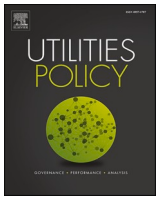
Utilities Policy 70 (2021) 101188

Contents lists available at ScienceDirect

Utilities Policy

journal homepage: http://www.elsevier.com/locate/jup



Data privacy and residential smart meters: Comparative analysis and harmonization potential

Dasom Lee [a], David J. Hess [b,*]

[a] Department of Governance and Technology for Sustainability, University of Twente Drienerlolaan 5, 7522, NB Enschede, Netherlands
[b] Department of Sociology, Vanderbilt University PMB 351811, Nashville, TN 37235-1811, USA

ARTICLE INFO

Keywords:
Privacy
Policy
Smart meters
Advanced metering infrastructure
Europe
U.S.
Canada

ABSTRACT

Building on privacy principles of the Fair Information Practice Principles and the European Union's General Data Protection Regulation, the study compares national policies and programs in Europe and North America and identifies prevailing practices for implementing privacy goals for residential energy customers: customer opt-out policies, sampling and sharing guidelines, independent data storage, and governmental enforcement authority. The analysis provides the basis for privacy standards that could apply to advanced-metering customer data across countries, even with rapidly evolving technology.

1. Introduction

In comparison with analog meters, digital smart meters offer various benefits for both utilities and customers, among them reduced costs for reading meters, more frequent meter readings with the potential for time-of-use pricing, the possibility of remote load management, the smoother integration of distributed energy into the grid, financial savings for customers, and more efficient responses to power outages (Doris and Peterson 2011; Hawk and Kaushiva 2014; Stephens et al. 2015). However, the deployment of smart meters and related digital technologies associated with the smart grid raises various societal concerns, among them privacy (Brown and Kennedy 2017; Miglani et al., 2020; Murrill et al., 2012; Sovacool et al., 2017; Zethmayer and Kolata, 2018). This study provides a comparative perspective on privacy policies for residential energy customers based on North American and European countries with high deployment levels and comparatively advanced privacy policies. The analysis identifies implementation strategies for privacy principles that could be the basis for harmonization of policy across world regions and countries.

2. Background

2.1. Definitions

There are many definitions of privacy, and the United Nations provides a useful international approach: "the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from state intervention and excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used" (UN General Assembly 2013:15). In other words, privacy refers to the extent of control that an individual (and by extension an organization) has over others' ability to gain and utilize personal or collective information without specific consent. Although the definition of privacy is much broader than personal data protection, the narrower concern has become the focus of attention in the area of smart-meter policy and privacy.

The terms "smart meter" or "advanced meter" refer to the interface, between the electricity grid and a building or building unit, that is capable of recording electricity consumption with remote data collection via wireless or wired communications. Some smart meters can also communicate with appliances inside the building to enable load management. In turn, the smart meter is one aspect of the broader digitalization of electricity, which is referred to more generally as the "smart grid" and "advanced metering infrastructure" (AMI).

In some cases, smart meters are capable of gathering very granular information over short intervals. Because the information can present a relatively detailed picture of what appliances are being used and other household activities, concerns have emerged over the use of such

* Corresponding author.
E-mail addresses: Dasomlee1@gmail.com (D. Lee), david.j.hess@vanderbilt.edu (D.J. Hess).

https://doi.org/10.1016/j.jup.2021.101188
Received 11 April 2020; Received in revised form 6 February 2021; Accepted 7 February 2021
Available online 15 March 2021

information (Kaatz, 2017). For example, Beckel et al. (2014) found that fine-grained electricity consumption data can lead to identifying specific characteristics that may reveal information about a home's socio-economic status, dwelling, and appliances, with an accuracy of more than 70% for all households. Moreover, privacy concerns are linked to security risks because criminals may be able to access the data and use the information to enable inferences about what people are doing in their home or if they are away from home (McDaniel and McLaughlin, 2009). Nevertheless, as Buchmann (2017) has argued, information and data management have become central for the development of AMI, and institutional changes will be needed.

2.2. Approaches to privacy policy

Privacy policies are guided by an underlying set of privacy principles that were first articulated during the 1960s and 1970s. The Fair Information Practice Principles (FIPPs) originated when computers began to increase their capability for information processing, and the public became concerned with the risks to privacy that these new technologies presented. These principles helped to guide privacy legislation that developed during the subsequent decades. At present, one of the most significant privacy regulations is the European Union's (E.U.'s) General Data Protection Regulation (GDPR), which outlined several fundamental digital privacy rights similar to the FIPPs (European Commission 2016). (See Table 1, which shows a version of the FIPPs used by the U.S. government.) Another approach, privacy by design, connects system design with general privacy goals, and a version of this approach was developed by the Privacy Commissioner of the Canadian province of Ontario (Cavoukian 2009).

Although the FIPPs and GPDR share common principles, they have a different policy role. The FIPPs are an underlying framework that governments, especially in North America, have used as the basis for privacy guidelines and policies (Dahn 2014; Homeland Security 2020; Privacy First 2020). However, as researchers have noted, in the U.S., the translation of FIPPs into digital privacy law is limited at the federal-government level. For example, Mármol et al. (2012) stated that existing laws in the U.S. were not equipped to meet the challenges posed by high-frequency data transaction. Unlike the FIPPs, the GDPR is an enforceable regulation that harmonizes privacy laws for the E.U. member states. Although the GDPR is widely recognized as a global milestone for privacy policy, the extent to which the GDPR successfully achieves the balance between individual privacy rights and collective benefit has been questioned (Politou et al., 2018). Furthermore, the GDPR is a general privacy policy, and it is not yet clear how the GDPR should be implemented for AMI.

Table 1
Fairness in information practices principles and the GDPR.

Fairness in Information Practices Principles (FIPPs)	EU General Data Privacy Protection Act (GDPR) (Selected Sources)
Transparency: Organizations should provide notice to individuals about their policies and practices	Transparency (Ch. 3, Art. 12)
Individual participation and consent	Consent (Ch. 2, Art. 6, 7)
Purpose specification by organizations prior to gathering data	Purpose minimization (Ch. 2, Art. 5)
Data minimization: collect the minimal amount of data necessary	Data minimization (Ch. 2, Art. 5)
Use limitation: data used only for the purposes	Right to restrict the use of data (Ch. 2, Art. 5,6)
Data quality and integrity: accuracy with provisions to contest inaccurate data	Right to access data and to rectification and erasure (Ch. 3, Art. 15, 16)
Data security	Various security provisions (Ch. 4, Art. 32)
Accountability and Auditing	Independent supervising authority (Ch. 6, Art. 51, 52)

Source: Dahn (2014); European Commission (2016).

In addition to the contrast between North America and Europe, another important distinction for privacy policy is the complicated intersection of industry structure and multilevel governance. Electricity service providers such as utilities and local power companies often have their own privacy policies, and the policies may in turn be regulated at least partially by entities other than the federal government. For example, in the U.S., much of the regulation of investor-owned utilities occurs at the state-government level with public utilities commissions, but local power companies such as electricity cooperatives and public power organizations are often exempt from the purview of the utility commissions. Thus, privacy policy is constructed in a complex institutional environment that can result in a patchwork of laws, rulings, and guidelines.

Although analog meters had security and privacy challenges (McLaughlin et al., 2009; Petrlic 2010), the problems associated with smart meters and digital electricity data are different from those of analog meters principally because of the frequency, volume, and granularity of data collection. Furthermore, although some areas of the world use wired transmission, continuous wireless transmission of personally identifiable information (PII) can also increase security vulnerabilities that can lead to privacy breaches (Rouf et al., 2012:463). Thus, as the introduction of smart meters and the associated AMI has occurred, privacy concerns have become increasingly salient. In the Netherlands, privacy concerns were a significant source of a delay in the enabling legislation for smart meters (Cuijpers and Koops 2013, see also Cuijpers 2017). In the U.K., privacy was the third-highest concern discussed in the media (Hielscher and Sovacool 2018), and privacy concerns were also salient in a study of promotional materials and focus groups (Michalec et al., 2019). In France, privacy was also an important concern in the mobilizations against smart-meter installations (Chalom, 2019); Draetta and Tavner 2019). Likewise, in North America, privacy and security concerns were among the leading reasons for organized public opposition to smart meters and demands for opt-out policies (Hess 2014). Given the general public concern with privacy, it is important to understand possible approaches to maintaining digital privacy for customer data associated with smart meters and models for privacy practice and protection.

This study builds on the existing literature in two ways. First, it extends the analysis of privacy from broad, principle-based approaches such as the FIPPs and the guidelines of the GDPR to the more concrete policy solutions for customer data associated with smart meters and AMI. Second, it develops a broad comparative framework by including both European and North American approaches. Thus, the study addresses the following two research questions: *How are smart-meter privacy issues currently regulated in Europe and North America? Based on prevailing practices, what are the pathways for harmonizing future regulations on smart meters and privacy?* In addressing these research questions, we focus on residential customers, with attention to the privacy of individuals or households rather than organizations or groups.

3. Method

3.1. Country selection

For European countries, France, the Netherlands, Norway, and the U.K were selected. For North America, we focus on the U.S. and Canada. Because these two countries have regulations at the state and provincial level, we also include California for the U.S. and Ontario for Canada.

These countries were chosen because they had relatively advanced privacy regulations and implementation of smart meters. For example, the U.S. planned for 80% of households to have a smart meter by the end of 2020 (GYT Analytics 2020), and more than 83% of Canadian customers were classified as smart meter users in 2018 (Natural Resources Canada 2018). In Europe, the U.K. had the goal of reaching most homes by 2024 (Gompertz 2019), the Netherlands had a plan of 100% installation by 2021 (O'Brien 2019; Teller Report 2019), by 2019 Norway had

almost completed installing smart meters with only 2% not having smart meters due to technical reasons (CEER 2019), and France had the goal of reaching 80% of homes by 2020 (Connexion 2019). Due to the increased level of smart meters and other information technologies, these countries have also developed advanced privacy regulations to protect personal data. Moreover, because of the dominant position of the North American and European economies globally, if harmonization were to occur across the North Atlantic region, it would likely influence other regions of the world.

Initially, we had considered the inclusion of Germany (the largest economy in Europe) as well as some East Asian countries such as China, Korea, and Japan. However, there has been limited smart meter deployment in Germany because of certification issues (Association of Energy Market Innovators 2020). In Asia, to date, there is a lack of emphasis on privacy in this policy area.

3.2. Data selection and analysis

The study uses a descriptive methodology based on the comparative social sciences. In other words, the primary goal is to describe ways that privacy concerns have been implemented in policy related to smart meters. Based on the descriptive comparison, some areas of common ground and potential for policy harmonization are identified.

The study uses the standard method for review studies known as the Preferred Reporting Items for Systematic reviews and Meta-Analysis (PRISMA) (Moher et al., 2009; Tricco et al., 2018), which involves a systematic selection of articles and papers to conduct a comparative analysis for meta-analysis. Phase 1 of the data analysis involved a systematic search for peer-reviewed and additional publications on smart meters and privacy in the selected countries (See Fig. 1.). We searched the terms "smart meter/s" and "privacy" on the Web of Science without restricting publication dates. These searches resulted in 644 articles. Another search was conducted to find articles that may not be available on the Web of Science. On Google and Google Scholar, we searched "smart meter privacy policy" and "smart meter privacy regulation" with the relevant country name attached. This search resulted in government sources (such as legislative summaries), reports, guidelines, and relevant news articles. Once these searches were completed, the duplicates were removed, and 633 articles were left in the data set.

In Phase 2 of the data analysis, the abstracts of the remaining articles were read, and irrelevant articles were removed. The main reasons for removal were that the abstract indicated that the article was engineering-based and provided solutions to privacy rather than a discussion of privacy regulations.

In Phase 3 of the data analysis, the remaining 199 articles were read in full text. After excluding 42 articles mainly because of lack of coverage of relevant privacy or policy issues, 157 articles and reports were the basis of the review. No specific time limitations were imposed to enable the understanding of how the regulations developed over a long period. This decision was sound because some regulations dated back to the 1970s. The articles were reviewed to identify key policy developments, such as the passage of privacy laws and guidance documents, and to identify prevailing practices. The final articles were then listed and classified according to their country of concern on an Excel spreadsheet.

4. Results

4.1. Comparative analysis of smart meter privacy policy

Table 2 shows the relevant regulations that directly impact either smart-meter policies or privacy policies that extend to customer data associated with smart meters and AMI. Some of the regulations were introduced during the analog meter era (i.e., the regulations approved before 2010 are most likely to be addressing privacy issues based on analog meters). However, they remain relevant for the smart meters because they provide the foundational understanding of PII and privacy. All four European countries implemented the GDPR in their privacy policies, and the GDPR continued to apply in the U.K. during the period of this study (IT Governance 2020).

In Europe, member states and relevant companies began compliance with the GDPR on May 25, 2018. The cost of noncompliance is a fine of up to €20 million or four percent of the company's global annual turnover. As indicated in Table 2, some member states had prior privacy laws, but these laws were updated or replaced with the implementation of the GDPR. In some cases, such as the Netherlands, countries had protections beyond those of the GDPR.

Canada and the U.S. are not obligated to adhere to the GDPR, and they have developed their own approaches to privacy. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) is the primary federal regulation (Office of the Privacy Commissioner of Canada, 2019). PIPEDA applies to private-sector organizations in Canada that collect, process, and use personal information in their commercial activity. It states that an individual's consent is required when data are collected, used, or disclosed and that personal information can only be used for the specified purpose. The PIPEDA rules are mandatory for provinces unless they have their own privacy law comparable to the federal ones. At the provincial level, Ontario stands out because the province has introduced additional privacy regulations that stress the importance of consent and using data only for the

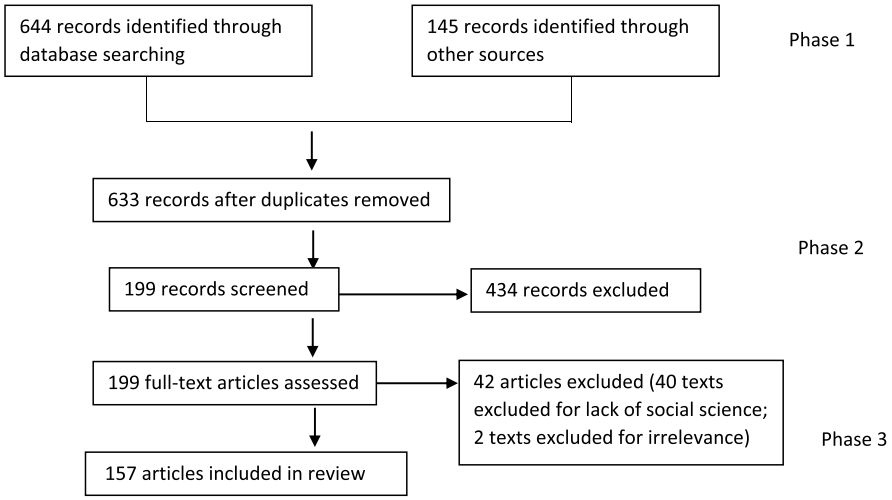


Fig. 1. Selection process for research sources.

Table 2
List of privacy and smart meter regulations in North America and Europe.

Name of Law or Policy	Brief Description	References
Europe		
France		
Act No 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (1978, 2014)	Allows data collection; states that data should be accurate, relevant, and not excessive as to purposes	CNIL (2014)
Law No 2018-493 (2018)	Modifies the above law to align the French data protection law with the GDPR, establishes the "French Data Protection Act"	Government of France (2018)
Netherlands		
Law for the Protection of Personal Information (Wet bescherming persoonsgegevens, Wbp) (2018)	Gives citizens the right to know what is happening with their data, to view their own data, and to object to using and processing data	De Minister van Justitie, (2018)
General Data Protection Regulation (GDPR, or the "Algemene Verordening Gegevensbescherming" in Dutch) (2018)	Replaces the above law with the E.U.'s GDPR	Autoriteit Persoonsgegevens (2020a)
Implementing Act General Data Protection Regulation (Uitvoeringswet Algemene verordening gegevensbescherming, UAVG) (2018)	Establishes the Personal Data Authority (de Autoriteit persoonsgegevens), an organization that manages and processes personal data; enables consumers to file a complaint on their website	De Minister van Justitie en Veiligheid (2018)
Norway		
Energy Act (Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.) (1990, 2018)	Approves the storage of information, including personal data	Olje- og energidepartementet (2018)
Personal Data Act (Lov om behandling av personpplysninger) (2000, 2018)	Implements the GDPR, allows personal data to be processed for public interest and to be archived for scientific, historical research, or statistical purposes	Justis-og beredskapsdepartementet (2018)
United Kingdom		
Smart Meter Bill (2018)	Authorizes half-hourly electricity consumption data called market-wide half-hourly settlement	UK Parliament (2018a)
The Data Protection Act (2018)	U.K.'s implementation of the GDPR	UK Parliament (2018b)
North America		
Canada (federal)		
Canadian Charter of Rights and Freedoms	Life, liberty, and security of person, freedom from unreasonable search and seizure	Government of Canada (1982)
Privacy Act (1985, 2019)	Protection of personal information	Government of Canada (2019)
Personal Information Protection and Electronic Documents Act (PIPEDA) (2000, 2019)	Protects personal information, introduces ten fair information principles	Office of the Privacy Commissioner of Canada (2019)
Ontario, Canada		
Ontario Energy Board Act (1988, 2019)	Authorization of smart meters	Government of Ontario (2019a)
Electricity Act (1998, 2019)	Allows collection of energy consumption data, allows the Smart Metering Entity (e.g., utility or a partnership corporation) to manage and aggregate data	Government of Ontario (2019b)
Freedom of Information and Protection of Privacy Act (1988, 2019)	Requires consent for data collection and limitation of scope for the purpose specified (applies to Ontario government, board, commission, corporation)	Government of Ontario (2019c)
United States (federal)		
4th Amendment of the U.S. Constitution (1789)	Security of papers, security from unreasonable search and seizure	Murrill et al. (2012); National Constitution Center (2020)
Health Insurance Portability and Accountability Act of 1996	Regulates PII in health transactions; provides regulatory and methodological guidance for energy data	US Congress (1996)
Gramm-Leach-Bliley Act (Financial Services Modernization act) (1999)	Requires corporations to send privacy notices, annual notices of information collection and sharing practices, and opt-out notice; provides regulatory and methodological guidance for energy data	US Congress (1999)
Confidential Information Protection and Statistical Efficiency Act (2002)	Data acquired by the Energy Information Administration under the pledge of confidentiality can be used exclusively for statistical purposes and must not be in identifiable form	US Congress (2002)
Energy Independence and Security Act (2007)	National Institute of Standards and Technology to a platform for smart grid information management	US Congress (2007)
Guidelines for Smart Meter Grid Cybersecurity, National Institute of Standards and Technology (2014)	Recommends privacy impact assessment and privacy practices risk assessment; proposes ways to mitigate privacy risks such as employee training, audits, and data retention	National Institute of Standards and Technology (2014a)
Framework and Roadmap for Smart Grid Interoperability	Customers should be able to access their own data, ongoing	National Institute of Standards and Technology (2014b)

(*continued on next page*)

Table 2 (*continued*)

Name of Law or Policy	Brief Description	References
Standards 3.0, National Institute of Standards and Technology (2014)	review of standards for cybersecurity, further research on cyber-physical system	
California, U.S.		
Information Practices Act of 1977	Acknowledges that privacy must be protected	California Civil Code (1977)
Government Code sections for the State of California (1999)	Notification for the user when data is being collected, purpose specification, notice to the user for the length of time of saving the data, PII cannot be sold	State of California Government Code (1999)
Provisions Applicable to Privately Owned and Publicly Owned Public Utilities. Chapter 5. (2010)	States that electrical corporations cannot share, disclose, or make available any customers' electricity or gas consumption data	California Legislative Information (2010)
Public Utilities Commission Decision (2011)	Requires consent from customers to collect smart-meter data and to release pricing, usage, and cost data	California Public Utilities Commission (2011)
Assembly Bill 1274 (2013)	Prohibits utility companies and any related businesses that handle the collected data from sharing the information to third parties without the customers' consent	Assembly Bill 1274 (California Assembly 2013)
Public Utilities Decision (2014)	Allows customers to opt out of smart meter data collection with a fee	California Public Utilities Commission, 2014a
Consumer Privacy Act, Assembly Bill 375 (2018)	Establishes four fundamental privacy rights	Assembly Bill 375 (California Assembly, 2018)

specified purpose (Office of the Privacy Commissioner of Canada, 2019; Government of Ontario 2019c).

In the U.S. during the 1990s, the federal-government developed rules for the medical and financial industries. Although these rules did not apply to energy, they provided a background that some researchers have suggested could be applied to energy data (e.g., Henderson and Harak 2015). In 2002, the Confidential Information Protection and Statistical Efficiency Act (Public Law 107–324) provided one basis for privacy guidelines for energy data. The law specified in article 3564 that energy data can be used for statistical purposes as long as PII remain undisclosed. In 2014, the federal government issued guidelines and recommendations for privacy in the context of AMI, but implementation was left to state governments (National Institute of Standards and Technology 2014a; 2014b).

A patchwork of state privacy regulations applies to energy-related data, including rules that predate AMI. (For a review, see American Council for an Energy Efficient Economy, 2020.) California's established regulatory frameworks will be the focus here. The Information Practices Act of 1977 acknowledges that privacy must be protected, and privacy is included in the state's civil code (California Civil Code 1798–1798.78, State of California Government Code 1999). After nearly a decade of groundwork, the California state government approved the 2018 Consumer Privacy Act (California Assembly 2018). Described as a "landmark policy constituting the most stringent data protection regime in the U.S." (Ghosh 2018), the law highlights four fundamental rights that suggest an overlap with the FIPPs and GDPR principles: the right to know the type of information collected, the right to opt-out of data sales to third parties, the right to have their personal information deleted, and the right to receive equal service and pricing. A further refinement, Assembly Bill 1281 of 2020, exempted some employment information and personal information involved in business-to-business transactions (California Assembly 2020).

In summary, in both Europe and North America, privacy rules have continually developed along with changing technology, and privacy rules are likely to continue to change. There is some agreement on general principles, but specific policies and practices are not always aligned.

4.2. Approaches for the implementation of privacy principles

This section identifies four main approaches that countries have developed that show how general and abstract privacy principles are being implemented for customer data associated with smart meters and the AMI. This group is not intended to be exhaustive, but it does reflect the most salient approaches that emerged in the review of laws and policies and the background literature, and it can provide the basis for further discussions of how to connect fundamental privacy principles with real-world implementation strategies.

4.2.1. Customer opt-out policies

Both the FIPPs and GDPR recognize that consent is foundational to privacy, but the focus is on consent to gathering personal data. As smart meters have been implemented widely, public concern and in some cases opposition (described above) have articulated the goal of an "opt-out" principle. It can mean the right to retain an old analog meter or to have substantial limitations imposed on the collection of data from digital meters, such as having a smart meter that must be read monthly by a person or having a smart meter that only sends information at a time interval of a specific duration (such as one month). The right to opt out of a smart-meter installation is already in practice in the Canadian provinces of British Columbia and Quebec (BC Hydro 2020; Coalition to Stop Smart Meters in BC 2019; Scassa 2019), the Netherlands (Landis+Gyr, 2014); the UK (Ofgem 2020); and in some U.S. states, such as California (PG&E 2020b; Hess 2014). In Norway, smart-meter installations are mandatory (CEER 2019), and in France, a court order is needed to remove a smart meter (Connexion 2019). The reasons for wanting to opt out often include privacy, but frequently there is a mixture of other reasons as well, and privacy is not necessarily the leading reason (Hess 2014; Hielscher and Sovacool 2018).

Because an opt-out provision generally does not permit within-day, time-of-use data to be collected, the provision can be used as one mechanism to increase the likelihood of relatively robust protection of privacy. However, a customer's decision to opt out creates a negative marginal cost for the utility. If a high number of customers were to opt-out, the utility could lose access to significant revenues and grid-stabilization benefits from programs such as load management, time-of-use pricing, and transactive energy. The opt-out program enables customers to retain an analog meter or have a digital meter that has remote communication disabled. The utility also incurs costs for sending a service representative to the building to read the meter. The utility would also lose a potentially valuable technology to support the intermittency of renewable energy, and it would lose information that would be helpful during a power outage. Thus, a trade-off emerges between the customer's demand for privacy in the form of a right to opt-out and the general benefits of sustainability, resilience, and cost savings from the widespread use of the smart meter and AMI.

Consequently, utilities have sought approval for monthly fees to impose on customers who opt out, and conflicts have emerged over what a reasonable charge should be. In California, the Consumer Privacy Act has established the general right of customers to equal treatment.

However, the provision does not apply directly to the opt-out situation because the state government also authorized set-up fees and monthly charges for customers who opt out. In the United States, second-order conflicts have emerged over the level of the fees and what a reasonable charge should be, if any, for customers who opt out. In the U.K., the same tariff may not be available if customers decide to opt out of smart meters (Ofgem 2020).

It is not easy to achieve a balance between a customer's right to opt out (and to do so at a reasonable fee) and the utility's loss of benefits from the exercise of the customer's right. There is potential for international harmonization at the level of broad guidelines and principles; however, the balance would need to be determined by national or subnational energy jurisdictions and based on local perspectives.

4.2.2. Sampling and sharing guidelines

As the previous discussion indicates, sampling frequency is associated with privacy; however, the general issue of sampling is more associated with the privacy principle of data or purpose minimization than with consent, and thus it is discussed separately here. The broad policy issue with respect to sampling includes both the frequency and the unit of sampled information. With AMI technology, sampling can become very granular or specific, such as under every 5 min for demand-response programs at a household level. Table 3 summarizes the available information on the frequency of information collection for standard uses of smart meters in the sample countries. The data suggest that a typical interval is relatively short-term sampling of 15 min to a half hour, which compares with analog meters that may be read once per month or less. The shorter the sampling interval, the greater the potential for utilities or other organizations to have information about household consumption such as appliance use at specified times of the day. In most cases, the unit of sampled information is energy consumption measured by the smart meter, usually tied to an individual household, rather than a group of meters in a building or neighborhood.

In some cases, policy documents have discussed the aggregation of customer data. Aggregation of energy consumption data can be used for measuring regional capacity demands, and it is also used to protect privacy when customer data are shared. In the U.S., some states allow the collection and release of customer information in aggregate form if specific customers cannot be identified (California Public Utilities Commission, 2014b; US Department of Energy 2020). The European Commission also suggested only reporting aggregated data to the energy supplier (European Commission 2011; Eurostat 2016). In the U.K., the suppliers are also allowed to aggregate data for forecasting purposes (Ofgem 2019b).

Although aggregation of data can be used to protect customer privacy for utility use, there is no generally accepted standard for data sharing of aggregated data with third parties (e.g., local governments, building owners, and other electricity-service providers). All four European countries that we reviewed, as well as Canada and California, have regulations that prohibit selling or sharing energy consumption data with third parties without consent. Where exceptions occur (such as to meet energy-efficiency or resilience goals), the general principles of data aggregation and deletion of PII apply. E.U. directives do not include detailed specification of processes other than to follow GDPR guidelines such as data aggregation (European Parliament 2019).

In the U.S., California established the "15/15 Rule" as a threshold for defining acceptable privacy for data sharing. Under this rule, a utility could only share data if it aggregated for 15 or more customers and if each customer comprised less than 15% of the group's aggregated consumption (California Public Utilities Commission, 2014b). Other states, such as Colorado and Illinois, adopted a similar rule. However, for some types of data sharing, complaints emerged that the 15/15 Rule was too restrictive. For example, the New York State Public Service Commission (2018) determined that the 15/15 rule was too restrictive for aggregated building information and instead adopted a 4/50 rule (a minimum of four accounts with no account more than 50% of the energy usage).

Although longer sampling intervals and data aggregation rules are consistent with the principle of data minimization, they reduce the utility's or electricity service provider's ability to offer benefits from real-time pricing, dynamic load management, or transactive energy. These programs can require sampling at frequent intervals, such as every 5 min or less (Hammerstrom et al., 2007). Thus, a balance is needed between the privacy benefits of non-granular sampling and the need to allow both the utility, its partners, and customers to have access to beneficial programs that require granular data collection. One solution to this problem is to offer the programs that require customers to opt-in to collecting or sharing of highly granular data. This approach requires system design that only collects highly granular data for customers who have accepted the incentives offered for participation.

In summary, a policy that sanctions low-frequency sampling and aggregated customer units to protect privacy would not be feasible for some demand-management programs. It would not make sense to suggest general policy guidance or a principle that precludes real-time, customer-specific data collection. Instead, the more common practice to date is to offer the programs on an opt-in basis and to allow customers to choose to have real-time data collected by utility providers and possibly shared with third parties in exchange for financial incentives. Privacy protections would then come not with the granularity of data collected but instead with the rules for data management and sharing.

4.2.3. Independent data management

The FIPPs and GDPR provide general principles for data management, storage, and deletion, but there are specific issues that emerge with their application to data associated with AMI. The data stored fall mainly within two categories: data necessary for billing and grid management, which measures energy consumption for specific customers, and data necessary for customer energy efficiency and management.

One leading example of data management is Norway's Elhub, a company established under the amended regulation 301 (Olje- og energidepartementet, 2019). The central task of Elhub is the storage and distribution of measured values and consumer information for organizations participating in the energy market. In Elhub, all customers are identified by their national identification number, and customers can receive an overview of the personal data stored in Elhub. Personal data include name, national identification number, address, contact details, and historical electricity consumption for the past three years, but no other personal data is stored on Elhub (NVE 2015). Electricity suppliers have the right to pull the national identification number from the National Registry but can also contact the customer directly to check if the information given is correct. Elhub receives consumption data in an automated process from all customers, and the data are distributed to the relevant power suppliers daily to allow electricity customers to receive quotes on an hourly basis (Statnett 2019). Elhub stores energy consumption data for three years, but a question has emerged about the

Table 3
Time frame of the energy use data sampling interval.

Country	Data Collection Frequency
Europe	
France	30 min (Marolleau 2020)
Netherlands	Read once a month for monthly statements and once a year for annual energy bill (Rijkoverheid 2020); distribution system operator and independent service providers may have access to data at more frequent intervals with customer consent (Van Aubel and Poll 2019)
Norway	30 min (Sælør 2018)
The U.K.	Depends, as often as every 30 min (UK Parliament 2018a)
North America	
Canada	15 min (Canadian Electricity Association 2020)
The U.S.	Varies. California is hourly for residential use, 15 min for commercial use (PG&E 2020a)

appropriate period of time needed to store the data (Sælør 2018).

Another example of a robust data management policy is the U.K.'s Data Protection Impact Assessment (DPIA), a process that organizations follow to identify and mitigate privacy risks associated with personal information. Completing the DPIA has become mandatory for high-risk activities. The most recent version of the DPIA was updated in 2019 with final policy decisions reflecting stakeholders' responses (Ofgem 2019a). As of 2019, the Office of Gas and Electricity Markets (Ofgem), the government office that oversees DPIAs for smart meters, was considering two additional options for "enhanced privacy" (Ofgem 2019a: 5). First, there is anonymization, which refers to how customers have their data retrieved and processed by a centralized body rather than suppliers. Second, customers are given a new unique identifier, which obscures their true identity and cannot be tracked without a key (Ofgem 2019a).

As the Norwegian and British approaches to data storage and deletion indicate, practices are emerging beyond the general principle that data collection and storage should not be excessive. These practices include the following: data should be encrypted and stored by a reliable third party, data should be anonymized (the U.K. case), and data should be deleted or permanently taken out of access after a period deemed reasonable to meet utility load-management goals.

4.3. Government enforcement authority

Another problem for privacy is monitoring and enforcement to ensure that the principles and rules are implemented. In Europe, there were several approaches to the issue. In the Netherlands, the Dutch Data Protection Authority (de Autoriteit persoonsgegevens) receives complaints from consumers regarding privacy-related problems (Autoriteit Persoonsgegevens, 2020b). Two types of complaints can be filed online: a possible privacy violation and a complaint regarding personal data processing. When a problem is found, the Personal Data Authority sends letters to the concerned organizations and seeks a change in practices. Cases of repeated violations are transferred to the Enforcement Department. In France, the Commission Nationale de I'Informatique et des Libertés (CNIL) ensures that privacy law is applied correctly. It helps people understand their rights regarding personal data, and it also issues warnings to correct measures as guided by the GDPR. The penalty for continuous violation can be up to €20 million or, for companies, 4% of annual global turnover (CNIL 2020). The U.K. has the Information Commissioner's Office (ICO), an independent authority but sponsored by the Department for Digital, Culture, Media, and Sport.

Similarly, a complaint can be filed through the ICO, which will give advice and warnings about privacy (Information Commissioner's Office 2020; Gov.uk, 2020). Norway also has the Norwegian Data Protection Authority, which is financed by the Norwegian government and is under the Ministry of Local Government and Modernization. The Norwegian Data Protection Authority monitors organizations' compliance with privacy rules, provides advice to industry organizations, and receives individuals' complaints (Norwegian Data Protection Authority 2020).

In North America, Ontario has the Information and Privacy Commissioner of Ontario (2020a), to which consumers can make a complaint, file an appeal against a decision made by a provincial government regarding information request, and request records. The Commissioner also provides guidance for organizations regarding privacy, and if a breach is reported, the Commissioner conducts an investigation and can file a report that includes recommendations. Investigators are also required to do follow-ups (Information and Privacy Commissioner of Ontario 2020b). California does not have a separate privacy authority, but the state government's Department of Justice handles privacy complaints and regulation violations. If there are any breaches, the Justice Department conducts an investigation, and the organization that has breached the privacy regulation is required to send a breach notice to residents (State of California Department of Justice 2020). These notices are also filed and can be accessed online (State of California Department of Justice 2020).

In summary, five of the six countries' practices suggest that the starting point is to establish a separate government agency with authority to review, apply, and enforce privacy regulations for data associated with smart meters. This organization should also have power beyond giving out warnings. A good example is the Dutch Data Protection Authority, which takes repeated violations of privacy to the Enforcement Department within the authority.

4.4. Prevailing practices

In both Europe and North America, governments have developed a range of policies that address the protection of the right to privacy with respect to smart-meter or digital-electricity technology. These practices go beyond the general privacy principles of the FIPPs and GDPR to identify specific solutions for the implementation of privacy principles for data collection and use from electricity customer data and, increasingly, in the context of AMIs. Four prevailing practices can be identified from the discussion of privacy and residential smart meters:

1. Smart-meter opt out. As noted above, an opt-out policy is in place in several jurisdictions in response to public opposition to smart-meter deployment. The policy may not be necessary in all areas of the world, and utilities should consider the level of public demand for an opt-out policy. Because collecting and recording energy data provides benefits to the utility, the policy can include a "reasonable" charge associated with a customer decision to opt out. In general, the percentage of customers who select opt-out tends to be low, and the utility will likely have robust demand-management programs even if a small percentage of customers opt out of participation.

Privacy concerns are one motivation for customers to support an opt-out policy, but they are not necessarily the most important reason. Studies have indicated that the motivation for public support for an opt-out option also involves a variety of other, non-privacy-related concerns, such as health, fires, hacking, costs, non-functioning meters, and interference with other wireless systems (Hess 2014; Hess and Coley 2014; Hielscher and Sovacool 2018; Sovacool et al., 2017). To some degree, privacy concerns may reflect a lack of understanding of how privacy is managed in digital systems with PII. However, there is also public awareness of ongoing data breaches of systems with apparently high data security levels, including electricity consumption data. Where there is public opposition to any highly granular data collection that can identify daily routines and appliance use, a reasonable approach is to consider an opt-out policy similar to successful ones already in effect in various countries. Thus, policy solutions to this challenge should consider this option but also take into account cultural and institutional differences.

2. Opt-in for demand-management programs and associated data sharing. For beneficial programs that require highly granular data with high-frequency sampling (e.g., real-time pricing, dynamic load management, and transactive energy), utilities or other energy-service providers generally encourage customers to enroll but do not require them to do so. Most utilities offer demand management pricing incentives, which can be adapted to local demand to encourage voluntary participation. Specific aggregation rules for data sharing such as the California-based "15/15 Rule" are too stringent under many circumstances (Livingston et al., 2018; Ruddell et al., 2020), and researchers have examined more flexible practices. For example, an assessment process would examine the threat of privacy breaches that could occur with a specific use case for shared data, such as data sharing with owners of properties with multiple units (Henderson and Harak 2015). Another practice could build on procedures for sharing of health information in the U.S., which include assessment by an expert and removal of specified categories of PII, again depending on the use case (Ruddell et al., 2020).

3. Independent data storage and rules for data sharing. Norway has established an independent organization that stores encrypted energy-consumption data, and the U.K. conducts a privacy assessment process for utilities. These provisions can help to ensure that there is compliance

with privacy guidelines. Practices can be summarized as management by an independent third party, encryption and anonymization of data, and deletion of data or permanent restriction on access after a period deemed reasonable to meet utility load management goals (such as three years).

4. Separate monitoring and enforcement agency. A separate governmental agency or department that oversees privacy-related practices has been established in several countries. The agency or department handles privacy monitoring and complaints, and it has enforcement authority.

This set of practices provides a basis for assessing the opportunities for cross-cultural harmonization of digital privacy policy for electricity. It should be stressed that the list is not intended to be exhaustive, and other areas could also emerge. However, the broader point is to note the need for comparative policy research that can begin to identify areas of common ground that could underlie a more consistent approach to electricity privacy policy. We also note that some studies argue that a self-regulatory approach can eventually lead to equilibrium among the utilities and related security and privacy concerns (Habibzadeh et al., 2019; Liu et al., 2016). However, because approaching the equilibrium often takes time and because data collection and breaches can happen without relevant stakeholders' knowledge, we stress that government-issued guidelines and regulations are important and that adopted practices must comply with those policies. Moreover, government policies should be developed with transparent and accountable decision-making processes.

5. Conclusion

Although AMI deployment has been happening for some time, privacy regulations have not kept pace with technological change. Both the FIPPs and GDPR provide an overall framework for privacy in the digital age. However, there is a need to think through how general privacy principles can be articulated with the more specific problems posed by electricity customer data in the context of AMI. This review compared the privacy regulations of Canada, France, Netherlands, Norway, the U. K., and the U.S. Based on an examination of country-specific laws, policies, and practices, we identified four areas of potential common ground that can be characterized as strategies for implementing privacy policies and principles for AMIs. These general strategies are consistent with the privacy principles of the FIPPs and GDPR but are more specific for customer data associated with electricity data in general and the smart meter and AMI in particular. These strategies can help to ensure that the new combinations of software, consumption, and the electricity system associated with digitized electricity systems do not lose public confidence and lead to public opposition, which as noted above has occurred in some countries. They can also ensure that system designers are thinking about building technologies that can be used in multiple countries without encountering design failures due to unforeseen constraints imposed by differences across countries in privacy rules and regulations.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding and Acknowledgements

This project was partially supported by the U.S. National Science Foundation, OISE-1743772, Partnerships for International Science and Engineering (PIRE) Program: "Science of Design for Societal-Scale Cyber-Physical Systems." Any opinions, findings, conclusions, or recommendations expressed here do not necessarily reflect the views of the National Science Foundation. We also thank Magdalena Sudibjo for research assistance.

References

California Public Utilities Commission, 2014a. Decision Regarding Smart Meter Opt-Out Provisions. http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M143/K904/143904205.PDF. (Accessed 18 January 2021).

California Public Utilities Commission, 2014b. Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data while Protecting Privacy of Personal Data. https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M090/K845/90845985.PDF. (Accessed 18 January 2021).

National Institute of Standards and Technology, 2014b. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pdf. (Accessed 18 January 2021).

American Council for an Energy Efficient Economy, 2020. Data Access. https://database.aceee.org/state/data-access. (Accessed 18 January 2021).

Association of Energy Market Innovations, 2020. Smart Meter Roll-Out: the German Case. https://www.bne-online.de/en/news/article/smart-meter-roll-out-the-german-case. (Accessed 18 January 2021).

Beckel, Christian, Sadamori, L., Staake, T., Santini, S., 2014. Revealing household characteristics from smart meter data. Energy 78, 397–410.

Brown, A., Kennedy, R., 2017. Regulating intersectional activity: privacy and energy efficiency, laws and technology. Int. Rev. Law Comput. Technol. 31 (3), 340–369.

Buchmann, M., 2017. Governance of data and information management in smart distribution grids: increase efficiency by balancing coordination and competition. Util. Pol. 22, 63–72.

California Assembly, 2013. Assembly Bill No. 1274 Chapter 597, an Act to Add Title 1.81.4 (Commencing with Section 1798.98) to Part 4 of Division 3 of the Civil Code, Relating to Privacy. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1274. (Accessed 18 January 2021).

California Assembly, 2018. Assembly Bill No. 375 Chapter 55, an Act to Add Title 1.81.5 (Commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, Relating to Privacy. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. (Accessed 18 January 2021).

California Assembly, 2020. Assembly Bill 1281. https://custom.statenet.com/public/resources.cgi?id=ID:bill:CA2019000A1281&ciq=ncsl&client_md=13a5d10a9fd39f1846a7ebcb346f80f3&mode=current_text. (Accessed 18 January 2021).

California Civil code 1798-1798.78, 1977. Information Practices Act 1977. https://www.calhfa.ca.gov/privacy/ipa.pdf. (Accessed 18 January 2021).

California Legislative Information, 2010. Division 4.1. Provisions Applicable to Privately Owned and Publicly Owned Public Utilities (Chapter 5). Privacy Protections for Energy Consumption Data. accessed 18th January 2021. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PUC&division=4.1.&title=&part=&chapter=5.&article=.

California Public Utilities 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. http://docs.cpuc.ca.gov/efile/PD/134875.pdf. (Accessed 18 January 2021).

Canadian Electricity Association, 2020. Smart Technology. https://electricity.ca/learn/future-of-electricity/smart-tech. (Accessed 18 January 2021).

Cavoukian, A., 2009. Privacy by Design: the 7 Foundational Principles. Information & Privacy Commissioner, Ontario, Canada. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. (Accessed 18 January 2021).

CEER, 2019. Implementing Technology that Benefits Consumers in the Clean Energy for All Europeans Package: Selected Case Studies. https://www.ceer.eu/documents/104400/-/-/bd457593-900f-f995-eac4-ed989255b26f. (Accessed 18 January 2021).

Chalom, S., 2019. Compteur Linky: pourquoi est-il si conteste? [Interview with sociologiest A. Danieli.]. Capital, Aug. 2. https://www.capital.fr/economie-politique/compteur-linky-pourquoi-est-il-si-conteste-1326899. (Accessed 18 January 2021).

CNIL, 2014. Loi Informatique et Libertes Act No 78-17 of January 1978 on information technology, data files and civil liberties. https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf. (Accessed 18 January 2021).

CNIL, 2020. Mission (4): Contrôler et sanctionner. https://www.cnil.fr/fr/mission-4-controler-et-sanctionner. (Accessed 18 January 2021).

Coalition to Stop Smart Meters in BC, 2019. Smart Meter Opt-Out Chart. http://www.stopsmartmetersbc.com/wp-content/uploads/OPT-OUT-FEES.pdf. (Accessed 19 January 2021).

Connexion, 2019. French Court Rules against Linky for Health Reasons. https://www.connexionfrance.com/French-news/French-court-rules-against-Linky-smart-meters-for-health-reasons-in-Tours. (Accessed 18 January 2021).

Cuijpers, C., 2017. Courts, privacy and data protection in The Netherlands: European influence and trends in litigation. In: Brkan, M., Psychogiopoulou, E. (Eds.), Courts, Privacy and Data Protection in the Digital Environment. Edward Elgar Publishing Limited, Cheltenham, pp. 162–179.

Cuijpers, C., Koops, B.J., 2013. Smart metering and privacy in Europe: lessons from the Dutch case. European Data Protection: Coming of Age. Springer, Dordrecht, pp. 269–293.

Dahn, S., 2014. Fair Information Practice Principles (FIPPs). Department of Homeland Security, Privacy Office. https://www.dhs.gov/publication/fair-information-practice-principles-fipps. (Accessed 18 January 2021).

De Minister van Justitie, 2018. Wet Bescherming Persoonsgegevens. https://wetten.overheid.nl/BWBR0011468/2018-05-01#Hoofdstuk3. (Accessed 18 January 2021).

De Minister van Justitie en Veiligheid, 2018. Uitvoeringswet Algemene Verordening Gegevensbescherming. https://wetten.overheid.nl/BWBR0040940/2018-05-25. (Accessed 18 January 2021).
Doris, E., Peterson, K., 2011. Government Program Briefing: Smart Metering. https://www.nrel.gov/docs/fy11osti/52788.pdf. (Accessed 18 January 2021).
Draetta, L., Tavner, B., 2019. De la "fronde anti-Linky" à la justification écologique du smart metering: retour sur la genèse d'un projet controversé. Lien Soc. Politiques (82), 52–77.
European Commission, 2011. Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection: Recommendation to the European Commission. https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1_0_clean%20%282%29.pdf. (Accessed 18 January 2021).
European Commission, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. (Accessed 18 January 2021).
European Parliament, 2019. Directive EU 2019/944 of the European Parliament and of the Council of 5 June 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944. (Accessed 18 January 2021).
Eurostat, 2016. ESSnet Big Data. https://ec.europa.eu/eurostat/cros/content/essnet-big-data-1_en. (Accessed 18 January 2021).
Ghosh, D., 2018. What you need to know about California's new data privacy law. Harvard Bus. Rev. July 11. https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law. (Accessed 18 January 2021).
Gompertz, S., 2019. Smart Meter Roll Out Delayed for Four Years. https://www.bbc.com/news/business-49721436. (Accessed 18 January 2021).
IT Governance, 2020. GDPR and Brexit: What's the Impact. https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr. (Accessed 18 January 2021).
Government of Canada, 1982. Constitution Act. https://laws-lois.justice.gc.ca/eng/const/page-15.html. (Accessed 18 January 2021).
Government of Canada, 2019. Privacy Act. https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html. (Accessed 18 January 2021).
Government of France, 2018. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1). https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte. (Accessed 18 January 2021).
Government of Ontario, 2019a. Ontario Energy Board Act, 1998. https://www.ontario.ca/laws/statute/98o15. (Accessed 18 January 2021).
Government of Ontario, 2019b. Electricity Act, 1998. https://www.ontario.ca/laws/statute/98e15#BK132. (Accessed 18 January 2021).
Government of Ontario, 2019c. Freedom of Information and Protection of Privacy Act. https://www.ontario.ca/laws/statute/90f31#BK60. (Accessed 18 January 2021).
Gov.uk, 2020. Information Commissioner's Office. https://www.gov.uk/government/organisations/information-commissioner-s-office. (Accessed 18 January 2021).
GYT Analytics, 2020. Canadian Board Analyzes the Benefits and Approves the Rollout of Smart Electricity Meters. http://gytanalytics.com/a-canadian-utility-board-analyzing-the-benefits-and-approving-the-rollout-of-smart-electricity-meters. (Accessed 18 January 2021).
Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B., Soyata, T., 2019. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain. Cities Soc. 50, 101660.
Hammerstrom, H.D., Ambrosio, R., Brous, J., Carlon, T.A., Chassin, D.P., DeSteese, J.G., Guttromson, R.T., Horst, G.R., Järvegren, O.M., Kajfaz, R., Katipamula, S., Kiesling, L., Le, N.T., Michie, P., Oliver, T.V., Pratt, T.G., Thompson, S.E., Yao, M., 2007. Pacific Northwest GridWise Testbed Demonstration Projects Part I. Olympic Peninsula Project. US Department of Energy, Pacific Northwest National Laboratory. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-17167.pdf. (Accessed 18 January 2021).
Hawk, C., Kaushiva, A., 2014. Cybersecurity and the smarter grid. Electr. J. 27 (8), 84–95.
Henderson, P., Harak, C., 2015. How utilities can give building owners the information needed for energy efficiency while protecting customer privacy. Electr. J. 28 (9), 33–44.
Hess, D.J., 2014. Smart meters and public acceptance: comparative analysis and governance implications. Health Risk Soc. 16 (3), 243–258.
Hess, D.J., Coley, J.S., 2014. Wireless smart meters and public acceptance: the environment, limited choices, and precautionary politics. Publ. Understand. Sci. 23 (6), 688–702.
Hielscher, S., Sovacool, B.K., 2018. Contested smart and low-carbon energy futures: media discourses of smart meters in the United Kingdom. J. Clean. Prod. 195, 978–990.
Homeland Security, 2020. Privacy Office. https://www.dhs.gov/privacy-office. (Accessed 18 January 2021).
Hydro, B.C., 2020. Meter Choices. https://app.bchydro.com/accounts-billing/rates-energy-use/electricity-meters/meter-choice.html?WT.mc_id=rd_meterchoices. (Accessed 18 January 2021).
Information and Privacy Commissioner of Ontario, 2020a. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca. (Accessed 18 January 2021).
Information and Privacy Commissioner of Ontario, 2020b. Privacy Complaints. https://www.ipc.on.ca/privacy-organizations/privacy-complaints. (Accessed 18 January 2021).
Information Commissioner's Office, 2020. Who We Are. https://ico.org.uk/about-the-ico/who-we-are. (Accessed 18 January 2021).
Justis- og beredskapsdepartementet, 2018. Lov Om Behandling Av Personopplysninger (Personopplysningsloven). https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#KAPITTEL_3.
Kaatz, J., 2017. Resolving the conflict between new and old: a comparison of New York, California and other state DER proceedings. Electr. J. 30 (9), 6–13.
Landis+Gyr, 2014. Landis+Gyr Supplies First Stage of Smart Meter Rollout in the Netherlands. https://eu.landisgyr.com/blog/landisgyr-supplies-first-stage-of-smart-meter-rollout-in-the-netherlands. (Accessed 18 January 2021).
Liu, B., Zhou, W., Zhu, T., Zhou, H., Lin, X., 2016. Invisible hand: a privacy preserving mobile crowd sensing framework based on economic models. IEEE Trans. Veh. Technol. 66 (5), 4410–4423.
Livingston, O., Pulsipher, T., Anderson, D., Vlachokostas, A., Wang, N., 2018. An analysis of utility meter aggregation and tenant privacy to support energy use disclosure in commercial buildings. At. Energ. 159, 302–309.
Mármol, F.G., Sorge, C., Ugus, O., Martínez Pérez, G., 2012. Do not snoop my habits: preserving privacy in the smart grid. IEEE Commun. Mag. 50 (5), 166–172.
Marolleau, L., 2020. GDPR and Linky Meters: the French Data Protection Authority Puts EDF and Engie on Notice. https://www.soulier-avocats.com/en/gdpr-and-linky-meters-the-french-data-protection-authority-puts-edf-and-engie-on-notice. (Accessed 18 January 2021).
McDaniel, P., McLaughlin, S., 2009. Security and privacy challenges in smart grids. Institute of Elect Electronics Eng. Sc. Privacy. 7 (3), 75–77.
McLaughlin, S., Podkuiko, D., McDaniel, P., 2009. September. Energy theft in the advanced metering infrastructure. Int. Workshop. On Critical Information Infrastructures Security. Springer, Berlin, Heidelberg.
Michalec, A., Hayes, E., Longhurst, J., Tudgey, D., 2019. Enhancing the communication potential of smart metering for energy and water. Util. Pol. 56, 33–40.
Miglani, A., Kumar, N., Chamola, V., Zeadally, S., 2020. Blockchain for internet of energy management: review, solutions, and challenges. Comput. Commun. 151, 395–418.
Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Ann. Intern. Med. 151 (4), 264–269.
Murrill, Brandon J., Liu, Edward C., Richard, M., 2012. Thompson. Smart Meter Data: Privacy and Cybersecurity. http://marylandsmartmeterawareness.org/wp-content/uploads/2012/07/Congress-Research-Service-SM-privacy-and-cybersecurity.pdf. (Accessed 18 January 2021).
National Constitution Center, 2020. Search and Seizure. https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv. (Accessed 18 January 2021).
National Institute of Standards and Technology, 2014a. Guidelines for Smart Meter Cybersecurity. Volumes 1,2, and 3. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf. (Accessed 18 January 2021).
Natural Resources Canada, 2018. Smart Grid in Canada. https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/canmetenergy/pdf/Smart%20Grid%20in%20Canada%20Report%20Web%20FINAL%20EN.pdf. (Accessed 18 January 2021).
New York State Public Service Commission, 2018. Order Adopting Whole Building Energy Data Aggregation Standard. http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B4C4CE28E-54CC-4514-967D-B513678E3F37%7D.
Norwegian Data Protection Authority, 2020. About Us. https://www.datatilsynet.no/en/about-us. (Accessed 18 January 2021).
NVE, 2015. All Electricity Suppliers and Grid Operators Are Not Required to Register the National Identification Numbers of All Their Customers. http://publikasjoner.nve.no/faktaark/2015/faktaark2015_11.pdf. (Accessed 18 January 2021).
Office of the Privacy Commissioner of Canada, 2019. PIPEDA in Brief. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief. (Accessed 18 January 2021).
Ofgem, 2019a. Access to Half-Hourly Electricity Data for Settlement Purposes: Data Protection Impact Assessment. Version 2. https://www.ofgem.gov.uk/system/files/docs/2019/06/data_protection_impact_assessment_v2_june_2019.pdf. (Accessed 18 January 2021).
Ofgem, 2019b. Consultation on Access to Half-Hourly Electricity Data for Settlement Purposes: Ofgem Decision and Response to Stakeholder Feedback. https://www.ofgem.gov.uk/system/files/docs/2019/06/access_to_data_consultation_ofgem_response_0.pdf. (Accessed 18 January 2021).
Ofgem, 2020. Smart Meters; A Guide to Your Rights: Are Smart Meters Mandatory? https://www.ofgem.gov.uk/consumers/household-gas-and-electricity-guide/consumer-guide-understanding-energy-meters-ofgem/smart-meters-guide-your-rights. (Accessed 18 January 2021).
Olje- og energidepartementet, 2018. Lov Om Produksjon, Omforming, Overføring, Omsetning, Fordeling Og Bruk Av Energi m.M. https://lovdata.no/dokument/NL/lov/1990-06-29-50?q=energilov. (Accessed 18 January 2021).
Olje- og energidepartementet, 2019. Forskrift Om Produksjob, Omforming, Overforing, Omsetning, Fordeling, Og, Bruk Ac Energi m.M. https://lovdata.no/dokument/SF/forskrift/1990-12-07-959. (Accessed 18 January 2021).
O'Brien, J., 2019. Dutch Government Mandates 100% Smart Meter Roll-Out by 2020. https://essentialinstall.com/news/smart-home/internet-of-things-home-automation-news/dutch-government-mandates-100-smart-meter-roll-out-by-2020. (Accessed 18 January 2021).
Persoonsgegevens, Autoriteit, 2020a. Algemene Verordening Gegevensbescherming (AVG). https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg. (Accessed 18 January 2021).
Persoonsgegevens, Autoriteit, 2020b. Klacht melden bij de AP. https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap. (Accessed 18 January 2021).
Petrlic, R., 2010. A privacy-preserving concept for smart grids. Sicherheit in vernetzten Systemen 18, B1–B14.

PG&E, 2020a. FAQs about the SmartMeter what Are Meter-Connector Benefits? https://www.pge.com/en_US/residential/save-energy-money/analyze-your-usage/your-usage/view-and-share-your-data-with-smartmeter/smartmeter-faq.page. (Accessed 18 January 2021).

PG&E, 2020b. The Smart Meter Opt-Out Program. https://www.pge.com/en_US/residential/save-energy-money/analyze-your-usage/your-usage/view-and-share-your-data-with-smartmeter/smartmeter-updates/smart-meter-opt-out-program.page. (Accessed 18 January 2021).

Politou, E., Alepis, E., Patsakis, C., 2018. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. J. Cybersecurity 4 (1), 1–20.

Privacy First, 2020. The Fair Information Principles. https://www.privacyfirst.nl/acties-3/item/154-the-fair-information-principles-canada.html. (Accessed 18 January 2021).

Rijkoverheid, 2020. Hoe Zit Het Bij Se Dlimme Meter Met Mijn Privacy? https://www.rijksoverheid.nl/onderwerpen/energie-thuis/vraag-en-antwoord/slimme-meter-privacy. (Accessed 18 January 2021).

Rouf, I., Mustafa, H., Xu, M., Xu, W., Miller, R., Gruteser, M., 2012. October. Neighborhood watch: security and privacy analysis of automatic meter reading systems. Proceedings of the 2012 ACM Conference on Computer and Communications Security 462-473.

Ruddell, B., Cheng, D., Fournier, E., Pincetl, S., Potter, C., Rushforth, R., 2020. Guidance on the usability-privacy trade-off for customer utility data aggregation. Util. Pol. 67, 101106.

Sælør, I., 2018. Personvernrettslige Problemstillinger Ved Smarte Strømmålere Og Elhub-Er Det Norske Regelverket Som Setter Krav Til Smarte Strømmålere Og Elhub I Samsvar Med Norsk Lov, EMK Art. 8 Og GDPR? https://www.duo.uio.no/bitstream/handle/10852/62590/692.pdf?sequence=5&isAllowed=y. (Accessed 18 January 2021).

Scassa, T., Vilain, M., 2019. Governing Smart Meter Data in the Public Interest: Lessons from Ontario's Smart Metering Entity. https://www.cigionline.org/sites/default/files/documents/Paper%20no.221_1.pdf. (Accessed 18 January 2021).

Sovacool, B.K., Kivimaa, P., Hielscher, S., Jenkins, K., 2017. Vulnerability and resistance in the United Kingdom's smart meter transition. Energy Pol. 109, 767–781.

State of California Department of Justice, 2020. Search Data Security Breaches. https://oag.ca.gov/privacy/databreach/list. (Accessed 18 January 2021).

State of California Government Code, 1999. Government Code Title 2. Government of the State of California. http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=11015.5. (Accessed 18 January 2021).

Statnett, 2019. The Energy Industry's Common Data Hub, Elhub, Now in Operation. https://electricenergyonline.com/article/energy/category/automation-it/53/750689/the-energy-industry-s-common-data-hub-elhub-now-in-operation.html. (Accessed 18 January 2021).

Stephens, J.C., Wilson, E.J., Peterson, T.R., 2015. Smart Grid (R)evolution: Electric Power Struggles. Cambridge University Press, New York.

Teller Report, 2019. Half of Dutch Households Own Smart Energy Meter. https://www.tellerreport.com/tech/2019-08-20—%22half-of-dutch-households-own-smart-energy-meter%22-.S1O0hZYES.html. (Accessed 19 January 2021).

Tricco, A.C., Lillie, E., Zarin, W., O'Brien, K.K., Colquhoun, H., Levac, D., Moher, D., Peters, M.D., Horsley, T., Weeks, L., Hempel, S., 2018. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. Ann. Intern. Med. 169 (7), 467–473.

UK Parliament, 2018a. Smart Meters Act 2018. https://www.legislation.gov.uk/ukpga/2018/14/data.pdf. (Accessed 18 January 2021).

UK Parliament, 2018b. Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/data.pdf. (Accessed 18 January 2021).

UN General Assembly, 2013. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf. (Accessed 1 March 2020).

US Congress, 1996. Public Law 104-191. Health Insurance Portability and Accountaibilty Act of 1996. https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf. (Accessed 18 January 2021).

US Congress, 1999. Public Law 106-102. Gramm-Leach-Bliley Act of 1999. https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm. (Accessed 18 January 2021).

US Congress, 2002. Public Law 107-347. Confidential Information Protection and Statistical Efficiency Act of 2002. https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf. (Accessed 18 January 2021).

US Congress, 2007. Public Law 110-140. Energy Independence and Security Act of 2007. https://www.govinfo.gov/content/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf. (Accessed 18 January 2021).

US Department of Energy, 2020. Comments of Avista Corporation. https://www.energy.gov/sites/prod/files/gcprod/documents/Avista_Comments_DataAccess.pdf. (Accessed 18 January 2021).

Van Aubel, P., Poll, E., 2019. Smart metering in The Netherlands: what, how, and why. Int. J. Electr. Power Energy Syst. 109, 719–725.

Zethmayr, J., Kolata, D., 2018. The costs and benefits of real-time pricing: an empirical investigation into consumer bills using hourly energy data and prices. Electr. J. 31 (2), 50–57.

David J. Hess is the James Thornton Fant Chair in Sustainability Studies and Professor of Sociology at Vanderbilt University, where he is also the Associate Director of the Vanderbilt Institute for Energy and Environment and the Director of the Program in Environmental and Sustainability Studies (www.davidjhess.net).

Dasom Lee is an assistant professor in the Department of Governance and Technology for Sustainability at the University of Twente, Netherlands. She received her Ph.D. from Vanderbilt University in sociology and has a master's degree in economics from Kyoto University (www.dasomlee.com).