28] See Treaty of Lisbon amending the Treaty on European Union, the Treaty establishing the European Community, OJ 2007 C 306/1, (recognizing Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and requiring Members of the European Union to respect the fundamental rights guaranteed by the Convention). Article 8 of the ECHR goes beyond data protection, "covering all activities regarded as constituting private and family life," and providing an "extra layer of safeguards for physical, personal and psychological development." Savirimuthu, (fn 7) 172. A similar wording is found in the Charter of Fundamental Rights of the European Union, OJ 2000 C 364/1 (the Charter), Article 7: "Everyone has the right to respect for his or her private and family life, home and communications."

[29] See generally, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31, (Data Protection Directive); Proposal of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (25 January 2012) (Draft Data Protection Regulation).

[30] See generally, Directive of the European Parliament and of the Council 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular E-Commerce, in the Internal Market, OJ L. 178/1,17.07. 2000 (E-Privacy Directive).

on the roll-out of smart metering systems that includes a significant discussion of data protection.[31] Further, some Member States have adopted legislation or regulatory guidance directly addressing privacy and data protection concerns related implementing smart metering systems.[32]

4.2. *The U.S. perspective*

In contrast to the EU, one must examine many sources of U.S. law to see if any laws are applicable to privacy and data protection in smart metering systems because a comprehensive legal framework for information privacy does not exist in the U.S. Although there is generally an absence of statutory privacy or personal data protection law that could be applied to smart metering systems, U.S. laws (primarily found in state privacy tort laws and state and federal constitutional rights) have long protected individual privacy from unreasonable intrusions, including the right of people to privacy in their homes and personal communications.[33] Further, federal statutes restrict interception of electronic communications and unauthorized access to consumers' stored electronic communications, as may occur when smart metering systems are hacked.[34] And there are industry-specific federal laws protecting information privacy related to personal health information collected by health providers, financial data collected by financial institutions, consumer credit data collected by consumer credit reporting agencies and data collected online by websites that relate to children under the age of thirteen. However, given the industry-specific nature of existing privacy statutes (and apart from potential application of constitutional and tort laws), it is likely that smart meter data will receive little privacy protection under current U.S. laws as it does not fall within the scope of existing legal protections.

Where there is no applicable federal law, regulation of privacy and data protection in smart metering systems is left to the states and this is typically the responsibility of state legislatures or state PUCs that regulate energy suppliers.[35] If the state legislature or PUC has not adopted any data protection rules regarding smart metering systems and if other sources of state law do not apply (see above discussion of state tort laws including privacy torts and constitutional protections), then the matter is left to industry self-regulation. In the context of industry self-regulation, energy suppliers and third party businesses that collect and use smart meter data may choose whether to give consumers privacy and data protection rights, for example, by promising such rights under voluntarily adopted privacy policies.[36] A business's failure to follow its own voluntarily-adopted privacy policy and its failure to protect customers' sensitive personal data (even in the absence of any applicable privacy policy) has been found to violate consumer protection laws.[37]

Some states have acted to fill the regulatory gap related to privacy in smart metering systems. For example, California's PUC has adopted rules covering the privacy and security of smart metering data. Under these rules, customers have specified judicial and administrative remedies available for privacy and data protection violations in smart metering programs.[38] Currently, only a few states have adopted legislation or administrative rules regulating privacy and smart meters.

A U.S. Department of Energy task force was recently formed to address consumer privacy and smart grids. One of its key responsibilities is to craft a voluntary smart grid privacy code of conduct.[39] It remains to be seen whether this code of conduct will include a smart meter opt out

[31] See generally, Commission's Recommendation on Smart Metering Systems, (fn 6); EDPS Opinion on Smart Metering Systems, (fn 1); Art. 29 Opinion 12/2011, (fn 6).

[32] See Art. 29 Opinion 12/2011, (fn 6), 15 ("in some member states the possibility for the data subject to object to installation of the smart meter exists and that in such cases the data subject's preferences override any other interests"); European Smart Metering Landscape Report 2012, (fn 4) (summarizing legislation and proposed legislation in EU Member States regarding smart meter implementation programs). See also, the proposed regulatory guidance on data access and privacy for smart metering programs in the United Kingdom. UK Smart Metering Implementation Programme, Data Access and Privacy, Consultation Document, Department of Energy & Climate Change, United Kingdom, pp. 21–23 (April 2012) (U.K. Smart Meter Consultation Document); Smart Metering Implementation Programme, Data Access and Privacy, Government Response to Consultation, Department of Energy & Climate Change, United Kingdom, pp. 30–32 (December 2012) (UK Government Response to Consultation).

[33] U.S. scholars have been instrumental in developing arguments that personhood, or the right to define one's self, is a core privacy value to be protected by law. Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1980) 4 Harvard Law Review 193 (arguing individuals have a "right to be let alone"); Nancy King, 'Fundamental Human Right Principle Inspires U.S. Data Privacy Law, But Protection Are Less Than Fundamental' in Maria Verónica Pérez Asinari and Pablo Andrés Palazzi (eds), *Challenges of Privacy and Data Protection Law* (Cahiers Du Centre De Recherches Informatique Et Droit, Bruylant 2008).

[34] Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq. (2012); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq. (2012). Exceptions under these laws provide avenues for lawful access to electronic communications by providers of electronic communications and when the user has given authorization/consent.

[35] California has laws governing privacy and data protection in smart metering implementation systems. See California Public Utility Code, § 8380 (2012) (CPUC § 8380); Decision Adopting Rules to Protect 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, Rulemaking 08-12-009, California Public Utilities Commission (29 July 2011) (CUPC Rulemaking 08-12-009).

[36] See Michael Pryor, 'The White House Consumer Privacy Bill of Rights: Implication for Smart Grid Privacy Regulation' (2012) Smart Grid Update, DowLohnes, PLLC.

[37] Federal and state consumer protection laws protect consumers from unfair and deceptive business practices. See, eg, Section 5 of the Federal Trade Commission Act, which the Federal Trade Commission has interpreted to cover a business's failure to protect sensitive consumer data and failure to keep promises in privacy policies, Federal Trade Commission Act, 15 U.S.C. § 45 (2012).

[38] CPUC § 8380, (fn 32) (defining electrical or gas consumption data and establishing information privacy requirements for such); CUPC Rulemaking 08-12-009, (fn 35).

[39] Angelique Carson, 'Stakeholders Aim to Craft Smart Grid Privacy Code of Conduct', (2013) The Privacy Advisor.

mechanism. Another recent development that can be characterized as industry self-regulation is the creation of a voluntary smart grid privacy seal program for companies that use consumer energy data.[40] This privacy seal program does not require participating businesses to offer consumers the choice to opt out of having a smart meter installed in their homes or to provide other opt out mechanisms, such as the right to have a smart meter modified to limit collection and communication of smart meter data. Nor does the privacy seal program address whether an energy supplier may charge fees to consumers who opt out.

Despite their limitations, these recent developments provide helpful but non-binding guidance for energy suppliers, third party businesses and state public utility commissions that are engaged in designing practices and policies to protect consumers' information privacy. However, unless Congress takes the legislative step of enacting a federal law to address information privacy in smart metering systems (for example, Congress could enact a statute that incorporates the National Institute of Standards and Technology's guidelines for privacy and the smart grid) or enact other legislation (such as comprehensive data protection legislation of general applicability to consumer data including smart meter data), it is not likely that there will be federal information privacy law in the United States that protects consumers' privacy in this context.[41] If Congress does not act, it is still possible that other states may follow California's lead and decide to mandate consumer privacy in smart metering systems through state legislation or rulings of their PUCs.

4.3. *Comparison of opt out mechanisms*

Across the U.S., consumers continue to challenge smart metering implementation programs for a variety of privacy, health, or other reasons, including demanding the right to opt out and challenging the reasonableness of opt out fees.[42] In response, PUCs in Maine, Oregon and California require energy suppliers in their states to provide opt out programs.[43] Several other states are considering whether to require energy suppliers to provide opt out programs.[44] In states where the right to opt out is provided, there may be fees imposed on consumers who opt out and the amount of the fees may vary considerably depending on the state in which the consumer resides and on the business practices of the particular energy supplier that provides the electricity to the consumer. For example, the Oregon Public Utility Commission requires electrical energy suppliers in Oregon to have opt out programs, although the fees charged consumers for opting out differ depending on which supplier serves the customer. In Portland, Oregon, the fee for opting out of a smart meter to be installed by Portland General Electric is $254, with additional monthly charges of $51 per month for the length of time of the opt out. By way of comparison, the City of Ashland, Oregon allows its customers to opt out of having a smart meter without requiring customers to pay any additional charges.[45] Some states (including Maine) have proposed legislation to repeal or prohibit opt out charges imposed by energy suppliers on consumers in their states who opt out.[46]

Two U.S. Courts have held smart metering implementation programs that provide opt out mechanisms do not violate consumers' privacy rights.[47] The opt out mechanism provided by an energy supplier in Maine gave customers two opt out choices: 1) have an analog meter installed in the home instead of a smart meter, for an initial cost of $40 for the installation and additional fees of $12 per month for as long as the consumer continues to opt out; or, 2) keep the smart meter that has been installed in the home and have the radio communications from the meter disabled, for a one-time fee of $20, and additional fees of $10.50 per month for as long as the opt out continues. The court rejected consumers' claims that the energy supplier's opt out program was unlawful because it included opt out fees that were so large as to be unreasonable, unjust and discriminatory. Instead, the court agreed with the energy supplier's argument that its opt out fees were justified due to incremental costs of opt outs that were imposed on suppliers, including longer repair times for power restoration after storms and ongoing inefficient energy allocation to those customers using analog meters.[48]

In the EU, consumers in some Member States also have the option to object to installation of a smart meter in their homes.[49] For example, Dutch consumers have the option of refusing a smart meter and keeping their traditional meter.[50] Dutch consumers may exercise the right to opt out without having to pay any direct fees like the consumer opt out fees imposed in some U.S. states by energy suppliers.

[40] See Privacy Smart, Powered by TRUSTe <http://www.futureofprivacy.org/issues/smart-grid/> accessed 30 April 2014. This privacy seal covers companies that seek to access consumer energy data but the seal does not cover collection or use of data by energy suppliers for billing, operations, demand response, or for first party marketing.

[41] Alternatively, Congress could give a federal administrative agency, such as the Department of Commerce, authority to adopt administrative rules to protect consumers' privacy with regard to their smart meter data. Currently, because no federal or state laws (with some exceptions, as in California) provide specific information privacy protections for consumers' in smart metering systems, the privacy of smart metering data is protected only by weak consumer protection laws and industry self-regulation. See Frisby and Trotta, (fn 27) 339; DOE Access and Privacy Report, note (fn 11) 15.

[42] See generally, Evans, (fn 15).

[43] Evans, (fn 18), 4; Renew Grid, (fn 4).

[44] Ibid.

[45] Ibid.

[46] Evans, (fn 18).

[47] *Friedman and others v. Public Utilities Commission*, 2012 ME 90 (Maine Supreme Judicial Court, 12 July 2012); *Naperville Smart Meter Awareness v. City of Naperville*, No. 11 C 9299 (N. District of Illinois, 22 March 2013).

[48] N. Shah, 'Maine Supreme Court Affirms Validity of Smart Meter Opt-Out Program' (2012) Information Law Group 1 <http://www.infolawgroup.com/2012/08/articles/smart-grid-1/maine-supreme-court-affirms-validity-of-smart-meter-optout-program/> accessed 30 April 2014.

[49] Art. 29 Opinion 12/2011, (fn 6) 5 (commenting that this right to opt out may override all other interests).

[50] European Smart Metering Landscape Report 2012, (fn 4) 7–8 (describing provisions of the Dutch Electricity and the Gas Act that was approved in 2011 giving customers legal choices over whether they accept a smart meter; their choices range from "having no smart meter at all to [having] a smart meter with full functionality to provide interval data to the network operator and chosen service provider").

In other Member States, consumers may have no legal right to opt out of having a smart meter (compulsory or mandatory smart meter implementation programs), although consumer opt in or opt out rights may be legislated for collection and use of energy-consumption data by energy suppliers and third parties. For example, in the United Kingdom, implementation of smart metering systems is underway by suppliers and protection of consumers' privacy and personal data is included in suppliers' licensing terms. Under the licensing terms, the energy supplier: may collect monthly (or less granular) smart meter readings for billing and regulated purposes without obtaining consumer consent; may collect daily (or less granular) smart meter readings with opt out consumer consent; and may collect half-hourly smart meter readings only with opt in consumer consent.[51] consumers' retain full control about usage of daily smart meter data for purposes other than billing and regulated purposes, and may allow suppliers access to their daily smart meter data for some purposes (e.g., provision of energy efficiency advice), while refusing its use for other purposes (e.g., for wholesale hedging).[52] No matter the granularity of the energy use data that is involved, energy suppliers must obtain consumers' opt in consent to use energy consumption data from smart meters for marketing purposes.[53]

Consumers in the U.K. have the right to opt out of trial programs that relate to energy suppliers' collection and use of half-hourly energy consumption data, and these types of trial programs, which may collect very granular energy consumption data, require approval by government regulators.[54] Finally, in some Member States, installation of smart meters is compulsory and consumers do not currently have legal opt out rights in terms of refusing a smart meter or rights to limit collection and communication of energy consumption data.

Although health concerns about smart meters are not within the primary thrust of this paper, opt out mechanisms may be offered in order to assuage consumers' concerns about a variety of things, including health as well as personal privacy. Concerns about the public health consequences of consumers being exposed to radio frequency transmissions from smart meters and other wireless devices have been raised in Europe as well as in the United States.[55] For example, in Italy there have been two High Court judgments issued that recognize claims of adverse health effects from wireless transmissions such as mobile phones.[56] It is also conceivable that insurance companies may decline to cover liability for health effects from electromagnetic radiation.[57]

From the European perspective, the European Data Protection Supervisor (EDPS) recommends offering consumers the choice of not switching to smart meters, particularly when they do not wish to take advantage of time of use tariffs or other services based on smart meter functionalities (for privacy reasons, health reasons, or otherwise).[58] Alternatively, the EDPS recommends that consumers be given the option of having a smart meter installed, but having the meter's smart functionalities disabled, including disabling the meter from making granular readings and disabling the meter's remote on/off control switch (thus restricting the energy supplier's ability to remotely disconnect the consumer's power). The EDPS also recommends following principles of data minimization and requiring energy suppliers to obtain explicit consent to collect smart meter data beyond that necessary for providing energy, billing, detecting fraud and preparing aggregate data to maintain the energy grid. This latter recommendation would help protect consumers' privacy and data protection rights in smart metering implementation programs even when there is no opt out mechanism available to consumers.

5. Recommendation on opt out mechanisms

Having articulated and examined the privacy and data protection concerns consumers have that relate to having a smart meter installed in their homes and the relevant societal benefits to be gained from smart metering implementation programs, we come to the conclusion that opt out mechanisms should be offered to consumers that are consistent with balancing personal privacy and societal interests. Because the societal benefits to be achieved from smart metering implementation programs are important, we do not believe that opt in mechanisms requiring consumer consent to installation of smart meters is appropriate, because requiring advance and explicit consumer consent to all smart meter installations would greatly burden such programs and make it unlikely that the societal benefits of the programs could be achieved. However, we conclude that an opt out mechanism is necessary to give consumers the opportunity to object to smart meters in order to protect their privacy and personal data. When regulators are crafting such opt out mechanisms, the societal benefits to be achieved by smart metering programs should be compared with the related costs or burdens that will be borne by energy suppliers as well as customers, including both financial costs as well as non-monetary costs, such as intrusions into their privacy and personal data.[59] Having concluded that consumers' privacy and data protection rights should be recognized and protected in smart metering implementation programs and that an opt out mechanism is desirable for this purpose, what type of opt out mechanism should be offered? There are two parts to answering this question.

[51] UK Government Response to Consultation, (fn 32), 22.
[52] UK Government Response to Consultation, (fn 32), 24.
[53] UK Government Response to Consultation, (fn 32), 24–25.
[54] UK Government Response to Consultation, (fn 32), 25–27.
[55] The two U.S. court cases discussed earlier also discussed health concerns about smart meters that were raised by consumers (fn 47).
[56] Corte di Cassazz. 12.10.2012 Brescia Caso Marcolini and Cass. Civ. Sez. Lavoro, Sentenza n. 17438 del 12.10.2012. See also Corte Costituzionale Sentenza TAR Trentino Alto Adige Sez.I, 08.07. 2010, n. 171.
[57] See generally, Roseanne White Geisel, 'Insurers exclude risks associated with electromagnetic radiation' (2007) 41 23 Business Insurance 12.
[58] EDPS Opinion on Smart Metering, (fn 1) 11.
[59] See European Smart Metering Landscape Report 2012, (fn 4), 93 (discussing the balancing required between individual privacy and achieving societal goals in smart metering implementation programs).

First, what type of opt out mechanism should be included in a smart metering implementation program? From an information privacy perspective, choosing not to have a smart meter device installed in their homes is the ultimate opt out for consumers. This is so because such an opt out mechanism excludes the device that makes it possible for energy suppliers and others to initially collect household-level energy-use data, effectively precluding collection, use and subsequent sharing and processing of that data. A less drastic option would be to allow the consumer to choose to have a smart meter installed in the home that minimizes the collection of granular energy-use data, such as one that has been modified through programming of the device to collect and communicate only energy use data that are necessary to deliver energy to the consumer or that are essential to management of the energy grid. This latter option is preferable because it achieves a better balance between protecting consumers' privacy and personal data and achieving important societal interests that support participation in smart metering systems, such as promoting better management of the energy supply and improving energy conservation. Modifying the data collection and communication capabilities of smart meters also helps prevent privacy intrusive secondary uses of smart meter data by energy suppliers and third parties that are unrelated to the direct provision of energy, such as the use of granular household energy use data for behavioral advertising purposes.

Second, is it lawful (and equitable) for energy suppliers to charge consumers additional fees for opting out? Currently additional fees for opting out do not appear to be included in opt out mechanisms available to consumers in the European Union, but they are common in the United States. As in the *Friedman v PUC* case discussed earlier, energy suppliers argue that it is fair to charge additional fees to consumers who opt out because such opt outs result in additional expenses for energy suppliers and undermine potential societal benefits of smart metering systems.[60] From an information privacy perspective, we think much caution should be exercised in determining the amount of fees that energy suppliers may charge consumers who opt out. We reach this conclusion having considered that opt out fees may unfairly incentivize consumers to give up their information privacy rights at a time when exercising an opt out is viewed as increasing their energy bills without tangible benefit.

To the extent that the necessary purposes of smart metering systems can be achieved without charging customers for opting out, no opt out fees should be charged to customers who opt out. This is so because it is recognized that energy suppliers do not need data from all households to manage the energy supply, and many of the important societal benefits of the smart grid may be achieved without each household sharing granular energy use data.[61] However, if opt outs become prevalent among energy suppliers' customers, there may be insufficient data collected through smart meters to facilitate management of the energy supply and otherwise to achieve the societal benefits anticipated from the smart grid.[62] A reasonable balance of the relevant interests is to charge consumers no (or low) fees to opt out and to have energy suppliers and government regulators engage in ongoing assessment of the success or lack of success of smart meter implementation programs in terms of meeting the societal goals of the programs.

This ongoing assessment of impact of opt outs should examine whether the prevalence of opt outs is impacting the success of a smart metering implementation program. To determine the impact, it will be important to identify the essential societal goals of smart metering implementation programs and to distinguish purely commercial uses of smart metering data, such as secondary uses to generate behavioral advertising revenues, from the primary societal goals that relate to delivering energy to customers and better managing the energy supply. In some cases there may be evidence that opt outs result in significant additional expenses for energy suppliers, as was recognized by the court in Maine to include longer repair times to restore energy services after storms and ongoing inefficient energy allocation related to providing services to customers who have opted out.[63] In these cases, it may be anticipated that some government regulators, particularly those in the U.S. where consumers' privacy and data protection rights are weak, may determine that these types of expenses related to opt outs should be borne by consumers who opt out, as opposed to being passed on to all customers through general rate increases. In such cases, there should be a mechanism to make sure any opt out fees to be imposed directly on consumers who opt out are reasonable in light of the additional expenses incurred by energy suppliers that relate to such opt outs. Finally, it may also be important to correlate the applicable fees for opting out to the income of those who opt out, such that lower-income customers pay lower fees.[64] The adjustment of opt out fees for income level is needed to ensure that the cost of exercising one's privacy and data protection rights is not so high that it makes privacy and data protection out of reach to customers who have limited resources.

If challenged by consumers on consumer privacy and data protection grounds, an opt out mechanism as described above is likely to be upheld by the courts in the United States, where consumers do not have broad information privacy rights and privacy and data protection is not generally viewed as a fundamental human right in the context of commercial uses of that data.[65] But is it lawful to charge opt out fees to EU consumers who do have fundamental human rights of privacy and data protection that apply in all contexts including smart metering systems? The answer will likely depend on whether smart meter implementation programs and the personal data processing that these programs entail constitute lawful

[60] See European Smart Metering Landscape Report 2012, (fn 4) 59 (noting beneficial items include energy savings, savings on call center costs, a lower cost level as a result of the market, and savings in meter reading costs).

[61] Evans, (fn 18), 5–6.

[62] Evans, (fn 18) 5–6 (additional cost to the energy supplier could also result if too few customers opt out).

[63] Discussed at fn 48.

[64] Renew Grid, (fn 4) (providing an example of reduced opt out fees for low income customers in California).

[65] See previous discussion of the two U.S. court cases cited in fn 47.

processing that is permitted without the data subject's consent.[66] Further, it will entail balancing individuals' fundamental human rights of privacy and data protection in smart metering systems with competing interests of the larger society that are to be derived from smart grids and smart metering systems.[67] If no opt out mechanism is provided or the fees required to opt out are too onerous, consumers may rightly claim they are being unlawfully forced to give up their fundamental rights of privacy and data protection without proper justification. Further, recent research indicates that consumers are typically not willing to pay significantly higher costs for goods to obtain enhanced information privacy.[68] So, even if smart meter opt out fees are imposed that are consistent with preserving consumers' fundamental human rights of privacy and data protection, these fees may still be high enough to deter many privacy conscious people from opting out of participation in smart metering programs. And, this begs the question of whether charging consumers to exercise their fundamental rights of privacy and data protection can ever be justified.

In a recent preliminary ruling delivered by the European Court of Justice, the Court assessed the validity of the Data Retention Directive.[69] The question raised was, in particular, whether the data of subscribers and registered users – in light of Article 7 of the Charter – could be retained by the service provider, and whether the Directive met the requirements for the protection of personal data arising from Article 8 of the Charter.[70]

First, the Court examined whether the Directive established an interference with the fundamental rights to privacy and to the protection of personal data. Finding that there was in fact a wide-ranging and particular serious interference,[71] the Court then examined whether this interference could be justified in accordance with Article 52(1) of the Charter. This article provides that any limitation on the exercise of the rights and freedoms laid down in the Charter must be provided by law, respect the essence of those rights and freedoms, and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms. The Court held that the retention of data for the particular purpose of the Directive, genuinely did satisfy an objective of general interest,[72] but that the interference exceeded the limits of what was necessary to achieve this objective and, consequently, that the limits imposed by compliance with the principle of proportionality in light of Article 7, 8 and 52(1) of the Charter were also exceeded.[73]

It is very likely that the balancing between the legitimate objective pursued by the means of installing smart meters in homes and the limits provided by the EU principle of proportionality will also be decisive on the issue of whether consumers may be charged opt out fees to exercise their fundamental rights of privacy. If challenged in the Court, it is not likely that the inclusion of opt out fees in smart metering implementation programs would be considered either appropriate or necessary to achieve the objectives of the programs, and, in any case, it seems that the imposition of opt out fees on consumers would have to be laid down by law in the EU Member States in order to meet conditions similar to those stated in the EU Charter Article 52(1).

6. Conclusions

Society will benefit from achieving energy conservation and other improvements in energy management that are likely to flow from smart metering implementation programs, but these benefits should not come at the expense of undue sacrifice of consumers' rights to privacy and data protection. The right to be free of unnecessary and intrusive surveillance in the home and of one's personal communications is recognized under both EU and U.S. law, and energy consumers have significant concerns related to this traditionally private arena that are implicated by installation and operation of smart meters in their homes. Accordingly, consumers in both the EU and the U.S. should be provided with opt out mechanisms that respect their rights to privacy and data protection, provided these mechanisms do not significantly frustrate achievement of important societal benefits that can be gained from smart meter implementation programs.

However, not all of the societal benefits to be achieved from smart meters are equally important, and it will be imperative to reach consensus about which societal benefits are essential. Some potential societal benefits, including those that are related to secondary uses of smart meter data that have commercial value but are not directly related to delivering energy to the supplier or better managing the smart grid, should be found to be subordinate to consumers' privacy and data protection rights. Use of smart meter data for direct marketing of products and services to consumers is a prime example of a use that is not essential to smart metering implementation programs.

Accordingly, consumers should be allowed to opt out of privacy intrusive smart metering implementation programs, which should include having the choice of smart meters that

[66] Data Protection Directive, (fn 29), Art. 7; EDPS Opinion on Smart Metering Systems, (fn 1) 10–11.

[67] The fundamental rights to privacy and data protection are not unlimited and exceptions permit interference with those rights in accordance with the law and when necessary in a democratic society for national security, public safety or the economic well-being of the country, or for other specified reasons. ECHR, (fn 28), Art. 8.

[68] Nicola Jentzsch and others, *Study on monetising privacy: An economic model for pricing personal information* (Heraklion, 2012).

[69] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland LTD, ruling of 8 April 2014 (not yet reported) concerning the validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105/54, (Data Retention Directive).

[70] Para. 30. As earlier mentioned the wording of Article 7 of the Charter is similar to ECHR Article 8.1 regarding the right to privacy (fn 28). Article 8 of the Charter concerns the right to data protection.

[71] Para. 34.

[72] Para. 44.

[73] Para. 69.

have been modified to limit collection and sharing of energy use data except for data that is necessary to deliver energy to them and to enable the energy supplier to properly manage the energy grid. Further, when exercising their right to opt out, consumers should not be charged unreasonable fees and the reasonableness of opt out fees must be examined in light of the nature of consumers' privacy rights under EU and U.S. laws. In most cases, we think that charging consumers opt out fees is inconsistent with EU citizens' fundamental rights. Finally, fees charged to individual consumers for opting out should be reasonable in light of the consumers' relative income level, such that low-income consumers are not being asked to pay fees that make it unduly burdensome to exercise their privacy and data protection rights.

Acknowledgements

This research was partially supported by a Faculty Internationalization Grant from Oregon State University's International Programs in 2013.

Nancy J. King is a Professor of Business Law at Oregon State University's College of Business in Corvallis, Oregon, U.S.A. (Nancy.King@bus.oregonstate.edu). In 2008 Nancy was a Fulbright Fellow at the Centre de Recherches Informatique et Droit (CRID), at the University of Namur in Namur, Belgium. While at the CRID she conducted comparative legal research from an EU/U.S. regulatory perspective on data protection and privacy issues related to consumers' use of mobile phones incorporating location-tracking technologies. She has published papers in the American Business Law Journal, Computer Law & Security Review, International Journal of Law & Technology, International Journal of Private Law, and the Federal Communications Law Journal, among others. In 2012 she received the College of Business's graduate teaching award and the Holmes-Cardozo award for her research from the Academy of Legal Studies in Business. She has also taught e-commerce law and other courses as a visiting professor at Aarhus University, Aarhus, Denmark.

Pernille Wegener Jessen is an associate professor at Aarhus University, Aarhus School of Business and Social Sciences, Department of Law in Aarhus, Denmark (pwj@law.au.dk). In 2008 she was a visiting researcher at Facultés Universitaires Notre-Dame de la Paix, Centre de Recherche Informatique et Droit (CRID), Namur, Belgium. Further, she was a co-research leader and member of the steering committee in relation to the research project: *Legal aspects of mobile commerce and pervasive computing: privacy, marketing, contracting and liability issues* (2006-2009). PWJ has (co-)authored several articles addressing the application of EU's privacy and data protection regulation in relation to new and emerging technologies, especially in an EU-US comparative perspective.