It's About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering

TIMO JAKOBI, Information Systems and New Media, University of Siegen, Germany
SAMEER PATIL, School of Informatics, Computing, and Engineering, Indiana University Bloomington, USA
DAVE RANDALL, GUNNAR STEVENS, and VOLKER WULF, Information Systems and New Media, University of Siegen, Germany

Smart Meters are a key component of increasing the power efficiency of the Smart Grid. To help manage the grid effectively, these meters are designed to collect information on power consumption and send it to third parties. With Smart Metering, for the first time, these cloud-connected sensing devices are legally mandated to be installed in the homes of millions of people worldwide. Via a multi-staged empirical study that utilized an open-ended questionnaire, focus groups, and a design probe, we examined how people characterize the tension between the utility of Smart Metering and its impact on privacy. Our findings show that people seek to make abstract Smart Metering data *accountable* by connecting it to their everyday practices. Our insight can inform the design of usable privacy configuration tools that help Smart Metering consumers relate abstract data with the real-world implications of its disclosure.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; *Privacy protections*; • **Human-centered computing → Empirical studies in HCI**;

Additional Key Words and Phrases: Smart Metering, Smart Meters, usable privacy, design probe, privacy preferences, privacy settings

ACM Reference Format:
Timo Jakobi, Sameer Patil, Dave Randall, Gunnar Stevens, and Volker Wulf. 2018. It's About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Trans. Comput.-Hum. Interact.* 9, 4, Article 1 (October 2018), 43 pages. https://doi.org/0000001.0000001

1 INTRODUCTION

The rise of Ubiquitous Computing has dramatically improved the potential for sensing, processing, and triangulating personal data. Improvements in cost-performance ratios and form factors have paved the way for sensors to pervade everyday life. Simultaneously, a decline in power storage costs and a rise in cloud-based data-driven electronic services coupled with the 'sensorization' of the world, there is great potential for economic efficiencies on the part of service providers as well as consumers, e.g., through personalized services as envisioned by Weiser [141]. Tapping into these potential benefits through ubiquitous sensors in domestic environments will, however, make

Authors' addresses: Timo Jakobi, Information Systems and New Media, University of Siegen, Kohlbettstraße 15, 57068, Siegen, NRW, Germany, timo.jakobi@uni-siegen.de; Sameer Patil, School of Informatics, Computing, and Engineering, Indiana University Bloomington, 901 E 10th Street, Bloomington, IN, 47408, USA, patil@indiana.edu; Dave Randall; Gunnar Stevens; Volker Wulf, Information Systems and New Media, University of Siegen, Kohlbettstraße 15, 57068, Siegen, NRW, Germany, {dave.randall, gunnar.stevens, volker.wulf}@uni-siegen.de.

1073-0516/2018/10-ART1 $15.00
https://doi.org/0000001.0000001

it difficult to provide individuals with the awareness and control to manage data collection. In this regard, research has been dealing with the challenge of providing means for *accountability* in embedded technologies (often subsumed under the label 'Internet of Things' (IoT)). In addition, research on the privacy paradox [104] demonstrates a gap between privacy related intentions and actual behavior. The existence of the privacy paradox appears to stem, at least in part, from a lack of meaningful awareness mechanisms, an issue relevant to information technologies in general but heightened by the following specific features of embedded and connected applications in particular [114]:

(1) **Embeddedness:** Embedded sensors automatically collect (potentially) large amounts of personal data, in a manner largely hidden from users,
(2) **Profile Generation:** The collected data can be used to build individual user profiles with the potential for deriving sensitive information and detecting habits via techniques generally non-transparent to users, and
(3) **Default Presence:** Embedded sensors continually measure various parameters of everyday life activities by default and are increasingly hard to avoid as a citizen of modern society.

Ubiquitous sensing applications, without question, can improve the quality of a service and reduce perceived technological complexity by hiding the collection and processing of personal data [1]. At the same time, increasing amounts of data collection, coupled with sophisticated data processing algorithms, make the privacy implications of data based services harder to grasp for the average person. As a result, consumers are arguably using embedded devices and data-based services with minimal awareness of privacy implications [116, 118]. Moreover, data is becoming an economic asset which suppliers trade and consumers need to be able to control properly [50]. Therefore, designing privacy mechanisms for embedded applications has become an important research topic [8, 97, 98, 120].

So far, however, privacy associated with domestic life has largely been looked at from the perspective of security, as in securing communication channels and data storage, or with the aim of minimizing data collection, often relegating the user to a passive role [85]. Apart from the exceptions we discuss below, privacy issues have rarely been seen as relating to existing and future *practices* and the regulatory framework that surrounds them. How individuals and families relate to collected data and its processing remains an open question. Similarly, how people go about making sense (regarding privacy or otherwise) of available data and how systems provide this information to guarantee accountability as required by many design guidelines (e.g., Fair Information Processing Practices [138], European General Data Protection Regulation [41], etc.) is relatively under-researched. While it is widely acknowledged that transparency is a key characteristic of usable privacy management, how users make data collection and processing accountable and how information provided for privacy decision making could relate to existing everyday practices to facilitate transparency is not yet well understood.

The increasing deployment of embedded technologies throughout many Western societies is facilitated by popular consumer products, such as Smart Home devices and service-provider-installed devices (often with a statutory mandate) like Smart Meters. As a result, the need to explore the provision of transparency and accountability in these technologies has gained in relevance and urgency. Smart Meters deployment in many industrialized nations is on the rise. For citizens in many countries throughout the European Union (EU) and several states in the US, Smart Meters are, or will soon be, mandatory [147]. These developments question the fundamental idea of "doing privacy" as a voluntary, individual decision about (non-)disclosure [5]. Moreover, in Western societies, the home represents the private sphere par excellence, marking a clear border between the private and the public. Smart Meters, however, penetrate the sanctity of the domestic environment [87] by collecting data about what is going on in the home and transferring that data to third parties. Typically situated in remote corners within a residence, such as the basement, Smart Meters are physically detached from the routines of life yet track the household's power consumption behavior silently and continuously. Adding to the challenge, residents often have problems understanding power consumption data and tend to use imprecise or inaccurate folk methods for quantification [78].

So far, privacy in the domain of Smart Metering has been studied mainly from a technical and legal viewpoint: e.g., ensuring anonymization and privacy-preserving handling of data, complying with legal requirements, and providing operational security. Given that Smart Meter infrastructures are currently not commonplace, empirical studies are difficult to conduct. As a result, there is a lack of user-centered research in this domain. However, effective privacy management calls for supporting users in making privacy settings in advance of, or during, the installation of Smart Meters. Such support, while particularly important for novices and non-experts, can also serve those who are knowledgeable. Moreover, as important technical and legal decisions are still being made regarding this nascent technology, a window of opportunity exists take a consumer-oriented stance by applying user-centered research to influence technology development during deployment and expansion.

In particular, research is needed on how usable privacy design could be applied in Smart Metering to avoid fragmented, burdensome, and uninformed decision making. The challenge is to enable effective privacy management while leveraging personal and economic potential. To this end, we formulated a research agenda with three interrelated goals:

(1) exploring and analyzing how people make sense of Smart Metering data,
(2) elaborating and enriching our understanding of how individuals perceive the possible benefits and risks of Smart Metering, and
(3) utilizing a design probe to evaluate the importance of various criteria for supporting privacy decision-making in Smart Metering.

By describing how people make sense of privacy in the Smart Metering domain, we provide guidance for tools to support Smart Metering privacy management and contribute to the ongoing discussion on the future of privacy in a networked world [28, 108]. We do so by stressing the importance of a *practice based* approach [117, 145] in contrast to the typical approaches in the literature. Finally, we provide a set of methods for uncovering the *doing* of privacy-related practices to make them accessible as a resource for designing user-centered privacy for products and policies alike.

In the following section, we present an overview of relevant privacy research and describe the construct of privacy we used. Further, we outline related research on privacy in the domain of Smart Metering. Next, we describe the details of our three-step study followed by a presentation of the understanding of the perception of privacy regarding Smart Metering that emerged from our analyses. We apply the insight to demonstrate that privacy management mechanisms can benefit from highlighting the implications of data disclosure in terms of consequences for everyday practices. By these means, we aim to enable non-experts to engage in basic privacy impact assessment when handling abstract data such as that collected by Smart Meters. We discuss our study as a blueprint for sensitizing designers and policy makers to the privacy demands of consumers of emerging technologies. We end by pointing out a few limitations and presenting opportunities for future work.

2 RELATED WORK

We first provide some background information on the rollout of Smart Meters and the corresponding discussion on privacy. We then outline the various views on privacy that show the evolving nature of the concept. Focusing on information technology in general, and Smart Metering in particular, we outline modern approaches to privacy protection from the regulatory, technical, and individual perspectives and argue that providing effective privacy protection involves simultaneous consideration of all of these perspectives. We then take a closer look at privacy support from the individual perspective and motivate our work on privacy decision-making in the Smart Metering domain.

2.1 Operational Details of Smart Metering

A Smart Meter records a household's electricity consumption and sends that information to authorized parties, such as the utility provider, in intervals as short as 15 minutes. Across various countries, there are subtle differences in the technical and legal requirements for the implementation of Smart Metering. In California, for instance, Smart Meters send hourly consumption information exclusively to the utility provider. The only choice a consumer is offered is to opt-out by paying an annual fee [107]. In Europe, Smart Meters are considered a central element of sustainable strategies to manage (renewable) energy more efficiently by using real-time information on load, supply, and demand [147]. For example, in Germany, Smart Meters will soon be mandatory for new buildings and households with annual consumptions over 6,000 kWh.

Typically, consumers are free to choose and install domestic devices according to individual preferences and needs (among which privacy might be one of the considerations). In contrast, Smart Meters are often part of a mandatory infrastructure deployment prescribed by the State or the service provider. Moreover, Smart Meters are a potential gateway for other parties to peek into domestic living practices. For instance, unlike California, the German system architecture allows not just utility providers but also other parties access to the power consumption data. Therefore, Smart Meters arguably have a greater privacy impact in comparison to other embedded domestic devices. As a result, Smart Metering in Germany is strictly regulated by the protection profile of the Federal Office for Information Security (BSI) based on the Common Criteria [106].

Although Smart Metering data is considered private, the guidelines for Smart Meter deployment rarely discuss usable means for end user control [132]. Addressing citizens' privacy concerns regarding Smart Meters is arguably a major prerequisite for societal acceptance of the technology. This is aptly demonstrated by the failed rollout of Smart Meters in the Netherlands, where privacy concerns led state senators to reject measures to make Smart Meters mandatory. Consequently, in a second draft, the Dutch deployment provided means for opting-out as well as transparency [30]. Consumer reservations arise because Smart Meters touch several fundamental privacy rights, especially when parties other than the utility provider have access to power consumption data. These rights include the right to informational self-determination, the right to ensure the confidentiality and integrity of information technology systems, and the right to the inviolability of the home [80, 110].

Overall, various interest groups have outlined a number of benefits as well as risks [59, 96] in Smart Metering. Both must be taken into account when understanding privacy expectations of consumers and, subsequently, providing effective privacy management solutions. Enabling consumers to make informed choices to obtain desired benefits while avoiding unintended privacy risks is clearly important.

2.1.1 *Benefits of Smart Metering.*

Various stakeholders are expected to benefit from a nationwide rollout of Smart Meters: consumers, utility providers, network system operators, meter operators, providers of innovative power services, and society as a whole [102, 121]. In particular, Smart Meters are considered a prerequisite for building a renewable electricity infrastructure [6]. Moreover, it is assumed that the rollout will allow more efficient planning and management of power distribution based on real-time information regarding power load, supply, and demand. In addition, it is postulated that Smart Meters would enable efficient billing procedures, dynamic pricing, improved load analysis, remote management, and decreased likelihood of theft or fraud [24]. Consumers as well as companies may reap the benefits via lower prices and a more resilient electrical grid [52].

The greatest direct benefit to consumers, however, may lie in real-time, fine-grained power consumption feedback, allowing savings of money, power, and emissions. Research in Human Computer Interaction (HCI) shows that power consumption feedback helps households better understand their consumption behavior [128] and discover potential savings [48]. The power consumption profiles generated from Smart Metering data are being applied to develop tariff recommender systems as an additional potential benefit [44]. Further, Smart Metering data could be a source for enhancing the content and delivery of power consumption advice [43].

2.1.2 Risks of Smart Metering. Despite their benefits, Smart Meters introduce new risks and attack vectors. In this regard, data protection supervisors, researchers, and activists have outlined a number of risks that stem from a lack of data protection [59, 83, 96]. In particular, the Smart Grid constitutes a critical infrastructure that must be protected against cyberattacks by hackers, criminals, terrorists, or foreign states [42, 45]. As a result of digitization, cyberattacks are more common and damaging [95]. For the individual, the data collected by a Smart Meter poses the risk of others deducing life choices and domestic routines [17, 66]. Technology acceptance is also an important factor as consumers may not trust utility providers [63, 119].

Empirical studies on consumer perceptions of Smart Metering reveal that, in principle, consumers place a high value on maintaining control over the disclosure of personal power consumption data [82, 146]. At the same time, studies show that consumers lack proper understanding of who can access their data [77, 119]. Krishnamurti et al. [83] further showed that benefits and risks mentioned by consumers do not always match from what is currently feasible. Regardless, when people perceive risks as real, they treat their consequences as real and behave accordingly [135]. However, Krishnamurti et al. [83] mention that weighing the impacts of contradictory factors is a complex process. They found a desire for Smart Meters, despite perceived risks, because of expected benefits, such as improved home control, better accounting of power consumption, and potential cost savings. Even though the extent to which these benefits could be realized is unclear, they still seem to be powerful drivers of consumer behavior.

2.2 Conceptual Understanding of Privacy

In modern societies, privacy is a fundamental right codified in many national laws as well as the United Nations Universal Declaration of Human Rights [100]. However, the notion of privacy has changed over time, driven largely by the effects of new technology. As a result, there is no universal definition of privacy [131]. For instance, when photography entered the mainstream, privacy was proclaimed as the “right to be left alone” [139]; with advances in surveillance devices, privacy was described as the claim for self-determination of the communication of information about oneself [142]; with the advent of information technology, privacy was characterized based on control over the flows of personal data [46, 99]; with the growth of the Internet and online interactions, privacy was framed in terms of ‘contextual integrity’ [103]. Regardless, how users view privacy is still not fully understood. Moreover, recent technological advances, such as ubiquitous sensor networks, big data analytics, and data markets for everyday applications, raise new challenges that necessitate refining or redefining existing concepts [8, 97, 98, 120, 140].

Traditionally, understandings of privacy can be thought of as entailing a normativity or being bound up in issues like trust (see [65] for an overview). These perspectives are often shaped by the idea of two distinct social spheres: the private and the public. Whereas some theorists presume static boundaries between the two spheres, others, such as Altman [7], describe privacy as a dynamic process involving boundary regulation. In Altman's view, people engage in sophisticated practices to set the right level of privacy by continuous management of data disclosure and flow to other parties. Palen and Dourish [108] applied this view to promote privacy-sensitive design in networked systems. Their framework covers three dimensions: the disclosure boundary, the identity boundary, and the temporal boundary. Each boundary needs dynamic privacy management with corresponding disclosure decisions depending on the particular social situation at hand. This characterization was further developed by Crabtree et al. [28] for considering privacy in the age of ubiquitous computing. Research on trust and privacy has further covered domains such as social networking (see e.g., [35, 47]), data mining (see e.g., [88]), and mobile services (see e.g., [67]).

A second well-known view on privacy decision-making is the one described by economic thinkers, highlighting the benefits and costs of protecting or disclosing personal information [14]. From an economics viewpoint, privacy related choices can be characterized as a function of decisions made by a rational actor [4, 32]. Such a rational-actor perspective sees privacy related decisions as calculated tradeoffs regarding the benefits and risks of data disclosure. Overall, this line of research is primarily interested in studying the influence of the tradeoffs between benefits and costs (both real and perceived) on privacy related decisions of individuals as economic agents [14]. This individual balancing is also referred to as the mental privacy calculus [32] and takes into account several factors: (i) the types of data in question, (ii) the actual and potential data collectors and processors, (iii) potential (secondary) uses of the data, and (iv) the data control options [4, 14]. From this perspective, the mismatch between stated privacy attitudes and actual behavior presents a paradox [104] as people seem to make irrational decisions. The concept of 'bounded rationality' [55, 130] provides a partial explanation for the paradox, explaining it as a result of the opaqueness of privacy implications [9], context-dependency of decisions [64], and a lack of sufficient awareness and knowledge regarding matters relevant to privacy decision-making [112]. Privacy research must therefore take into account that individual decisions are dependent on a person's knowledge of technology and trust in the various parties involved. Moreover, a lack of awareness of data availability and use can affect decision-making ability [84]. Therefore, *perceived* pros and cons are as important as the actual consequences of a decision [135].

As Reckwitz [117] points out, human behavior must be understood against the background of historically contingent social practices. As such, behavior related to privacy is embedded in collective cognitive and symbolic structures that enable a socially shared way of ascribing meaning to the world [131] . Therefore, to understand and support privacy decision-making, we need to consider how these decisions are embedded in people's contextual understanding and expectations regarding the role and the behavior of the parties involved and the potential future uses of the disclosed information.

2.3 Approaches for Protecting Privacy

Privacy protection can be approached from three different perspectives, viz., regulatory, technical, and individual, and there is extensive literature covering each.

From the **regulatory perspective**, privacy laws such as the US Privacy Act of 1974 that introduced Fair Information Processing Practices (FIPPS) [105], the EU Directive 95/46/EC [39], and European General Data Protection Regulation (GDPR) [41] regulate the handling of personal information. Additional regulation and standards, such as the Common Criteria [106], play an important role in defining security requirements for systems that store and process private data.

For instance, the BSI protection profile outlines fundamental requirements for secure and safe collection, transmission, storage, and processing of personal data collected by Smart Meters [132]. In addition, it defines basic consumer rights such as ex ante transparency and the ability to control data disclosure to third parties. However, precise implementation details of these requirements are intentionally left open to avoid overregulation. In particular, requirements related to usability and human factors are largely absent. The current handling of browser cookies as defined by EU Directive 2009/136/EG [40], commonly referred to as the Cookie Directive, illustrates that a lack of consideration of User eXperience (UX) when drafting regulation can prohibit effective and privacy-sensitive implementation of the technology in question; Web site visitors are currently provided a practically meaningless choice between accepting cookies or leaving the site.

From the **technical perspective**, the major goal is to embed privacy protection in the system itself. Some approaches that fall under this approach include Privacy By Design (PbD), Privacy Enhancing Technologies (PET), and Privacy Preserving Technologies (PPT) [31]. These approaches provide best practices, guidelines, and schemes such as preventing data leakage, supporting data minimization, and providing various levels of anonymity, restricted linkage, and control over information disclosure, etc. These principles have been applied in many areas, including ubiquitous computing [84] and even Smart Metering [20]. In particular, a core technical strategy is to provide privacy *by default*, thus ensuring that "the settings that apply when the user is not required to take any action are as privacy-protective as possible" [19]. Such an approach includes efforts to put users in possession and control of their data [21, 94].

From the **individual perspective**, the objective is to facilitate and support privacy-related user behavior. Attempts to achieve this goal involve a variety of approaches such as providing usable privacy features, increasing privacy awareness, and providing privacy decision support. HCI research, more specifically usable privacy research, seeks to ensure that privacy management mechanisms are available and designed to be usable and understandable by non-experts [53, 132, 143]. Apart from a few notable exceptions, there is little published research on the impact of present practices on driving behavior in systems of the future.

The regulatory, technical, and individual perspectives are not mutually exclusive but are intertwined and must thus work in concert. This means that the design of privacy management interfaces must be informed not just by user demands but also by legal compliance requirements and technical constraints. More importantly, privacy approaches targeting the individual have suffered from low adoption rates if not backed by corresponding regulatory enforcement [123, 127]. Therefore, no matter which perspective is employed, providing effecting privacy mechanisms requires integration with the other perspectives. While the legislative prescription of applying PbD principles to Smart Metering in Europe considers regulatory and technological perspectives, it has mostly ignored human factors [20, 132].

2.4 The Role of Practice in Designing for Usable Privacy

Usable privacy, at a basic level, begins with applying general usability principles when designing technological systems and interfaces related to privacy. As Langheinrich [85] pointed out, systems must "balance privacy practices and goals with the (in)convenience associated with them. If people need to go to great lengths to protect their privacy, they won't." Some specific guidelines include enabling privacy management as a part of normal system usage without inhibiting established usage practices [86], e.g., taking into account mental models of the system operation [91] and providing mechanisms for managing access to personal data [72].

Closely related to existing guidelines and legal requirements demanding ex ante transparency for obtaining users' informed consent, there is a line of research attempting to raise individual attention, perception, and cognitive capacity regarding which personal data is recorded by whom and how the recorded data is stored, processed, and used [112]. Additionally, there are several general guidelines mentioned in the literature, such as including understandable privacy notices [125] or providing feedback and control regarding data disclosures [12]. A well-known general requirement in many design guidelines, such as PbD, as well as in legislation is the call for the provision of privacy related awareness and decision support by devices and services, especially since the collection of data in ubiquitous computing environments is often not readily apparent [85]. Support for privacy-related decisions aims to simplify privacy decision-making and guide users in making informed tradeoffs based on potential positive and negative consequences [10, 79, 89, 112]. Other similar commonly used strategies for making implications visible include using heuristic threat models that aim to assess risks [71] or providing justifications for requesting personal data [81]. With data becoming more and more abstract, making data collection, processing, and usage understandable to the user remains a challenge [129, 136]. As Cranor [29] points out, "There is increasing agreement that we need to design secure systems that people can actually use, but less agreement about how to reach this goal."

From a practice-theoretical perspective [117], current practices drive how users understand and appropriate technologies, at least to some degree. As a result, practice based research on usable privacy starts with understanding how individuals and households appropriate and make sense of systems and data in relation to their everyday life practices. Grinter et al. [60, 61], for instance, uncovered practical challenges in making home networks work. Focusing on support for power consumption advice, Fischer et al. [43] found that referring to household routines and practices made data more meaningful. Tolmie et al. [136] provided power consumption feedback for households to uncover and make sense of their routines and activities and found that social interpretation of data is key to sensemaking, thus demonstrating the role of practices for 'data work' as a type of articulation work. Leaving aside the accuracy of Big Data algorithms for interpreting data, the significance, granularity, frequency, and flow of data are obviously connected to privacy management as well as economic considerations.

For Smart Metering, individual practices related to interpreting data for making privacy decisions are largely unknown. We therefore aimed at a better understanding of the practices connected to assessing Smart Metering data and making it accountable by either keeping it private or sharing it with others. Uncovering these practices makes them accessible as a dual resource: (i) for designers to provide usable privacy to individuals, and (ii) for policy makers and industry to devise regulations and technical solutions based on people's privacy demands related to ubiquitous technologies.

2.5 Privacy Protection for Smart Metering

So far, research on protecting privacy in Smart Metering has largely examined privacy protection from the regulatory or technical perspectives; the individual perspective is largely missing. The Dutch case mentioned above and the BSI protection profile in Germany are examples of policy based on the regulatory perspective.

From the technical perspective, essential privacy and security protection are addressed via technical mechanisms, such as encryption, authentication, and anonymization [57]. The two main approaches for embedding privacy in Smart Metering involve manipulating or reducing the amount of data disclosed in order to try to thwart personal identification. The first approach involves statistical strategies such as distortion [124], data anonymization [90], random noise integration [137], and obfuscation via local buffers [76]. The second approach provides anonymity via aggregation [122] implemented in one of two ways [37]:

(1) *spatial* aggregation that summarizes the readings of a larger grid segment (e.g., all households attached to one converter station), thus concealing individual households within a larger group, or
(2) *temporal* aggregation that uses longer intervals between data collection and data transmission in order to avoid revealing fine-grained and potentially sensitive information.

Efthymiou and Kalogridis [36] suggest switching the mode of data disclosure according to the specific purpose of an authorized service: low-frequency readings (for instance, one reading per week or month, which does not compromise privacy) for billing and high-frequency readings (as frequent as multiple readings per minute) for other services (for instance, providing feedback regarding power consumption practices). However, these statistical and aggregation techniques create overhead, thus potentially reducing flexibility and affecting service quality for consumers (e.g., the utility of the consumption feedback) [57]. As a potential solution, Pallas suggested the introduction of a ‘data trustee’ responsible for storing data securely and eliminating the necessity to fall back on trusting non-neutral parties to handle consumer privacy [109]. Such legal and technical measures can be complemented by the processes for local privacy management according to end user preferences. Thus, individually personalized privacy mechanisms can help consumers make informed data disclosure decisions that balance utility and privacy according to the needs of the specific context and services at hand.

To the best of our knowledge, research has rarely considered the design of interfaces for privacy management in Smart Metering. A notable exception is the work by Döbelt et al. [34], who focused on consumer concerns and trust-building rather than on the design of the user interface (UI) and UX for Smart Meter privacy managers. How to design a usable privacy manager for Smart Meters that could help households make informed data protection decisions based on perceived and potential benefits and risks remains an open question. In particular, such design ought to consider that people are often unaware of their electricity consumption and, consequently, do not realize the extent to which the collected data reveals personal domestic routines. Moreover, the privacy risks attached to Smart Meter data arise not just from a single data point but from the aggregation and secondary use of large volumes of data collected as a continuous stream. Further, Smart Metering is a new technology where novices and non-experts are the norm, not the exception. Owing to the novelty and inexperience, individuals may easily overlook or misinterpret perceived risks as well as benefits.

We addressed this gap via two research questions:

(1) How can individuals be empowered to manage privacy in Smart Metering based on their understanding and conceptualization of the benefits and risks of Smart Metering?
(2) How can the insight generated from a user-centered approach to privacy management in Smart Metering inform and complement the requirements and considerations developed from the regulatory and technical perspectives?

3 METHOD

Our methods were informed by the design case study methodology [145], a multi-staged, action-research approach [68] that combines methods from ethnographically-oriented research on user behavior and the corresponding rationales underlying the behavior [115] with those from design research in which ‘probes’ are used in a range of ways, from stimulation of creative ideas to evaluation of prototype artifacts [26, 51]. The basic purpose of a design case study is to provide a means to relate the in-depth knowledge of current practice that an ethnographic orientation provides along with a means to assess the viability and consequences of technological intervention

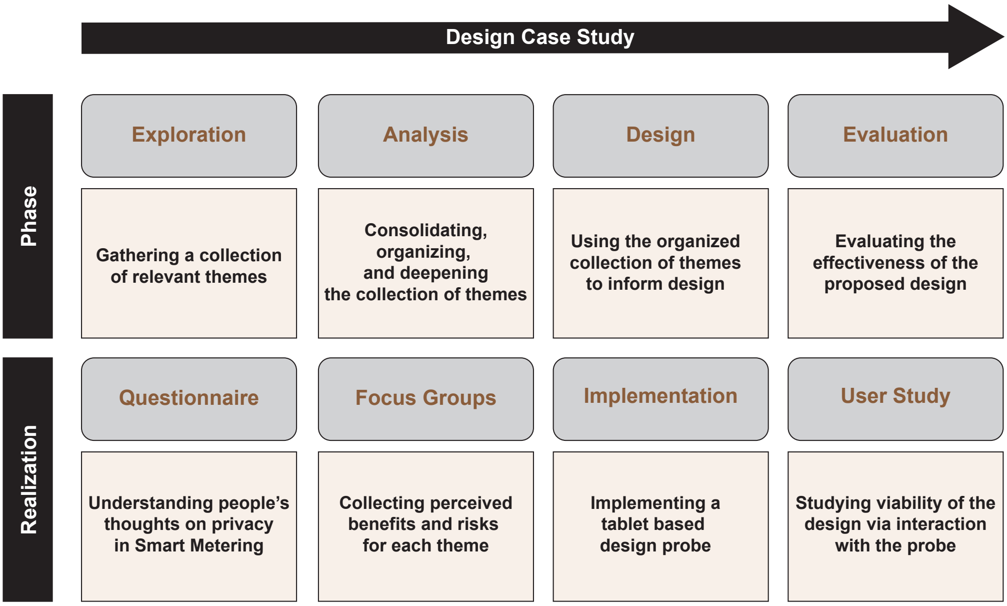

Design Case Study
Phase
Exploration
Analysis
Design
Evaluation
Gathering a collection of relevant themes
Consolidating, organizing, and deepening the collection of themes
Using the organized collection of themes to inform design
Evaluating the effectiveness of the proposed design
Realization
Questionnaire
Focus Groups
Implementation
User Study
Understanding people's thoughts on privacy in Smart Metering
Collecting perceived benefits and risks for each theme
Implementing a tablet based design probe
Studying viability of the design via interaction with the probe

Fig. 1. An overview of our multi-stage research approach.

with users. As such, design is understood as an open-ended process with a transformative potential informed by the current context.

Our perspective on methods is in line with Randall et al. [115] who suggest that qualitative methods in general, and the ethnographic approach to studying practice in particular, should be understood in relation to analytic commitments instead of being considered a distinct method. Such a view is in keeping with a broadly ‘anti-method’ line found in ethnomethodological work [93]. The point here is that an understanding of practice does not require a specific method but a commitment to the idea of members’ rationales [64], especially if we are to take seriously the individual perspective we spoke of above (see Section 2.3). In principle, rationales can be elicited in a variety of ways. In our case, practical difficulties of access for obtaining individual responses were by far the most important consideration. At the same time, we decided against soliciting questionnaire responses online since we wanted to target the views of those who had less experience with technology. We also decided against street interviews to ensure that participants would have the time to respond to open-ended questions.

Figure 1 outlines how we utilized the general principles of the design case study. In the initial exploration phase, we used an open-ended questionnaire as the first step for constructing a broad picture of how people relate to Smart Meters and Smart Metering data. While individuals may have opinions on privacy and trust regarding Smart Metering, they may well hold these opinions from a position of ignorance. Yet, privacy decision making should be supported before, during, and immediately after the installation of a Smart Meter, such that it applies from the very beginning. Moreover, research shows that experts and non-experts have different usability and information presentation needs [22, 58]. We therefore decided explicitly to target non-experts.

Guided by the insight from a thematic analysis of open-ended questionnaire responses, we proceeded to the second step of conducting four in-person focus groups aimed at a deeper unpacking of the salient aspects identified via the questionnaire. We opted for a complimentary combination of open-ended questionnaire and focus groups in part because of the sheer difficulty of collecting reliable data by purely observational means. Our third step involved a design probe [13] created to serve a dual purpose. First, the probe served as a tool to implement the design ideas that emerged from the earlier empirical findings. Second, the probe provided an artifact to study the reactions and engagement of individuals.

All steps were carried out in German, the native language of the participants. The description, screenshots, quotes, and other relevant details have been translated into English for the purposes of this paper. The next subsections describe our research setting followed by more details on each component of the study.

3.1 Study Setting

Our study was situated in Siegen, a mid-sized German city (of about 100,000 inhabitants) surrounded by several rural communities. In Germany, a 'soft' rollout of Smart Meters has recently begun. Smart Meters are mandatory for new buildings and for existing structures that choose to make renovations. In all other cases, Smart Meters can be purchased and installed on a voluntary basis. Currently, these Smart Meters do not allow communication with third parties. To establish a secure and safe communication infrastructure, Smart Meter Gateways are currently under development. A recently released governmental roadmap has defined the lower consumption limit for mandatory installation of Smart Meters at 6,000 kilowatt hours per year. As a result, in the near term, Smart Meters will remain optional for most private households. Successful realization of a comprehensive Smart Grid in Germany depends heavily on consumer interest and acceptance. Legal privacy compliance is an important consideration since Germany has strong data protection and privacy laws in comparison with other countries.

Although the rollout has begun, consumers in Germany are largely unfamiliar with Smart Metering [38]. Since Smart Meter Gateways are not being universally deployed as yet, few private households are experienced in, or knowledgeable about, the capabilities of Smart Meters to communicate with utility providers or third parties. This lack of awareness and experience is an unavoidable feature of studying future technologies [70, 75, 134]. For the Smart Metering case, this holds true for two main reasons. First, fundamental decisions related to standardization are difficult to change once infrastructure becomes part of everyday life, and it may be too late to accommodate and address emergent user concerns about the technology thereafter. Therefore, an early understanding of user beliefs and concerns is essential for informing and influencing the processes of development, regulation, and dissemination. Second, effective privacy management requires that privacy settings are specified during or before installation. As a result, providing usable privacy for Smart Metering needs to take into account the views, values, knowledge, and practices of novices who have not previously had Smart Meters installed in their homes.

3.2 Open-ended Questionnaire

For an initial exploration of people's views on Smart Metering, we pseudo-randomly distributed a paper questionnaire with open ended questions similar to an interview [126] throughout the city and neighboring regions during the summer of 2014.

The questionnaire included several questions covering attitudes related to power consumption and security, views on sharing power consumption data, hopes and fears regarding Smart Metering, and demographics (The complete questionnaire instrument is available in Section A.) In order to introduce the concepts of Smart Metering and Smart Grid, we included a short easy-to-read description. We asked 18 open-ended questions seeking detailed responses on the envisioned usage and benefits of Smart Meters, attitudes and expectations regarding the collected power consumption data, and expectations pertaining to privacy and security.

The questionnaire was distributed to 200 households with a stamped addressed return envelope. Those who filled out and returned the questionnaire were entered in a raffle for one of four €20 gift certificates for Amazon, the local mall, or a drugstore. Without any prior or follow-up contact, we received 34 completed responses, a response rate of 17 percent. Respondents were between 20 and 76 years old, with nearly three in four responsible for handling the utility services for their households (14 female, 17 male, and two who did not specify a gender).

The responses were analyzed by two of the authors and a student research assistant using thematic analysis [15] which emphasizes paying attention to how people express their expectations, concerns, and needs. Thematic coding is situated within the broad tradition of grounded theory [56] but allows focused research questions. We chose this approach largely because we shared its broad phenomenological orientation and lack of emphasis on theory building. Rather than generating theory, our primary interest was in eliciting a rich description of the phenomenon of making privacy decisions regarding Smart Meters. Using the MaxQDA coding software[1], the three coders individually coded three randomly chosen questionnaire responses. Besides looking for ways of expressing privacy expectations related to Smart Metering, no pre-defined codes were used. For our purposes, codes were defined as the ways in which respondents expressed their views on stakeholder involvement in Smart Metering and the Smart Grid. Afterward, the three researchers consolidated the codes identified during this process into a shared code set. This code set was subsequently applied to the analysis of the remaining responses and was critically and iteratively refined throughout the analyses conducted by the coders. Newly identified codes within the remaining questionnaire responses were added to the individual code sets and were discussed in a final round of consolidation.

3.3 Focus Groups

Questionnaire responses revealed that individuals operationalized the privacy risks of Smart Metering in relation to what third parties could know or infer about their everyday lives. Although respondents generally demonstrated good understanding of the technology, they repeatedly referred to the consequences of disclosing Smart Metering data in terms of what they believed others could derive from the data disclosed. This insight served as the starting point for our second step, aimed at unpacking the detail and nuance of such perceived risks and benefits. We tackled this goal by conducting four in-person focus groups during which we specifically discussed the perceived positive and negative consequences of disclosing Smart Metering data. In contrast to the sampling approach for the questionnaire, we specifically sought technologically savvy individuals for the focus groups. While such a sample could potentially reduce the variety of perceived risks and benefits elicited, we preferred participants who we believed could quickly grasp possible implications of future technology. As a result, we were able to dig deeper into the envisioned benefits and perceived privacy risks and refine the broad initial insight gained from the questionnaire responses.

We recruited focus group participants by soliciting tech-savvy students to take part in our research study. Focus group sizes varied between four and six participants per session with a total of 17 participants (3 female and 14 male). Most participants were Business or Business Informatics undergraduate students (aged between 24 and 37). Participants received no compensation. While this approach does not take into account the heterogeneity of prospective Smart Meter users, we deemed it sufficient for collecting information about possible privacy risks not identified by the questionnaire responses. Each focus group lasted about 70 minutes and followed identical procedures. First, we

[1] https://www.maxqda.com

Fig. 2. Screenshot from the introductory video on Smart Metering and the Smart Grid (https://www.youtube.com/watch?v=iyvAwd4p6ds).

showed an introductory video on Smart Metering produced by an independent foundation (see Figure 2). The video focuses on potential power savings and efficient grid management as the core benefits of Smart Metering. The video does not mention privacy implications, thus avoiding priming. As a result, the focus group discussion was relatively balanced in terms of the impact of Smart Metering on society as well as individuals. Next, participants were asked to imagine and describe how they might use Smart Metering technology in their everyday lives, first individually and, subsequently, in an open group discussion moderated by a researcher. The group then collaboratively listed potential scenarios for the use of Smart Metering data on Post-It notes distributed across the table. Finally, the participants were asked to evaluate the generated scenarios in terms of perceived benefits and risks. Each participant was provided with five positive and five negative markers to be distributed freely across the scenarios. We audio recorded and transcribed the focus group sessions and photographed the artifacts collectively generated by the participants during the sessions.

Two independent coders (an undergraduate student researcher and one of the authors) analyzed the focus group responses. Our joint analysis was composed of five steps:

(1) Coding the transcripts of the focus group sessions to augment the thematic analysis of the questionnaire responses.
(2) Classifying the participant evaluation of the generated scenarios for the use of Smart Metering data into perceived benefits and perceived risks.
(3) Categorizing the scenarios into themes based on the interpretation of the participants.
(4) Consulting technology experts and the literature to assign themes to scenarios which could not easily be associated with a theme via the codes.
(5) Identifying possible service providers and malicious actors for each theme.

The coding focused on the interrelation between the various categories of benefits and risks, akin to the kind of thematic analysis advocated by Braun and Clarke [15]. Our code set was iteratively derived. Differences in categorization were discussed to identify subjective interpretations and discrepancies were jointly resolved. The analysis resulted in a collection of possible value-added services for Smart Metering and associated privacy risks on the basis of the data collected by Smart Meters. Subsequently, we used the collection of benefits, risks, themes, and services as a resource for implementing a privacy management design probe for Smart Metering.

3.4 Design Implementation

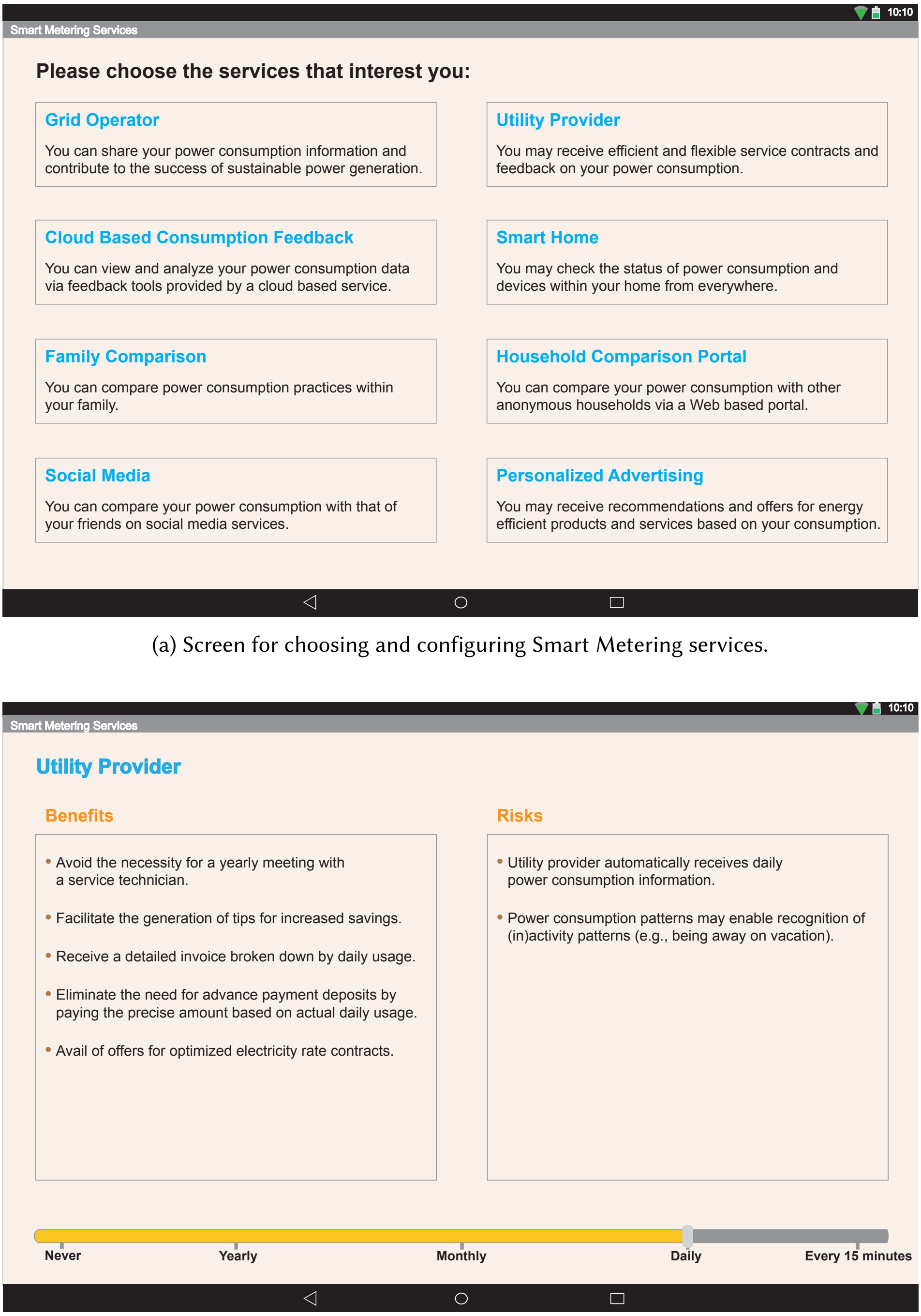
In the third step, we designed and implemented an app for Android tablets that presented a hypothetical privacy decision-making interface for Smart Metering, featuring the collected themes and scenarios along with the corresponding benefits and risks. We were interested in understanding whether making the implications of data distribution to third parties visible to end users could empower them to make informed decisions regarding the collection, distribution, and processing of Smart Metering data. Specifically, our design promoted an approach to privacy management that presents the consequences of privacy decision-making as a resource for fostering awareness. This immediate feedback loop is typically unavailable in real-life settings unless incorporated as an educational or training feature in privacy management systems. The app instantiated an interface for a privacy manager allowing the configuration of privacy settings by selecting from a menu of value-added Smart Metering services that were identified from the questionnaires and focus groups.

To design the app, we coupled our knowledge of user-centered privacy mechanisms with guidance from relevant literature. The app was designed to provide information on the benefits and risks of data disclosure [32] for possible Smart Metering services. As mentioned earlier, two techniques are commonly used to support privacy in Smart Metering: spatial aggregation and temporal aggregation. In essence, these techniques aggregate data across groups or over time to avoid revealing individual data points.

Although our design incorporated temporal aggregation principles [37, 122], representing an enhancement to the concepts proposed by Efthymiou and Kalogridis [36], we did not include spatial aggregation because the vast majority of mentioned benefits and envisioned services rely upon the provision of personalized data to some degree. It should be noted that we did not deal with the possibility of service providers or third parties triangulating the data from other sources or triangulating the usage of different individuals to learn about the data subjects. We utilized a five-point scale to show the differences in implications based on the granularity of the chosen data disclosure. Apart from an introductory video, the app was composed of two main parts (see Figure 3):

(1) A menu of Smart Metering services (taken from the themes identified from the questionnaire and focus group responses), and
(2) A list of risks and benefits for each service that varied based on the chosen temporal granularity of data disclosure.

The interface of the app required only three steps for getting to know about Smart Metering and managing privacy (see Figure 4). First, we provided a general introduction to the topic of Smart Metering and the Smart Grid. Second, the user was asked to choose desired Smart Metering services (see Figure 3a). Third, the user was shown a list of benefits and risks corresponding to the respective services. The list was compiled from the questionnaire and focus group findings (see Figure 3b). The presented privacy implications were based on the granularity of the data transfer chosen in the previous step. For each chosen service, users were presented with the implications of the data disclosure at five levels (every 15 minutes, daily, weekly, monthly, and never), each corresponding to a different granularity of data disclosure. The first option (i.e., every 15 minutes) was selected by default as it is the default interval for transferring Smart Metering data in Germany. In this third step, users could specify the desired privacy setting for the services selected earlier and refine or



Please choose the services that interest you:

Grid Operator
You can share your power consumption information and contribute to the success of sustainable power generation.

Utility Provider
You may receive efficient and flexible service contracts and feedback on your power consumption.

Cloud Based Consumption Feedback
You can view and analyze your power consumption data via feedback tools provided by a cloud based service.

Smart Home
You may check the status of power consumption and devices within your home from everywhere.

Family Comparison
You can compare power consumption practices within your family.

Household Comparison Portal
You can compare your power consumption with other anonymous households via a Web based portal.

Social Media
You can compare your power consumption with that of your friends on social media services.

Personalized Advertising
You may receive recommendations and offers for energy efficient products and services based on your consumption.

(a) Screen for choosing and configuring Smart Metering services.

Utility Provider

Benefits

- Avoid the necessity for a yearly meeting with a service technician.
- Facilitate the generation of tips for increased savings.
- Receive a detailed invoice broken down by daily usage.
- Eliminate the need for advance payment deposits by paying the precise amount based on actual daily usage.
- Avail of offers for optimized electricity rate contracts.

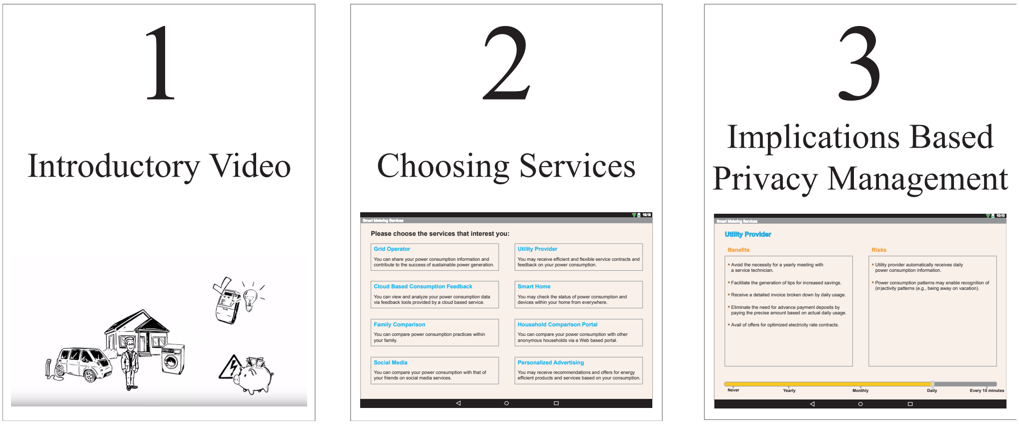
Risks

- Utility provider automatically receives daily power consumption information.
- Power consumption patterns may enable recognition of (in)activity patterns (e.g., being away on vacation).

Never — Yearly — Monthly — Daily — Every 15 minutes

(b) Screen for the case of the 'Utility Provider' service with 'Daily' data collection providing corresponding information on the privacy implications and the option to change the data disclosure interval.

Fig. 3. Screenshots of the tablet based app for Smart Metering privacy management.



Please choose the services that interest you:

Grid Operator
You can share your power consumption information and contribute to the success of sustainable power generation.

Utility Provider
You may receive efficient and flexible service contracts and feedback on your power consumption.

Cloud Based Consumption Feedback
You can view and analyze your power consumption data via feedback tools provided by a cloud based service.

Smart Home
You may check the status of power consumption and devices within your home from everywhere.

Family Comparison
You can compare power consumption practices within your family.

Household Comparison Portal
You can compare your power consumption with other anonymous households via a Web based portal.

Social Media
You can compare your power consumption with that of your friends on social media services.

Personalized Advertising
You may receive recommendations and offers for energy efficient products and services based on your consumption.

Utility Provider

Benefits
- Avoid the necessity for a yearly meeting with a service technician.
- Facilitate the generation of tips for increased savings.
- Receive a detailed invoice broken down by daily usage.
- Eliminate the need for advance payment deposits by paying the precise amount based on actual daily usage.
- Avail of offers for optimized electricity rate contracts.

Risks
- Utility provider automatically receives daily power consumption information.
- Power consumption patterns may enable recognition of (in)activity patterns (e.g., being away on vacation).

Never Yearly Monthly Daily Every 15 minutes

(a) Providing information regarding Smart Metering and the Smart Grid.

(b) Presenting value-added Smart Metering services.

(c) Adjusting data disclosure based on the corresponding privacy implications.

Fig. 4. Interaction flow of the design probe.

revoke the initial data transfer choices. Changing the granularity of data disclosure updated the benefits and risks shown.

3.5 User Evaluation

We utilized the app as a design probe to examine whether it was understandable and easy to use for managing Smart Metering privacy. Additionally, we were interested in examining whether providing real-world implications influenced privacy decision-making and whether the choices varied across services.

We carried out the evaluation by recruiting 205 participants from public places (100 female, 105 male, ranging in ages from 19 to 70 with an average age of 30 and median of 26). Two sites were used for recruiting participants: the university campus and the pedestrian zone of the town's main shopping area. As a result, participants were a roughly equal mix of university students and non-student residents of the town. Passers-by were randomly asked to participate in a research study. Upon consent, we invited participants to a quiet outdoors area. We then introduced the study in detail and handed over the tablet on which the Smart Metering video used for the focus groups (see Figure 2) was shown (see Figure 4a). Note again that the video makes no reference to privacy. Subsequently, we offered to answer questions regarding Smart Metering before letting participants proceed to the privacy management screens.

The probe presented participants with the scenario that a Smart Meter would be installed in their home and the app would allow them to choose Smart Metering services. Prior to and while navigating the app and making choices, we encouraged participants to verbalize their thoughts. Incorporating the service subscription scenario allowed us to let participants choose privacy settings as a natural extension of their actions and choices (see Figure 4b). This flow served two purposes: first, we wanted to minimize priming regarding privacy, and second, we mimicked the "real" situation of managing privacy as a secondary aspect of subscribing to a service. When participants chose services, we provided brief explanations for the services, if asked. During the phase of trading off data disclosure versus service quality (see Figure 4c), we explicitly avoided priming respondents.

On campus as well as at the pedestrian zone in the town, the study team consisted of two undergraduate students. The first guided participants through the study and conversed with them during the tasks. The second took field notes and observed participant behavior. We did not restrict the time taken by participants to make decisions. On average, study sessions lasted approximately five minutes. After participants completed the study, we conducted a brief post-study interview on their impressions of the user experience of the probe (especially the usefulness of the presented benefits and risks), their knowledge of Smart Metering in particular and technology in general, and their attitudes regarding privacy (in general as well as specific to Smart Metering). The interviews lasted between four and ten minutes and were audio-recorded and transcribed for analysis.

3.6 Ethical Considerations

Our research included the collection and analysis of personal data. Handling such data safely and securely was an important consideration throughout the research activities. The research procedures were designed by taking into account international and German national legislation. In Germany, the equivalent of an Institutional Review Board (IRB) evaluation is not necessary when conducting field research. Nonetheless, we paid extensive attention to ethical issues. For instance, we obtained informed consent for study participation, anonymous reporting of the findings, and the use of the audio recordings and photos. For safeguarding participant privacy, we anonymized the data by assigning a unique code to each participant of each research phase. We utilized self-provided names or addresses only for the purposes of contacting the winners of the raffle for the participation incentive and for further questions or clarifications, if needed. No personal data was used for any other purpose. All data was stored securely on the servers of our university.

One of our key research and design goals was to help people protect their privacy in the context of Smart Metering. Owing to our user-focused approach, ethical compliance was integral to the design of the app since it was implemented to enable people to manage privacy and maintain control over their Smart Metering data.

4 FINDINGS

The following subsections describe the findings of each phase of our study, respectively. We began with the exploratory open-ended questionnaire on electricity use and Smart Metering, where we identified the ways that people consider the data disclosure pertaining to these matters. In the subsequent focus groups, we refined our understanding to determine how people's characterizations and preferences could be applied to guide privacy decision-making in Smart Metering.

4.1 Open-ended Questionnaire: Exploring Characterizations of Benefits and Risks of Smart Metering

The initial exploratory questionnaire served two purposes. First, we aimed at gaining an understanding of practices and attitudes linked to power consumption in general and Smart Metering in particular. In this regard, we found that participants were interested and curios about Smart Metering. The technology was perceived to provide a number of possible benefits for individuals, utility providers, grid operators, society, and the environment. Second, we wanted to investigate people's understanding and characterizations of Smart Metering data disclosure. Here, participants indicated a principled desire to be in control of their Smart Metering data such that they would be able to decide, for instance, which parties could access the data under which circumstances. Thematic analysis revealed that participants often described privacy expectations and concerns in terms of everyday life practices along with judgments on whether it was acceptable for various other parties to know about the corresponding practices. In the following subsections, we describe the main themes identified in the questionnaire responses.

4.1.1 Envisioned Benefits and Success Factors. When considering the real-world implications of Smart Metering, respondents were able to foresee several benefits for themselves and third parties. The perceived individual benefits included control over specific appliances, savings achieved via flexible tariffs and reduced prices, comparisons with the power consumption of other households, facilitation of environmentally friendly habits, and personalization of advertisements and offers. With regard to third parties, institutions like grid operators, utility providers, and appliance manufacturers were believed to gain the most from the rollout of Smart Meters. A few respondents mentioned benefits to public institutions, e.g., guidance for public policy or savings for communal housing.

Respondents mentioned ease of use and potential savings as the main factors important for the deployment of Smart Meters to be successful and acceptable. Interestingly, another aspect important for a successful rollout was communication of best practices and possible advantages.

> "A lot of education with the people, savings for the customer, environmental aspects / CO_2 savings." — P6 (M, 37)

> "First, the benefits to the consumer must be clarified. Just creating yet another gadget for a smartphone will not be enough [to make Smart Metering attractive]." — P8 (M, 45)

Adaptability to daily use and to the demands on the infrastructure was a factor as well. For example, respondents desired that Smart Meters be easily integrated into households and existing meter boxes. In terms of usability, the success of Smart Meters was seen to depend on their integration with everyday life.

> "An important feature is ease of use, which allows one to have an overview of power consumption quickly and easily. In addition, failure and disruption rates should be as low as possible. Usability should be managed such that one feels safe with the Smart Meter after a short time." — P23 (F, 20)

Respondents wanted usable interfaces. For example, they wished to control Smart Meters and check consumption via personal computers or smartphones. Elderly respondents additionally stressed that Smart Meters should be designed in an accessible manner.

Most respondents were willing to accept the installation of Smart Meters. However, in a few exceptional cases, respondents reported complete opposition to the introduction of Smart Meters even at the cost of having to file a lawsuit.

> "I would choose a utility provider who does not use such nonsense, and, if necessary, join lawsuits against such an ordinance [of introducing Smart Metering]." — P8 (M, 45)

4.1.2 Safety and Security. Respondents demanded safety in terms of protection from physical harm, including the safety of nuclear power plants and the correct installation, isolation, and use of electric wires. Uninterrupted availability of electricity was deemed crucial for everyday life, both individually and socially, and taken for granted.

> "Ever since my childhood, I have experienced constant availability of electricity, such that I never had to consider this topic." — P2 (M, 27)

Another theme was a demand for technological security, such as data transport security, protection against hacking, fraud, and data theft. The worries respondents expressed about the data getting lost or falling into the wrong hands underscore the need for safeguarding the data.

> "A reservation for me is the high threat of misuse of data, such that the data will fall in the wrong hands." — P23 (F, 20)

4.1.3 Privacy Expectations and Behaviors. Overall, we found high sensitivity to privacy aspects in Smart Metering. At the same time, keeping data private was a relative value with respondents being open to tradeoffs based on perceived benefits. Respondents largely focused on obvious possibilities such as power consumption feedback. However, they possessed limited knowledge regarding the capabilities of Smart Metering and pointed towards a lack of information on possible benefits.

Few respondents had personal experience with Smart Metering. Therefore, it could have been difficult for them to evaluate how the new technology could impact their privacy. In general, it is unclear to people what information is encoded in the vast amount of data continuously collected by a Smart Meter, especially when analyzed in combination with other data sources. This aspect is further exacerbated when the purposes of data analyses are unknown or unclear. In this regard, respondents admitted not knowing enough to understand why and to what degree the data in question might be sensitive.

> "In principle, I would prefer savings [over privacy]. However, I am probably lacking information on what utility providers or other parties can do with my data. The extent [of what might be done] is not clear to me." — P32 (F, 53)

Yet, our questionnaire uncovered diverse privacy expectations regarding Smart Metering. A minority of respondents stated that power consumption data collected by Smart Meters and customer data maintained by the utility provider (i.e., billing address and account information) were unimportant to them.

> "I do not have a problem with third parties having access to my power consumption data, even hourly data." — P16 (gender unspecified, age unspecified)

However, a majority of respondents wanted to set boundaries for the data related to their power consumption and customer accounts. Most often, addresses and account details were understood to be private and were not to be disclosed. In contrast, power consumption data was perceived largely as a resource to be traded for value-added services that provided individual or societal benefit.

> "If it was for a certain benefit, such as reducing power consumption costs or promoting sustainability, that'd be okay." — P24 (F, 23)

Respondents showed a willingness to take a high degree of responsibility for appropriate rights management and access control, demonstrating that provision of user-control was implicitly assumed. Respondents commonly suggested allowing consumer control over Smart Metering data distribution.

> "Trust always plays a big role with regard to data. As long as each person can decide who gives what data about his or her own power consumption, I think Smart Meters can be a great thing." — P23 (F, 20)

Regulatory agencies and utility providers were frequently perceived as responsible for data protection, but respondents recognized their own responsibility as well.

> "The legal framework, the general terms and conditions of the utility provider, and thus ultimately myself [are responsible for data protection and privacy in Smart Metering]. I have to read the terms and either object to the disclosure of the data or prohibit it." — P21 (F, age unspecified)

4.1.4 Potential Negative Consequences. Respondents often feared that the installation and/or use of Smart Metering could result in higher costs. When considering the most important factors, costs typically played a major role:

> "The success of a project to spread intelligent electricity meters will in any case be measured by the potential savings achieved by the customer, not by means of politically allocated subsidies, but by the saved kWh, and therefore by the customer's Euros, as well as by the benefit to the environment." — P11 (M, 53)

Respondents perceived several undesired real-world implications of Smart Metering, such as the threat of social exclusion due to technological advances. Most fears were regarding unwanted advertisements or potential hacking leading, in turn, to unstable electricity supply or incorrect billing. Additionally, a few respondents envisioned potential misuse by public institutions and moral shaming if a household was found to be consuming more power compared to similar households.

We found concrete ideas about how Smart Metering data could be abused, if shared. For example, respondents feared that data access by unwanted third-parties could impact them negatively:

> "I don't want my power consumption information or customer data to be passed on in any way, used for advertising purposes, or the amount or time of consumption passed on to third parties. I do not want any kind of 'offers' due to my consumption data." — P21 (F, age unspecified)

From a phenomenological perspective, data is always interpreted by individuals within a specific context. Thus, the respondent's comment above should be understood not as related to the sheer act of passing on data to another human, machine, or organization, but as regarding the information that can be deduced or action(s) that can be taken on the basis of the transferred data.

> "When and what month is observed makes no difference. I would find it strange if someone saw exactly how long I watched TV or used the computer. That's rather private." — P24 (F, 23)

The underlying fear was often related to the potential linking of power load with daily routines and habits. For instance, as in the case mentioned above, respondents were concerned about third parties being able to deduce the usage of specific appliances and, consequently, infer specific activities in the home. The potential ability to utilize power consumption data to gain knowledge of the routines and activities, including absence from home, was considered an undesirable implication of Smart Metering data analysis.

> "The main problem is again, as already mentioned, the creation and possibly criminal exploitation of when someone is absent from home." — P11 (M, 53)

> "Others could even 'see' when you are going to bed [by seeing when you] switch off the lights." — P21 (F, age unspecified)

We found recurring mentions of such real-world practices as an explanation for reservations toward Smart Metering. When respondents deemed data sensitive, they were implicitly referring to what information could be derived from the data in question. We also found several instances where respondents explicitly referred to the undesired implications of what could be done with the data (see Table 1). In other words, rather than describing specific *data* to be privacy sensitive, respondents mentioned *information* regarding living conditions, practices, or behavior as worth protecting.

> "Additionally, my private sphere needs to be maintained, which is why information regarding the use of the sauna and solarium as well as the TV and the Internet should be considered off limits." — P11 (M, 53)

A deeper examination of these sentiments revealed that they typically referred to the benefits and risks connected to everyday life practices. In a few extreme cases, this was taken so far as to fear surveillance of Internet and TV use, including specific sites visited or programs watched, respectively. Although such threats would be possible only on the basis of highly granular data transmission [59], other threats are more basic and require less data.

These potential negative consequences served as ways to express and prioritize privacy concerns. Instead of referring to the nature and the amount of data, participants were concerned about how the data might be used. We explored this aspect in depth in the subsequent focus groups.

Table 1. Implicit and explicit references to the implications of data transfer.

	Benefit	**Risk**
Implicit / vague expression	"I could share my personal power consumption with those I trust."	"A reservation for me is the high threat of misuse of data, such that the data will fall in the wrong hands."
Explicit / concrete expression	"I could check the power consumption of individual appliances and replace them if necessary or use them less."	"When and what month is observed makes no difference. I would find it strange if someone saw exactly how long I watched TV or used the computer. That's rather private."

4.2 Focus Groups: Refining Characterizations of Benefits and Risks of Smart Metering

Our focus group design was motivated by the ways in which questionnaire respondents characterized beneficial and undesired uses of Smart Metering. Our goal was to utilize the focus groups to collect more details on these perceived benefits and risks. The findings reported in this subsection are derived from group discussions and therefore the corresponding quotes are not attributed to a single person. Overall, across the questionnaire and focus group responses, we identified 36 scenarios connected to the use of Smart Metering data (16 related to benefits and 20 to risks) (see Table 2). We organized these scenarios under several higher level themes.

4.2.1 Relationship with the Utility Provider. The scenarios that fell under this cluster were concerned with the relationship and interaction with the utility providers, such as saving costs by switching between tariff tiers or negotiating a tailored contract. Many positive features were mentioned, linked largely to contracts. One of the most commonly mentioned benefits was a flexible tariff structure that could help optimize power consumption and lower electricity costs. For instance, participants found value in automated control of appliances such that they could be operated during periods of cheaper tariffs. Participants desired that the utility provider help shift the power load to periods of low tariff.

> "Utility provider could provide added value in allowing the control of air conditioning or heating according to peak loads."

In addition, participants found it beneficial that a Smart Meter could be read remotely, thus eliminating the need for an in-person appointment for meter readout.

> "The utility provider could access power consumption data remotely, so the annoyance of scheduling appointments with service technicians will become obsolete."

Ironically, flexible tariffs, a much-advertised consumer benefit from Smart Metering, were perceived by some as a potential disadvantage. Participants feared that they could face price discrimination without their knowledge or have their electricity bills go up if their power consumption patterns lacked flexibility.

> "Less flexible households must consume power at peak price times."

Additionally, participants cautioned that electricity could be wasted on unnecessary uses simply because it is cheap during periods of lower tariffs.

Table 2. Perceived benefits and risks with number of corresponding mentions in the questionnaire and focus group responses, respectively.

Perceived Benefits	Perceived Risks
Feedback	**Actions of Utility Providers**
• Consumption data could be available online anytime, anywhere. (*31/4*)	• The utility provider could engage in price discrimination. (*1/3*)
• Consumption data could be compared and shared with family and friends. (*10/4*)	• The utility provider could get sensitive information. (*20/2*)
• Consumption data could be collected anonymously for comparison with similar households / appliances. (*13/4*)	• The utility provider could switch off power. (*3/1*)
Savings	**Exposure of Life Practices**
• Tariffs could be made flexible. (*3/1*)	• One may become a 'transparent citizen' and have privacy violated. (*31/4*)
• Tariffs could be optimized for individual households. (*2/2*)	• Home presence could be deduced. (*8/2*)
Flexibility	• Third parties could derive behavior patterns and create profiles. (*11/3*)
• Tariffs could be simplified. (*1/1*)	• Employers could engage in employee surveillance (e.g., coffee maker/computer use). (*1/0*)
• Meters could be read remotely (without an in-person appointment). (*0/1*)	• Others could know of one's purchases. (*1/0*)
• When moving, account changes can be processed faster. (*0/1*)	**Advertising**
Sustainability	• Advertisers could personalize ads. (*21/4*)
• People could be incentivized to engage in environmentally friendly habits. (*6/2*)	• Salespersons could know when someone is home. (*1/0*)
Independence	**Abuse**
• People could manage how other parties access the data. (*2/3*)	• Power could be disrupted by bad actors. (*7/2*)
Advertising	• Consumption data could be modified by hackers. (*11/2*)
• Advertising could be optimized through personalization (e.g., showing ads for a more efficient fridge based on meter readings). (*6/2*)	• Private information could be collected by malicious actors. (*4/0*)
Safety/Security	**General Concerns**
• People could receive a warning message in case an appliance (e.g., stove) is not turned off. (*12/2*)	• Smart Metering systems might be hard to handle. (*8/0*)
• People (especially the elderly) could receive a call/text message when no consumption is recorded or consumption differs from daily routines. (*5/1*)	• People may waste electricity when it is cheaper. (*0/1*)
• People could check on appliances from remote locations. (*4/1*)	• Consumption sharing may create moral exposure by the need to justify choices. (*7/1*)
Infeasible	**Infeasible**
• People could remotely (e.g., via mobile applications) switch appliances on/off. (*3/0*)	• Manufacturers could analyze the use of specific products. (*1/1*)
• People could separate the consumption of individual households in buildings with a Smart Meter shared across all apartments. (*1/0*)	• The agency that collects fees to support public broadcasting could check for the existence of specific appliances. (*1/0*)
	• Movie industry could target people based on their content consumption. (*1/0*)
	• Neighbors in apartment buildings could control each other's power consumption. (*1/0*)

4.2.2 Third Party Services. Participants were able to identify many beneficial third party services that could operate by using Smart Metering data. Most of these services were data driven and made use of power consumption monitoring. Infrastructure benefits were also mentioned.

4.2.3 Power Consumption Feedback. The most frequently mentioned scenarios were related to information regarding power consumption and, in turn, using that information to provide feedback that could help control and optimize consumption. Some participants liked the opportunity to learn about their own consumption patterns.

> "Real time feedback would allow me to learn about my power consumption in the first place. With the current meter in your basement, you get a bill only once a month, if not once a year."

This, however, was perceived as a double-edged sword as it could lead to the potentially uncomfortable discovery that one is consuming high amounts of power. Participants came up with a variety of additional possible uses for the feedback such as comparing one's power consumption with peers, family members, or households with similar appliances.

Real-time feedback was deemed valuable for optimizing power consumption. Participants mentioned that such feedback could help identify appliances that use high amounts of power so that these could be turned off or replaced if necessary. Another foreseen benefit was the ability to utilize the feedback to save money by shifting power consumption to exploit the variable tariffs offered by Smart Metering.

> "I can analyze my own data. Based on my power consumption, maybe I should run the washing machine at night. In doing so, I can save money and maybe I can plan better knowing: 'Ah, I consume more in the winter."'

Along with the benefits, participants identified privacy risks such as unwanted sharing of power consumption data with third parties and the potential for inferring personal routines based on the data (see Section 4.2.8).

4.2.4 Home Control. Some participants discussed scenarios that considered a Smart Meter as a piece within a larger 'Smart Home,' thus envisioning that Smart Metering data could make the Smart Home more 'intelligent.' For example, one participant indicated that the Smart Meter could send text alerts to a mobile phone in situations such as a stove left on by accident. Participants were also interested in remote access to the home to ensure that everything was in order in their absence.

> "Alarm functions in case an appliance does not work properly or is not shut off."

Similar to the features promised by other Smart Home products, participants felt that Smart Metering data could be applied to support safety checks for elderly people living on their own.

> "Checking on whether elderly relatives are still active at home, or whether their behavior is abnormal, compared to normal days."

4.2.5 Sustainability. Improved sustainability was second only to efficiency as a core benefit expected from the Smart Grid. Scenarios pertaining to sustainability expressed a general desire to utilize the capabilities of Smart Metering to engage in environmentally responsible behavior, such as reducing individual and societal carbon footprints and avoiding electricity wastage. By having a Smart Meter installed, participants wished to help grid managers save power by effectively managing the overall power load and distribution. For example, participants mentioned that the grid operator could use global power consumption data to manage the grid more effectively, reducing societal cost.

> "The power provider could better regulate its power supply because it has better control over when and where there is more or less power consumption."

4.2.6 Transparency and Trust. While participants showed a strong interest in Smart Metering, feelings about the benefits of the system were mixed. As a prerequisite, participants desired a high levels of transparency from the system and demanded that consumers be allowed control over data disclosure.

In line with the current state of knowledge on how consumers rate the trustworthiness of their utility providers, our participants indicated that trust – or lack thereof – would play a major role in decisions regarding the acceptability of Smart Metering. Participants saw the provision of means to control Smart Metering data distribution as a potential way to promote trust in the service providers. Yet, participants felt that those collecting and recording the data should bear the main charge of enforcing appropriate rights management and access control. While discussing the measures for helping people understand and control data disclosure, one participant mentioned the potential exploitation of a lack of sufficient information on the part of the users.

> "Users will be pushed in directions favorable to third parties."

Similarly, another participant feared gaining nothing from Smart Metering and was not willing to have a Smart Meter installed because she perceived the current circumstances as unfair to consumers such as herself.

> "Consumer will not have benefits while service providers get sensitive information."

4.2.7 Power Load Monitoring. Similar to most perceived benefits, security and privacy risks were connected to power load monitoring by third parties. In this regard, data collection was perceived to be ambiguous and data disclosure preferences depended on balancing the corresponding benefits and risks.

4.2.8 Potential Exposure of Everyday Practices. A frequently mentioned fear was the ability of third parties to derive information about routines and habits. As in the questionnaire responses, the identification of patterns of personal behavior was a regularly expressed concern in all of the focus groups.

> "[...] One could see who is lying in front of the TV all day ... that guy could maybe receive a higher bill or something."

Participants came up with many possible scenarios connected to the disclosure of living patterns within a home. Most of these centered on third parties being able to identify appliances by power load monitoring:

> "[People] can be surveilled during work times. How often was the coffee machine used? When was the computer shut down?"

> "The GEZ [Gebühreneinzugszentrale, the agency that collects fees to support German public broadcasting] could check which kind of appliances exist in a home [to calculate fees]."

4.2.9 Advertising. A readily identified theme was the potential for Smart Meters to collect and disclose data that could be used for personalized advertising. While advertisements in general were perceived as annoying, a few participants did see value in some forms of personalized advertising such as those for devices or appliances that could or should be replaced based on their power consumption patterns.

> "Manufacturers could have an interest in tracking the power consumption of their appliances."

> "Personalized advertising (i.e., for power saving fridges based on measured power consumption data)."

In general, participants expressed that it was absolutely necessary to have the ability to control the amount and kind of such advertising. Many participants foresaw unwanted access to their data for personalized advertising. In this regard, participants worried that salespersons would be able to plan their visits when power consumption indicated that someone was home.

> "Salespersons get to know when somebody is home."

A related scenario was the possibility of advertising by the utility providers themselves. Although the consumer could potentially benefit from such advertising, e.g., by becoming aware of cost saving opportunities, it was regarded as bothersome and inconvenient.

4.2.10 Potential for Abuse. Aside from legitimate third-party processing of power consumption data, participants imagined scenarios of abuse and manipulation. Participants were worried about the possibility of malicious actors viewing and changing billing information and stealing power.

> "[...] now it gets in somebody's head: 'Oh, wouldn't it be fun to cut off my neighbor's power supply!' Then he somehow hacks the meter, because, you know, like it has never happened that an IT-based system was hacked [...]."

These possibilities of manipulating power consumption data or the electricity supply itself were commonly mentioned fears. Ironically, preventing such abuse is touted as one of the benefits of Smart Metering. Yet, we found that some participants were worried about security related aspects, such as hacking and other malicious attacks. We excluded these scenarios from further consideration because they are out of the scope of a privacy management tool.

4.2.11 Usability. Although not directly connected to privacy, participants considered the usability of Smart Meters to be important. They worried that a system that is difficult to understand and use could result in unwanted data disclosure and bad power consumption decisions.

4.2.12 Infeasible Scenarios. Six of the scenarios mentioned by the participants were infeasible due to technological constraints (two deemed as benefits, four as risks; see Table 2). For example, some believed that third parties could use Smart Metering data to identify and read TV and computer screens.

> "The movie industry could check which movies were watched and identify pirated copies."

Even though these risks are unrealistic, since people perceive them as real, they are part of the motivational factors that shape people's attitudes towards Smart Metering. During the study, we did not point out the unrealistic nature of these fears as we did not wish to *influence* attitudes but to *understand* ones that currently exist. However, the infeasibility of these scenarios was explained at the end of the study. These six scenarios were excluded from further consideration as these are unsuitable for a realistic consideration of benefits and risks of Smart Metering.

4.3 Design Probe: Evaluating Benefits and Risks Information as a Privacy Management Resource

The questionnaire and focus group responses provided a rich picture of how people characterize the benefits and risks of Smart Metering in terms of anticipated real-world scenarios that highlight the desired and undesired implications of data disclosure. These implications frequently impacted disclosure decisions. Therefore, we created a design probe to evaluate whether we could assist people in making Smart Metering privacy decisions by presenting the respondent-generated implications as additional information related to the respective services. The probe was designed as an Android application featuring the three steps described in Section 3.4.

The design probe involved watching an introductory video followed by choosing Smart Metering services from a set of eight services, without any information on the implications of choosing the services. The service choice utilized the common all-or-nothing approach that lacks the ability to control the granularity of data disclosure. There was no information about, or instructions pertaining to, privacy. The eight services were based on the potential benefits that respondents in the questionnaires and focus groups expected from Smart Metering (see Figure 3a). After choosing services of interest, one was provided additional information regarding the implications of the subscriptions and allowed to adjust the granularity of the data disclosure or even cancel the subscription (see Figure 3b). Each service and level of granularity was associated with a corresponding set of benefits and risks regarding quality of service and privacy. By asking for basic interest in the service first and providing implications second, the probe was designed to uncover whether one was likely to change his or her mind based on the information presented.

The 205 individuals who interacted with the design probe subscribed to 597 services (an average of 2.9 services per participant) with all but 13 subscribing to at least one service. As noted above, this initial step offered no settings for privacy preferences. Instead, the disclosure option with the highest granularity was chosen by default (see Section 3.4).

Figure 5 shows the distribution of the choices across the services. The most subscribed service (N=137) was *Smart Control*, followed *Family Comparison* (N=85). On the other hand, *Personalized Advertising* (N=43) was the least popular. For most of the services, between 7% to 9% of the initial subscribers decided to cancel the service altogether during the subsequent step of examining the disclosure implications. Only the *Social Media* (0%) and *Family Comparison* services (2.4%) included fewer dropouts.

For all services, an overwhelming majority of participants adjusted their disclosure settings in the second step. The analysis of the adjustments made in the second step found that participants chose to change their disclosure settings or cancel their subscriptions in more than 86% of the cases, which provides strong support for the relevance and usefulness of the implications we included to facilitate more informed privacy decision-making. Figure 5 shows the percentages of participants who changed the default for each of the services. These are further split into those who reduced the granularity of the disclosure and those who chose to cancel the subscription altogether.

It could be argued that changes to the disclosure setting may not stem solely from the information provided by the probe but could instead be due to a general desire to avoid the default high-granularity data disclosure. However, it should be noted that the proportion of participants who adjusted their settings is very high. Further, more than 6% of the participants chose to cancel their initial subscriptions completely when they encountered the privacy implications. The desire to change granularity does not explain the complete revocation of a subscription, thus indicating that the privacy implication information provided did impact the data disclosure preferences. In terms of granularity, the most preferred setting was data disclosure on a monthly basis (43%) followed by the daily option (35%). These choices demonstrate that the probe helped participants choose the benefits of Smart Metering achievable within the constraints of their privacy desires.

Analysis of the post-study interview responses indicates that a vast majority of the participants found our design probe useful for understanding the Smart Metering technology and making related privacy decisions. The mean initial adoption rate of 2.9 services per participant gives us reason to believe that participants found the services offered to be valuable as well. A large group of participants reported using the provided implications as an important guideline. The implication information was found beneficial for deciding how to achieve a personally acceptable tradeoff between the benefits and privacy risks of the subscribed services. For instance, one participant remarked:

> "[..] just watching the pros and cons was helpful for me, when it showed me that they could know when I get up, when I do something and so on. I didn't think it would be so clear based on when I use electricity." — E13 (M, 24)

More than half of the participants mentioned that the implication information helped them choose an appropriate level of information disclosure. As a participant explained:

> "[It helped] that you can see the different service providers and the decision regarding how often data should be transferred . . . that one sees there directly, what influence it [the decision] has on the individual service provider and on your privacy based on the information that is passed on." — E17 (M, 26)

About one third of the participants made privacy decisions based primarily on the options for setting the temporal granularity of data disclosure.

> "I really kept my mind on the intervals in question. Annually or monthly would be okay, or maybe semiannual or quarterly, but certainly not more often." — E108 (F, 53)

This participant prioritized 'intervals' as a criterion for data disclosure decisions. However, simply providing interval based options does not signal the sensitivity of the corresponding disclosure and could still lead to undesired information sharing unless the settings are accompanied by information on the implications of each interval choice as included in our design probe. Therefore, those who focus mainly on temporal intervals when making data disclosure decisions can still be well served by the corresponding implications.

In particular, those without a professional or technological educational background reported that they found the additional information useful for privacy assessment. In contrast, those who indicated they were privacy-sensitive or technically savvy, reported comparatively lower benefit from the presented benefits and risks. These participants mentioned that they already knew the information provided.

> "I guess I was already able to judge the risks and benefits before I saw them. What was written there had some influence, but generally speaking, my decisions were already clear beforehand." — E7 (M, 19)

Note that this tech-savvy participant alludes to an indirect guiding influence of benefits and risks despite indicating that he did not find the information overly useful. Many other factors for making disclosure decisions are suggested by the literature, such as reliance on past experience or trust in the service provider. However, even those who mentioned preferring other decision-making resources did not react negatively to the benefits and risks we described, thus suggesting that inclusion of the information poses no adverse effects even if the information is not consulted.

Age or prior knowledge of Smart Metering made little difference in terms of perceived usefulness of the provided benefits and risks. While only a few participants stated that the design probe did not help their privacy decision-making, about 17% were undecided about the utility of the probe. Even though we imposed no time limit for completing the tasks, these participants felt that they needed more time and information to reflect on Smart Metering before feeling sufficiently confident in their ability to make appropriate privacy decisions. A few participants found the provided implication information insufficient or overly detailed. As a potential remedy for these issues, one person suggested personalizing the implications:

> "I believe it is hard to generalize [the implications] with only a few statements. You would have to look at it in a more personalized manner." — E61 (F, 19)

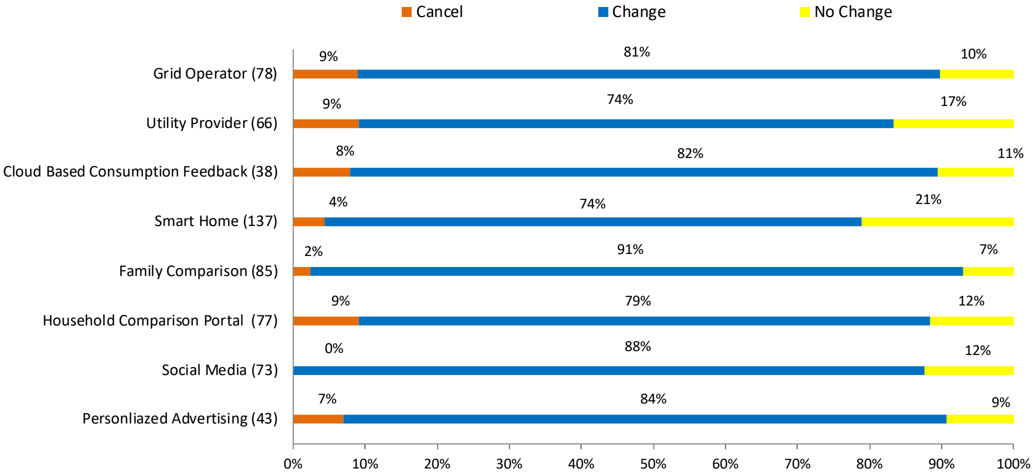


Fig. 5. Service subscription decisions of the participants after encountering the corresponding privacy implications.

The participant generally understood and valued the mechanism used to make the implications accountable but called for an even stronger connection via personalizing the information.

5 DISCUSSION AND IMPLICATIONS

Our primary goal was to connect existing practices that serve as meaningful resources for judging information disclosure in Smart Metering. We found that people harbor significant concerns regarding the collection and sharing of power consumption data collected by Smart Meters. Our findings contribute to the ongoing discourse on usable privacy in three ways:

- First, we uncover concrete instances of ‘privacy work’ in Smart Metering that point to the relevance of existing everyday practices in making disclosure decisions.
- Second, we suggest supplementing the dominant data-centered approach to privacy management with a perspective that makes the privacy implications of information disclosure accountable and meaningful in terms of people’s practices.
- Third, we provide a set of methods and a starting point for intertwining regulatory, technological, and individual perspectives on privacy.

5.1 Make Data Accountable via Connection to Practices

Legislation, such as the GDPR [41] and FIPPS [138], demands the provision of ex ante transparency for service subscribers, commonly interpreted as a key requirement for informed consent. As we discussed earlier, there is plenty of research on providing feedback on privacy settings and evaluating various privacy management mechanisms. We have taken a further step by looking at how users go about becoming informed and applying their privacy choices when they are given certain kinds of information. In this regard, our approach is similar to practice based research on data work [43]. However, our approach differs by taking a strict ex ante perspective since Smart-Meter-equipped households will need to make their privacy decisions up-front. We, therefore, refrained from collecting and showing actual Smart Metering data, looking instead at existing practices and the refinement of these practices as and when individuals are provided relevant information about the practices.

Analysis of the open-ended responses in the questionnaire highlighted that concerns regarding Smart Metering were commonly expressed in terms of what third parties could get to know about everyday practices based on the data collected by a Smart Meter. As we have shown, many of the attitudes on display were connected to the degree of trust in utility providers and third parties. Few respondents mentioned issues of trust within the family context, though some were concerned with surveillance by others in the neighborhood. Motivated by the findings of our initial exploration, we delved deeper into the relevance and utility of supporting privacy decision-making by providing people with the implications of their choices framed in terms of existing life practices. Our results demonstrate that connecting data disclosure its potential real-world consequences is a promising design technique for usable privacy. For example, many participants were concerned that Smart Metering data could reveal domestic activities and routines, such as the presence of someone at home or usage patterns of appliances.

Even though we identified a wide variety of scenarios, some individuals found these too vague or impersonal to connect with their own practices. The complexity of privacy is itself well described, e.g. by Barkhuus [11]. Still, highlighting the implications for everyday life seems to serve as a design resource that non-experts find relatable, thus distinguishing it from the typical complex and technology-dominated discourse related to ubiquitous computing technologies. In this regard, our work is similar to Crabtree et al. [28] who found people managing their ‘attack surface’ in the digital world against third parties. However, it is important to note that privacy related choices were shaped by not just the potential but also the perceived implications of data disclosure. The folk theories that people have about such matters often guide behavior [113].

5.2 Support Information-centered Privacy Management

Privacy legislation typically stresses the importance of the data to be transferred along with its transfer frequency and recipients. Such data-centric perspective is also seen in privacy management tools across systems, such as social networks [62], organizational information systems [16], and e-commerce [3]. In our study, we too frequently found users being concerned about ‘who gets what and how often.’ By taking a data-centered approach prevalent privacy mechanisms lead to users being burdened with interpreting the consequences of the data disclosure. In cases where the data provided is relatively familiar, such as credit card information when shopping online, attack vectors may be largely clear. However, as IoT applications become commonplace, more and more sensors are collecting abstract data which users as yet cannot judge in terms of informational value for themselves or third parties.

Our study showed the relevance of another, often complementary, collection of related practices of making the disclosed data accountable, revolving around worries concerning the information third parties could derive in terms of “what do they know about me?” [116]. These viewpoints are not well covered by the privacy protection mechanisms currently envisioned for Smart Metering or addressed at all in the related privacy protection legislation. Our collection of perceived privacy implications and potential value-added services provides a substantial addition to an otherwise one-sided discourse focused on the data rather than the potential or feared consequences of its disclosure. In this regard, Crabtree et al. articulate a main challenge in human data interaction (HDI): “If users are to have the ability to exercise agency within an HDI system in any meaningful way, data sources must provide a minimum level of legibility as to what data they contain, what inferences might be drawn from that data [. . .]” [27].

Forms of impact assessment are known from technology research and computer ethics [69, 73]. With regard to privacy impact assessment [23], there are frameworks for companies or developers to assess the ethical impact of their technologies and products [144]. For highly sensitive data, such as data regarding health or religion, the GDPR prescribes such impact assessment [41]. The literature and the GDPR argue for enabling individuals to handle their online privacy. Our study suggests that individuals could potentially perform a privacy impact assessment for themselves. In this regard, we have shown that connecting data disclosure to existing practices is a promising way to provide meaningful information to support data work. Implementing the design probe by incorporating the scenarios collected via questionnaire and focus group responses was a successful approach; participants used the corresponding implications in their privacy decision-making as a resource for making sense of Smart Metering data .

We argue for extending the traditional data-centric view to *information-centered* privacy management, thus allowing non-experts to engage in personal privacy impact assessment. We demonstrate that individuals may perceive information in varied ways, and the implications of privacy settings can be made accessible such that they could be judged in accordance with existing life practices, even when the data in question is abstract. Opening up the design space in this way provides greater flexibility to support a range of privacy related behaviors by surfacing the potential for secondary uses of data and perceived threats brought about by the data disclosure. Jones and Soltren [74] provided a such a threat analysis of privacy management on Facebook, albeit not in a user-centered manner. While tools for abstract risk-benefit analysis do exist, we suggest grounding their design in everyday routines and practices, thus providing a bridge to technologically complex and abstract information on the data to be transferred. Optimally, the users themselves would generate relevant scenarios and the corresponding implications, although the implications could arguably be extended and/or managed by domain experts as well. Generation of scenarios and their implications could also be crowd-sourced. Further, the scenarios and implications connected with specific data or services could be made available publicly as a community design resource for *practice based privacy management* in ubiquitous computing technologies. In this regard, our user-generated benefits and risks of Smart Metering provide the basis for privacy impact assessment that could be conducted by non-experts.

5.3 Include End Users in the Development of Smart Infrastructures

The current discourse on privacy is largely concerned with regulatory factors and/or stresses the importance of security mechanisms and privacy algorithms from a technological perspective. The introduction of smartphones and their privacy implications were largely unforeseen from the policy perspective and, as a result, PbD guidelines are mainly encountered in the technological regulation of ubiquitous computing devices. In contrast to industry representatives, users typically have no voice or representation when decisions are made about the requirements to inform system design. At the same time, the purposes of data collection are only vaguely specified. Concrete potential implications visible to consumers would extend purpose-assignment of data disclosure required by German law [54]. Without understanding consumer demands, decisions on usability or interfaces to specify privacy parameters lack a grounding in practice and, consequently, are based on speculative assumptions about a hypothetical ‘average’ user. Beyond the concrete case of Smart Metering, we argue that consumers should not be reduced to passive objects subjected to political forces and technological measures. Instead, consumers should be considered active subjects in the standardization process of Smart Infrastructures. Otherwise, technologies face an increased danger of lacking user acceptance [120] as reflected in the acceptance problems regarding electronic health records [18] or digitally enhanced ID cards [101, 134]. In this regard, user-centered design [2], and, more specifically, multilateral security [111], provide appropriate and well-established process models.

Our research provides a method to uncover the role of practices in privacy decision-making, in turn opening up the design space for industry, designers, and policy makers. A majority of our study participants had not heard of Smart Metering and the Smart Grid prior to the study.

Nevertheless, the participants grasped the basic concept quickly and produced a number of ideas for possible benefits and undesirable aspects. Our findings show that even non-experts are able to develop and express an understanding of a complex technology before actively experiencing its use, thus demonstrating that non-experts can articulate privacy demands regarding future technologies. Not having to rely on experts allows stakeholders involved in long-term legislative procedures to generate a realistic assessment of the demands for possible protective measures, not only for existing services and products but, more importantly, also for the ones yet to come. We argue that our approach can help generate more usable solutions for privacy management in a number of different domains. For instance, current technological trends that could be addressed by such an integrative view of privacy are Smart Homes, Smart Cities, or Connected Cars. Knowing how people react to and use information about privacy-related implications (and, indeed, other information resources) ought to provide useful and complementary insight to inform design decisions.

6 LIMITATIONS

Given that we have drawn our insight via three distinct methods, we are fairly confident in the robustness of our findings. That said, several limitations must be kept in mind when considering the general applicability of these results.

The sample sizes for the questionnaire and the focus groups are relatively small, and the participants in all three parts of the research hail from a single geographical region in Germany. Therefore, we cannot claim to have included a representative sample of users of Smart Meters. Even so, in the sense of theoretical sampling [25], our findings cover a broad spectrum of participants. Moreover, Germany is considered a leader among Western societies in its treatment of privacy and data protection issues. With the advent of the GDPR [41], these aspects will become more pressing in the rest of the EU as well.

The response rate for the questionnaire was relatively low (17%), resulting in a potentially skewed sample that may disproportionately include those with strong opinions on privacy or high interest in Smart Metering. Such self-selection is a common shortcoming of questionnaire responses collected by mail. We tried to minimize this bias by providing an incentive to respond to the questionnaire. Further, the questionnaire responses served only as a starting point for understanding how people characterize privacy considerations in Smart Metering. The focus groups served the purpose of validating the insight from the questionnaire responses in addition to providing more information about the implications of data disclosure.

The focus groups were not gender-balanced, with a relatively small proportion of female participants. However, the focus groups were conducted primarily to verify and expand the insight gained from the earlier questionnaire responses. Moreover, the questionnaire and evaluation phases were reasonably gender balanced. While it is possible that additional female participants in the focus groups could have provided more/other insight, it should be noted that we did not aim for an exhaustive list of scenarios for the use of Smart Metering data. Rather, our goal was to utilize the collected scenarios as a basis for the design of usable privacy management features. The evaluation via the design probe was gender balanced with nearly 50% female participation (100 female participants out of 205 participants), and we did not find any gender differences in usefulness of the provided scenarios.

Although we obtained a large sample for interacting with the design probe by soliciting participants in public places, the sample may be biased based on self-selection and the recruitment times and places. It could be further argued that the approach may have led to the recruitment of those who may not have been fully attentive to the study. Further, the design probe had no actual effects because the service subscriptions and privacy settings chosen during the study were hypothetical.

While we feel that the design probe was real enough to provide useful results, generalizing from the hypothetical to the real should be treated with caution.

As mentioned above, our collection of scenarios and corresponding privacy implications is not exhaustive. Our research was intended to provide an initial insight into how people treat privacy matters when additional relevant information is provided. An important aspect of this approach was uncovering the relationship of data disclosure preferences with existing practices and privacy concerns. As such, we argue that our collection provides a basic set of implications relevant to privacy decision-making in Smart Metering, thus constituting a starting point to inform design. The list can be extended by future work. Additionally, it would be useful to investigate the relevance and effectiveness of expert-generated implications to support privacy expectations and choices of non-experts.

None of the participants had a Smart Meter installed in their homes. When Smart Meters are eventually deployed, users must inevitably make privacy decisions without prior experience with these systems. In line with the research on technology appropriation [133], we wanted to understand perceived privacy issues in Smart Metering with non-experts (in the sense that, regardless of familiarity with other technologies, they had no direct exposure to Smart Metering). Future studies should aim for more balanced and representative samples of those with Smart Meters installed at home.

7 FUTURE WORK

In the future, as suggested by Solove [131], we plan to evaluate the concept of making the implications of data disclosure transparent to users in contexts other than Smart Metering. Our approach could be applied to a variety of services and infrastructures which collect data automatically and (mostly) invisibly. We are especially interested in technologies already in widespread use. For example, smartphones are complex devices with an extensive ecosystem of apps, supported by the data collected (often invisibly) by a multitude of sensors on the phone. Similarly, ordinary households are increasingly adopting Smart Home devices that capture and potentially reveal fine grained information about domestic life. Another upcoming domain is the automotive sector which is currently investigating Connected Cars for autonomous driving and value-added services. The approach we utilized to study privacy aspects of Smart Metering can be useful for unpacking privacy considerations in these cyber-physical systems.

We described how to support privacy decision-making related to abstract fine-grained data. Yet, even when privacy management UX is usable, it is typically perceived as a burden and an overhead [148]. More research is needed on techniques to alleviate this burden. To this end, privacy agents based on Artificial Intelligence (AI) are promising for suggesting or presenting personalized recommendations for privacy choices [92]. Similarly, peers or experts could be leveraged for supporting privacy management [49].

One challenge in trying to map the potential privacy consequences arises from the potential triangulation of data from different sources (e.g., Smart Metering data combined with data from social network sites, Web browser histories, etc.). Such triangulation may examine data relationships across sources to derive sensitive private information. Choosing to leave out triangulated relationships across multiple data sources could make privacy-relevant information and implications less precise. Yet, including the information could lead to information overload, potentially lowering the quality of privacy decision-making. Further exploration is needed to understand effective and optimum UX for helping users make sense of the privacy implications due to the fusion of data from diverse sources, such as IoT.

8 CONCLUSION

We presented an understanding of the privacy demands in Smart Metering from a consumer perspective. Based on a design case study approach [145], we derived design implications for usable privacy management in Smart Metering and demonstrated how to integrate the perspectives of future users into the design of novel technologies.

Connected technologies are increasingly introduced into everyday life, sometimes voluntarily (e.g., Smart Home technology), sometimes without choice (e.g., Smart Metering in some countries). The potential of such technologies for collecting and transmitting sensitive personal data about everyday practices poses challenges for individual privacy decision-making.

Most of our participants were able to articulate privacy needs for Smart Metering without prior exposure to such a system. Our findings thus demonstrate that non-experts can contribute to framing privacy demands for novel technologies. While these initial reactions may change as the technology is appropriated [33], privacy demands of novices should nonetheless be taken into account to foster user acceptance and adoption in the first place. Taking privacy needs and concerns seriously can guide the design of appropriate tools and controls to manage the disclosure of personal data, not only in Smart Metering, but in an increasingly networked world.

Specifically with regard to design, our research revealed that participants made their assumptions about the disclosure of power consumption data accountable by referring to the information that could be derived from the data. Consequently, data disclosure decisions were driven by an assessment of the privacy impact of disclosing the derived information. As a result, highlighting the potential consequences of data disclosure in terms of everyday practices helped people understand the implications of the available privacy choices.

In contrast, current privacy management systems typically highlight data and its recipients, disconnected from the practices of the individuals. Therefore, we advocate that privacy tools strive to make abstract data more accountable by framing privacy decision-making in terms of the real-world consequences of the privacy decision in question. To this end, we contribute an initial collection of user-generated scenarios with corresponding benefits and risks to serve as a basis for making privacy management systems more usable.

We see three relevant strands for future work. First, we need a deeper understanding of privacy implications of Smart Metering based on real-world usage. As people get used to Smart Metering and gain expertise, their privacy attitudes and behaviors will likely evolve beyond the initially expressed desires in the novice phase. Second, we seek to transfer our approach for investigating privacy demands from a user perspective to other domains like smartphones, Smart Homes, and Connected Cars. As upcoming technological developments, such as IoT devices, continue to introduce new data sensors into everyday life, privacy management is becoming increasingly complex and non-trivial, thus raising the burden on users. To alleviate this burden in a useful and usable way, privacy management tools will have to balance comprehensiveness with the needs of minimizing the required effort. Third, policy makers can apply the methodological starting point we have provided to cater to people's desire for usable privacy management. The HCI community has the potential to inform and enrich regulatory initiatives related to future technologies by service as the voice of the end users.

ACKNOWLEDGMENTS

We want to thank all participants of our studies for their efforts and contribution. We acknowledge Julian Weber, Christopher Klein, David Bismor, and Tim Rübsamen for their help with the data collection and Mati Steinelli for general support. Thanks are due to Morgan Brockman and Mihir

Mahajan for proofreading a draft version of this paper. The research was funded by the German Federal Ministry for Economic Affairs and Technology under grant number KF2111503LF2.

A QUESTIONNAIRE INSTRUMENT

A.1 Background Text

Rising electricity prices are a trending topic in recent years. For many people, electricity costs are increasingly an important factor in the household budget. But where and how can you save? In the near future, a Smart Meter, which simply replaces your old electricity meter, could provide you with information and assistance about precisely this issue. A Smart Meter captures the power consumption of your household and can immediately display and evaluate it. It can also, for example, accurately assess past power consumption to reveal electricity usage and leaks that might have gone unnoticed. In addition, the Smart Meter can provide information on how much power was and is currently being consumed (e.g., via an App on a smartphone or a tablet, a laptop, or a computer). Thus, the consumer can gain control and, ultimately, power consumption can be lowered.

The utility providers themselves gain various advantages from Smart Metering. The Smart Meter can transmit power consumption in near real-time to the respective utility providers, allowing more detailed calculation of the power required, thus limiting excessive overproduction. Such a mode of operation also protects the environment because the buffer capacity needed to keep the grid stable can be reduced. Smart Meters thus provide important benefits to consumers as well as providers.

The German federal government has initiated a process so that Smart Meters may be installed voluntarily on the request of the consumer in each household. In this questionnaire, we want to learn about your personal attitude toward Smart Metering.

Please answer the following questions in complete sentences or bullet points. Please be as clear as possible.

Note: We will hold a raffle that includes all carefully completed questionnaires. The raffle will be for 4 vouchers each with a value of 20 Euros for Amazon, the local mall, or the DM drugstore. (More information about the raffle is at the end of the questionnaire.) Personal data will be used only for conducting the raffle associated with this questionnaire. All addresses will be destroyed after collecting questionnaire responses and holding the raffle. You will receive no further correspondence from us unless you win the raffle or want to be kept informed about the project.

A.2 Demographics

To understand your opinion and analyze your responses, please tell us some information about yourself.

- Gender:
  - Male
  - Female
- Age:
- Do you own your place of residence?
  - Yes
  - No
- How many people live in your household?
- Are you responsible for paying for the electricity in your household?
  - Yes
  - No
- What is your monthly gross income? (*Optional*)

  - None
  - 1–450€
  - 451–2000€
  - 2001-4000€
  - >4000€

A.3 Introductory Questions on Electricity

- What comes to your mind when you think about the topic of electricity as connected with safety?
- What comes to your mind when you think about the topic of electricity as connected with privacy?
- What is important to you when it comes to your power consumption data and customer information provided to the utility company?

A.4 Settings and Profiles for Smart Meters

Imagine that you could assess the information on the power consumption of any person or group of people participating in Smart Metering if, in return, you share your information as well.

- With whom would you want to share your data? (e.g., neighbors, friends, family, other people, the utility providers, the federal government or the Federal Office of Energy and Environment, anonymous comparison websites, other companies involved in the electricity supply, etc.)
- Why would anonymous power consumption data from other households be of interest to you?
- What do you think about the fact that others could view, for example, your power consumption for the current day, the previous day, or the previous month?
- How would you characterize the differences based on what can be viewed and when?
- Who do you see as responsible for ensuring that your power consumption data is accessible only to those people and organizations you would want to have access to the data?

A.5 Privacy in Smart Metering

People might share the data on their power consumption because they perceive value in comparing their consumption with others.

- Which safeguards would you wish to have in order to protect your data?
- Which concerns do you have in distributing the data? What data do you consider particularly worthy of protection?
- How do you rate the difference between others knowing your total power consumption in Watts and others knowing the consumption based on individual appliances?
- People who can access your complete consumption data could, for example, determine which appliances are on. What would you possibly worry about?
- To what extent would electricity cost savings compensate for possible for privacy and security concerns related to Smart Meters?
- What is your take on the following tension: More privacy provides less savings while less privacy allows more savings?
- To what extent would you be interested in a Smart Meter that would transfer only the current total power consumption in Watts, but not the consumption values of individual appliances, to the utility providers and possibly other parties, such as the Consumer Association? (You yourself can access all consumption data, including the consumption of individual appliances. Note that this would mean that you would not receive any hints or tips to save electricity.)

A.6 Security

- You can save money with Smart Metering but criminals could interrupt or access the data transmission to the utility providers, e.g., to manipulate consumption information. How would you assess this risk?
- Imagine that a Smart Meter comes with a seal of approval or certificate by a federal office (for example, the Federal Office for Security in Information Technology). To what extent would this alleviate your concerns, if any?

A.7 Acceptance

- What qualities of Smart Meters are the most important to you? What role does usability play?
- What would be the most important benefits you would expect from a Smart Meter? What else should a Smart Meter be able to achieve for you?
- How do you rate additional functions such as generating an alarm when the stove is left on or receiving personalized advertising when the Smart Meter notices relevant power consumption patterns (e.g., the refrigerator consuming too much power)?

A.8 Deployment

As a consumer, you may have to pay an annual fee for a Smart Meter.

- Who do you think should bear the cost?
- What is the financial responsibility of the household given the potential electricity savings?
- What do you think is essential for the successful adoption of Smart Meters?

A.9 Contact Information

Unless you win the raffle or want to be kept informed about the project, you will not receive any more mail from us.

- Would you like us to update you on the project?
  - Yes
  - No
- If you would like to participate in the raffle, we need the following information:
  - Last name:
  - First name:
  - Street and house number:
  - Postcode and town or city:
- If you win, which of the following prizes would you like to receive?
  20-Euro Gift Certificate from:
  - Amazon
  - City Gallery mall
  - DM store

  (Note that only complete questionnaires with valid and complete address information will be included in the raffle.)

Thank you for your time and effort!

REFERENCES

[1] Gregory D. Abowd and Elizabeth D. Mynatt. 2000. Charting Past, Present, and Future Research in Ubiquitous Computing. *ACM Trans. Comput.-Hum. Interact.* 7, 1 (March 2000), 29–58. https://doi.org/10.1145/344949.344988

[2] Chadia Abras, Diane Maloney-Krichmar, and Jenny Preece. 2004. User-centered design. In *Encyclopedia of Human-Computer Interaction*, William Bainbridge (Ed.). Vol. 37. Thousand Oaks: Sage Publications, 445–456.

[3] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce (EC ‘99)*. ACM, New York, NY, USA, 1–8. https://doi.org/10.1145/336992.336995

[4] Alessandro Acquisti. 2010. The Economics of Personal Data and the Economics of Privacy. https://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf.

[5] Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (January 2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[6] Christian Aichele and Oliver D. Doleski (Eds.). 2013. *Smart Meter Rollout: Praxisleitfaden zur Ausbringung intelligenter Zähler*. Springer Vieweg, Wiesbaden. https://doi.org/10.1007/978-3-8348-2440-0

[7] Irwin Altman. 1977. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues* 33, 3 (1977), 66–84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

[8] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The Internet of Things: A survey. *Computer Networks* 54, 15 (2010), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

[9] Naveen Farag Awad and M. S. Krishnan. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Q.* 30, 1 (March 2006), 13–28. https://doi.org/10.2307/25148715

[10] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. “Little Brothers Watching You”: Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS ‘13)*. ACM, New York, NY, USA, Article 12, 11 pages. https://doi.org/10.1145/2501604.2501616

[11] Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ‘12)*. ACM, New York, NY, USA, 367–376. https://doi.org/10.1145/2207676.2207727

[12] Victoria Bellotti and Abigail Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work (ECSCW ‘93)*, Giorgio de Michelis, Carla Simone, and Kjeld Schmidt (Eds.). Springer Netherlands, Dordrecht, 77–92. https://doi.org/10.1007/978-94-011-2094-4$_6$

[13] Kirsten Boehner, Janet Vertesi, Phoebe Sengers, and Paul Dourish. 2007. How HCI Interprets the Probes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ‘07)*. ACM, New York, NY, USA, 1077–1086. https://doi.org/10.1145/1240624.1240789

[14] Laura Brandimarte and Alessandro Acquisti. 2012. The Economics of Privacy. In *The Oxford Handbook of the Digital Economy*, Martin Peitz and Joel Waldfogel (Eds.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195397840.013.0020

[15] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[16] Carolyn Brodie, Clare-Marie Karat, John Karat, and Jinjuan Feng. 2005. Usable Security and Privacy: A Case Study of Developing Privacy Management Tools. In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS ‘05)*. ACM, New York, NY, USA, 35–43. https://doi.org/10.1145/1073001.1073005

[17] Erik Buchmann, Klemens Böhm, Thorben Burghardt, and Stephan Kessler. 2013. Re-identification of Smart Meter Data. *Personal Ubiquitous Comput.* 17, 4 (April 2013), 653–662. https://doi.org/10.1007/s00779-012-0513-6

[18] Kelly Caine and Rima Hanania. 2013. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association* 20, 1 (2013), 7–15. https://doi.org/10.1136/amiajnl-2012-001023

[19] Ann Cavoukian. 2012. Operationalizing privacy by design: A guide to implementing strong privacy practices. http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf. *Information and Privacy Commissioner of Ontario, Canada* (2012).

[20] Ann Cavoukian and Alexander Dix. 2012. Smart meters in Europe: Privacy by Design at its best. *Information and Privacy Commissioner of Ontario, Canada* (2012).

[21] Amir Chaudhry, Jon Crowcroft, Heidi Howard, Anil Madhavapeddy, Richard Mortier, Hamed Haddadi, and Derek McAuley. 2015. Personal Data: Thinking Inside the Box. In *Proceedings of the Fifth Decennial Aarhus Conference on Critical Alternatives (CA ‘15)*. Aarhus University Press, 29–32. https://doi.org/10.7146/aahcc.v1i1.21312

[22] Sherry Y. Chen, Jing-Ping Fan, and Robert D. Macredie. 2006. Navigation in hypermedia learning systems: Experts vs. novices. *Computers in Human Behavior* 22, 2 (2006), 251–266. https://doi.org/10.1016/j.chb.2004.06.004

[23] Roger Clarke. 2009. Privacy impact assessment: Its origins and development. *Computer Law & Security Review* 25, 2 (2009), 123–135. https://doi.org/10.1016/j.clsr.2009.02.002

[24] Cédric Clastres. 2011. Smart grids: Another step towards competition, energy security and climate change objectives. *Energy Policy* 39, 9 (2011), 5399–5408. https://doi.org/10.1016/j.enpol.2011.05.024

[25] Imelda T. Coyne. 2008. Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing* 26, 3 (2008), 623–630. https://doi.org/10.1046/j.1365-2648.1997.t01-25-00999.x

[26] Andy Crabtree. 2004. Design in the Absence of Practice: Breaching Experiments. In *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS '04).* ACM, New York, NY, USA, 59–68. https://doi.org/10.1145/1013115.1013125

[27] Andy Crabtree and Richard Mortier. 2015. Human Data Interaction: Historical Lessons from Social Studies and CSCW. In *Proceedings of the 14th European Conference on Computer Supported Cooperative Work (ECSCW '15)*, Nina Boulus-Rødje, Gunnar Ellingsen, Tone Bratteteig, Margunn Aanestad, and Pernille Bjørn (Eds.). Springer, Cham, 3–21. https://doi.org/10.1007/978-3-319-20499-4_1

[28] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work (CSCW)* 26, 4 (01 December 2017), 453–488. https://doi.org/10.1007/s10606-017-9276-y

[29] Lorrie Cranor and Simson Garfinkel. 2005. *Security and Usability.* O'Reilly Media, Inc.

[30] Colette Cuijpers and Bert-Jaap Koops. 2013. *Smart Metering and Privacy in Europe: Lessons from the Dutch Case.* Springer Netherlands, Dordrecht, 269–293. https://doi.org/10.1007/978-94-007-5170-$5_1$2

[31] George Danezis and Seda Gürses. 2010. A critical review of 10 years of Privacy Technology. https://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf. , 16 pages.

[32] Tamara Dinev and Paul Hart. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research* 17, 1 (2006), 61–80. https://doi.org/10.1287/isre.1060.0080

[33] Alan Dix. 2007. Designing for Appropriation. In *Proceedings of the 21st British HCI Group Annual Conference on People and Computers (BCS-HCI '07)*, Vol. 2. BCS Learning & Development Ltd., Swindon, UK, 27–30.

[34] Susen Döbelt, Markus Jung, Marc Busch, and Manfred Tscheligi. 2015. Consumers' privacy concerns and implications for a privacy preserving Smart Grid architecture – Results of an Austrian study. *Energy Research & Social Science: Special Issue on Smart Grids and the Social Sciences* 9 (2015), 137–145. https://doi.org/10.1016/j.erss.2015.08.022

[35] Catherine Dwyer, Starr Roxanne Hiltz, and Katia Passerini. 2007. Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. http://aisel.aisnet.org/amcis2007/339. In *Proceedings of the Americas Conference on Information Systems (AMCIS 2007).*

[36] Costas Efthymiou and Georgios Kalogridis. 2010. Smart Grid Privacy via Anonymization of Smart Metering Data. In *Proceedings of the First IEEE International Conference on Smart Grid Communications.* 238–243. https://doi.org/10.1109/SMARTGRID.2010.5622050

[37] Zekeriya Erkin and Gene Tsudik. 2012. Private Computation of Spatial and Temporal Power Consumption with Smart Meters. In *Applied Cryptography and Network Security*, Feng Bao, Pierangela Samarati, and Jianying Zhou (Eds.). Springer, Berlin, Heidelberg, 561–577. https://doi.org/10.1007/978-3-642-31284-$7_3$3

[38] European Commission. 1995. Country fiches for electricity smart metering Accompanying the document Report from the Commission Benchmarking smart metering deployment in the EU-27 with a focus on electricity. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014SC0188.

[39] European Parliament and Council of the European Union. 1995. 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. http://data.europa.eu/eli/dir/1995/46/oj.

[40] European Parliament and Council of the European Union. 2009. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance). http://data.europa.eu/eli/dir/2009/136/oj.

[41] European Parliament and Council of the European Union. 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) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[42] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. 2012. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys Tutorials* 14, 4 (April 2012), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087

[43] Joel E. Fischer, Andy Crabtree, Tom Rodden, James A. Colley, Enrico Costanza, Michael O. Jewell, and Sarvapali D. Ramchurn. 2016. "Just Whack It on Until It Gets Hot": Working with IoT Data in the Home. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16).* ACM, New York, NY, USA, 5933–5944.

https://doi.org/10.1145/2858036.2858518

[44] Joel E. Fischer, Sarvapali D. Ramchurn, Michael Osborne, Oliver Parson, Trung Dong Huynh, Muddasser Alam, Nadia Pantidi, Stuart Moran, Khaled Bachour, Steve Reece, Enrico Costanza, Tom Rodden, and Nicholas R. Jennings. 2013. Recommending Energy Tariffs and Load Shifting Based on Smart Household Usage Profiling. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces (IUI '13)*. ACM, New York, NY, USA, 383–394. https://doi.org/10.1145/2449396.2449446

[45] Tony Flick and Justin Morehouse. 2010. *Securing the Smart Grid: Next Generation Power Grid Security.* Syngress Publishing.

[46] Luciano Floridi. 2005. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology* 7, 4 (01 December 2005), 185–200. https://doi.org/10.1007/s10676-006-0001-7

[47] Joshua Fogel and Elham Nehmad. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior* 25, 1 (2009), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

[48] Jon Froehlich, Leah Findlater, and James Landay. 2010. The Design of Eco-feedback Technology. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1999–2008. https://doi.org/10.1145/1753326.1753629

[49] Vaibhav Garg, Sameer Patil, Apu Kapadia, and L. Jean Camp. 2013. Peer-produced privacy protection. In *2013 IEEE International Symposium on Technology and Society: Social Implications of Wearable Computing and Augmediated Reality in Everyday Life (ISTAS '13)*. 147–154. https://doi.org/10.1109/ISTAS.2013.6613114

[50] Carrie Gates and Peter Matthews. 2014. Data Is the New Currency. In *Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14)*. ACM, New York, NY, USA, 105–116. https://doi.org/10.1145/2683467.2683477

[51] William Gaver. 2012. What Should We Expect from Research Through Design?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 937–946. https://doi.org/10.1145/2207676.2208538

[52] Clark W. Gellings. 2009. *The Smart Grid: Enabling energy efficiency and demand response.* The Fairmont Press, Inc..

[53] Paul Gerber, Melanie Volkamer, and Karen Renaud. 2015. Usability Versus Privacy Instead of Usable Privacy: Google's Balancing Act Between Usability and Privacy. *SIGCAS Comput. Soc.* 45, 1 (Feb. 2015), 16–21. https://doi.org/10.1145/2738210.2738214

[54] German Federal Constitutional Court. 1983. BundesVerfassungsGericht 61,1 – Volkszählung. http://www.servat.unibe.ch/dfr/bv065001.html.

[55] Gerd Gigerenzer and Daniel G. Goldstein. 1996. Reasoning the fast and frugal way: Models of bounded rationality. *Psychological Review* 103, 4 (1996), 650–669. https://doi.org/10.1037/0033-295X.103.4.650

[56] Barney G Glaser. 1998. *Doing grounded theory: Issues and discussions.* Sociology Press.

[57] Sanjay Goel, Yuan Hong, Vagelis Papakonstantinou, and Dariusz Kloza. 2015. *Smart Grid Security.* Springer, London, UK. https://doi.org/10.1007/978-1-4471-6663-4

[58] Nancy C. Goodwin. 1987. Functionality and Usability. *Commun. ACM* 30, 3 (March 1987), 229–233. https://doi.org/10.1145/214748.214758

[59] Ulrich Greveler. 2016. Die Smart-Metering-Debatte 2010–2016 und ihre Ergebnisse zum Schutz der Privatsphäre. *Datenbank-Spektrum* 16, 2 (01 July 2016), 137–145. https://doi.org/10.1007/s13222-016-0219-4

[60] Rebecca E. Grinter, W. Keith Edwards, Marshini Chetty, Erika S. Poole, Ja-Young Sung, Jeonghwa Yang, Andy Crabtree, Peter Tolmie, Tom Rodden, Chris Greenhalgh, and Steve Benford. 2009. The Ins and Outs of Home Networking: The Case for Useful and Usable Domestic Networking. *ACM Trans. Comput.-Hum. Interact.* 16, 2, Article 8 (June 2009), 28 pages. https://doi.org/10.1145/1534903.1534905

[61] Rebecca E. Grinter, W. Keith Edwards, Mark W. Newman, and Nicolas Ducheneaut. 2005. The Work to Make a Home Network Work. In *Proceedings of the European Confernce on Computer Supported Cooperative Work (ECSCW '05)*, Hans Gellersen, Kjeld Schmidt, Michel Beaudouin-Lafon, and Wendy Mackay (Eds.). Springer Netherlands, Dordrecht, 469–488. https://doi.org/10.1007/1-4020-4023-$7_2$4

[62] Ralph Gross and Alessandro Acquisti. 2005. Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)*. ACM, New York, NY, USA, 71–80. https://doi.org/10.1145/1102199.1102214

[63] Greg S. Guthridge. 2010. Understanding consumer preferences in energy efficiency: Accenture end-consumer observatory on electricity management. *Accenture, Dublin, Ireland, Technical Report* ACC10-0229 (2010).

[64] Richard Harper, Dave Randall, and Wes Sharrock. 2017. *Choice.* John Wiley & Sons.

[65] Richard H. R. Harper. 2014. *Trust, Computing, and Society* (1st ed.). Cambridge University Press, New York, NY, USA.

[66] George W. Hart. 1992. Nonintrusive appliance load monitoring. *Proc. IEEE* 80, 12 (Dec 1992), 1870–1891. https://doi.org/10.1109/5.192069

[67] Tanzima Hashem and Lars Kulik. 2011. "Don't trust anyone": Privacy protection for location-based services. *Pervasive and Mobile Computing* 7, 1 (2011), 44–59. https://doi.org/10.1016/j.pmcj.2010.04.006

[68] Gillian R. Hayes. 2011. The Relationship of Action Research to Human-Computer Interaction. *ACM Trans. Comput.-Hum. Interact.* 18, 3, Article 15 (Aug. 2011), 20 pages. https://doi.org/10.1145/1993060.1993065

[69] Kenneth Einar Himma and Herman T. Tavani. 2008. *The handbook of information and computer ethics.* John Wiley & Sons, Hoboken, NJ, USA. xxxi, 671 p. pages.

[70] Alexander Hoerbst, Christian Dominik Kohl, Petra Knaup, and Elske Ammenwerth. 2010. Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens. *International Journal of Medical Informatics* 79, 2 (2010), 81–89. https://doi.org/10.1016/j.ijmedinf.2009.11.002

[71] Jason I. Hong, Jennifer D. Ng, Scott Lederer, and James A. Landay. 2004. Privacy Risk Models for Designing Privacy-sensitive Ubiquitous Computing Systems. In *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS '04).* ACM, New York, NY, USA, 91–100. https://doi.org/10.1145/1013115.1013129

[72] Giovanni Iachello and Jason Hong. 2007. End-user Privacy in Human-computer Interaction. *Found. Trends Hum.-Comput. Interact.* 1, 1 (Jan. 2007), 1–137. https://doi.org/10.1561/1100000004

[73] Deborah G. Johnson. 2009. *Computer Ethics* (4th ed.). Prentice Hall Press, Upper Saddle River, NJ, USA.

[74] Harvey Jones and José Hiram Soltren. 2005. Facebook: Threats to Privacy. https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf. *Project MAC: MIT Project on Mathematics and Computing* 1 (December 2005), 1–76.

[75] Erik Joukes, Ronald Cornet, Martine C. de Bruijne, and Nicolette F. de Keizer. 2016. Eliciting end-user expectations to guide the implementation process of a new electronic health record: A case study using concept mapping. *International Journal of Medical Informatics* 87 (2016), 111–117. https://doi.org/10.1016/j.ijmedinf.2015.12.014

[76] Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, Tim A. Lewis, and Rafael Cepeda. 2010. Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures. In *2010 First IEEE International Conference on Smart Grid Communications.* 232–237. https://doi.org/10.1109/SMARTGRID.2010.5622047

[77] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. https://www.usenix.org/conference/soups2015/proceedings/presentation/kang. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15).* USENIX Association, 39–52.

[78] Willett Kempton and Laura Montgomery. 1982. Folk quantification of energy. *Energy* 7, 10 (1982), 817–827. https://doi.org/10.1016/0360-5442(82)90030-5

[79] Bart P. Knijnenburg. 2013. Simplifying Privacy Decisions: Towards Interactive and Adaptive Solutions. http://ceur-ws.org/Vol-1050/Decisions2013Proceedings.pdf#page=44. In *Proceedings of Decisions@RecSys.* 40–41.

[80] Rainer Knyrim and Gerald Trieb. 2011. Smart Metering under EU data protection law. *International Data Privacy Law* 1, 2 (2011), 121–128. https://doi.org/10.1093/idpl/ipr004

[81] Alfred Kobsa and Maximilian Teltzrow. 2005. Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. In *Privacy Enhancing Technologies*, David Martin and Andrei Serjantov (Eds.). Springer, Berlin, Heidelberg, 329–343. https://doi.org/10.1007/11423409$_{2}$1

[82] Johann Kranz, Julia Gallenkamp, and Arnold Picot. 2010. Exploring the Role of Control – Smart Meter Acceptance of Residential Consumers. https://aisel.aisnet.org/amcis2010/315. In *Proceedings of the Americas Conference on Information Systems (AMCIS 2010).*

[83] Tamar Krishnamurti, Daniel Schwartz, Alexander Davis, Baruch Fischhoff, Wändi Bruine de Bruin, Lester Lave, and Jack Wang. 2012. Preparing for smart grid technologies: A behavioral decision research approach to understanding consumer expectations about smart meters. *Energy Policy* 41 (2012), 790–797. https://doi.org/10.1016/j.enpol.2011.11.047 Modeling Transport (Energy) Demand and Policies.

[84] Saadi Lahlou, Marc Langheinrich, and Carsten Röcker. 2005. Privacy and Trust Issues with Invisible Computers. *Commun. ACM* 48, 3 (March 2005), 59–60. https://doi.org/10.1145/1047671.1047705

[85] Marc Langheinrich. 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*, Gregory D. Abowd, Barry Brumitt, and Steven Shafer (Eds.). Springer, Berlin, Heidelberg, 273–291. https://doi.org/10.1007/3-540-45427-6$_{2}$3

[86] Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. 2004. Personal Privacy Through Understanding and Action: Five Pitfalls for Designers. *Personal Ubiquitous Comput.* 8, 6 (Nov. 2004), 440–454. https://doi.org/10.1007/s00779-004-0304-9

[87] Jack I. Lerner and Deirdre K. Mulligan. 2008. Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home. *Stanford Technology Law Review (STLR)* 3 (2008).

[88] Yaping Li, Minghua Chen, Qiwei Li, and Wei Zhang. 2012. Enabling Multilevel Trust in Privacy Preserving Data Mining. *IEEE Transactions on Knowledge and Data Engineering* 24, 9 (September 2012), 1598–1612. https://doi.org/10.1109/TKDE.2011.124

[89] Ilaria Liccardi, Joseph Pato, Daniel J. Weitzner, Hal Abelson, and David De Roure. 2014. No Technical Understanding Required: Helping Users Make Informed Choices About Access to Their Personal Data. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS '14)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, Belgium, 140–150. https://doi.org/10.4108/icst.mobiquitous.2014.258066

[90] Huang Lin and Yuguang Fang. 2013. Privacy-Aware Profiling and Statistical Data Extraction for Smart Sustainable Energy Systems. *IEEE Transactions on Smart Grid* 4, 1 (March 2013), 332–340. https://doi.org/10.1109/TSG.2012.2210289

[91] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 501–510. https://doi.org/10.1145/2370216.2370290

[92] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (SOUPS '16)*. USENIX Association, 27–41.

[93] Michael Lynch and Wes Sharrock. 2011. *Ethnomethodology: Volume I*. SAGE Publications Ltd.

[94] Derek McAuley, Richard Mortier, and James Goulding. 2011. The Dataware Manifesto. In *Proceedings of the Third International Conference on Communication Systems and Networks (COMSNETS '11)*. 1–6. https://doi.org/10.1109/COMSNETS.2011.5716491

[95] Patrick McDaniel and Stephen McLaughlin. 2009. Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy* 7 (05 2009), 75–77. https://doi.org/10.1109/MSP.2009.76

[96] Eoghan McKenna, Ian Richardson, and Murray Thomson. 2012. Smart meter data: Balancing consumer privacy concerns with legitimate applications. *Energy Policy* 41 (2012), 807–814. https://doi.org/10.1016/j.enpol.2011.11.049 Modeling Transport (Energy) Demand and Policies.

[97] Carlo Maria Medaglia and Alexandru Serbanati. 2010. An Overview of Privacy and Security Issues in the Internet of Things. In *The Internet of Things*, Daniel Giusto, Antonio Iera, Giacomo Morabito, and Luigi Atzori (Eds.). Springer, New York, NY, USA, 389–395. https://doi.org/10.1007/978-1-4419-1674-7$_3$8

[98] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. 2012. Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks* 10, 7 (2012), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

[99] James H. Moor. 1997. Towards a Theory of Privacy in the Information Age. *SIGCAS Comput. Soc.* 27, 3 (Sept. 1997), 27–32. https://doi.org/10.1145/270858.270866

[100] United Nations. 1948. Universal Declaration of Human Rights. http://www.un.org/en/universal-declaration-human-rights.

[101] Ingo Naumann and Giles Hogben. 2008. Privacy features of European eID card specifications. *Network Security* 2008, 8 (2008), 9–13. https://doi.org/10.1016/S1353-4858(08)70097-7

[102] Bernard Neenan and Ross C. Hemphill. 2008. Societal Benefits of Smart Metering Investments. *The Electricity Journal* 21, 8 (2008), 32–45. https://doi.org/10.1016/j.tej.2008.09.003

[103] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washingto Law Review* 79, 119 (2004), 101–139.

[104] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[105] The Privacy Act of 1974. 1974. 5. *United States Code §552a* (1974).

[106] Members of the Common Criteria Recognition Arrangement. 2017. Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5. https://www.commoncriteriaportal.org/cc/.

[107] Pacific Gas & Electric. 2018. Find out how SmartMeter^{TM} communicates with PG&E. https://www.pge.com/en$_{US}$/residential/save-energy-money/analyze-your-usage/your-usage/view-and-share-your-data-with-smartmeter/smartmeter-network.page.

[108] Leysia Palen and Paul Dourish. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. ACM, New York, NY, USA, 129–136. https://doi.org/10.1145/642611.642635

[109] F. Pallas. 2012. Data Protection and smart grid communication – The European perspective. In *Proceedings of ISGT 2012: IEEE PES Innovative Smart Grid Technologies*. 1–8. https://doi.org/10.1109/ISGT.2012.6175695

[110] Vagelis Papakonstantinou and Dariusz Kloza. 2015. *Legal Protection of Personal Data in Smart Grid and Smart Metering Systems from the European Perspective*. Springer London, London, UK, 41–129. https://doi.org/10.1007/978-1-4471-6663-4$_2$

[111] Andreas Pfitzmann. 2006. Multilateral Security: Enabling Technologies and Their Evaluation. In *Emerging Trends in Information and Communication Security*, Günter Müller (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–13. https://doi.org/10.1007/11766155$_1$

[112] Stefanie Pötzsch. 2009. Privacy Awareness: A Means to Solve the Privacy Paradox?. In *The Future of Identity in the Information Society*, Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrček, and Petr Švenda (Eds.). Springer, Berlin, Heidelberg, 226–236. https://doi.org/10.1007/978-3-642-03315-5$_1$7

[113] Emilee Rader and Janine Slaker. 2017. The importance of visibility for folk theories of sensor data. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/rader. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, 257–270.

[114] Edith Ramirez, Julie Brill, Maureen K. Ohlhausen, Joshua D. Wright, and Terrell McSweeny. 2014. Data brokers: A call for transparency and accountability. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. *Federal Trade Commission* (May 2014).

[115] David Randall and Mark Rouncefield. 2007. *Fieldwork for Design: Theory and Practice* (1 ed.). Springer-Verlag, London, UK. https://doi.org/10.1007/978-1-84628-768-8

[116] Ashwini Rao, Florian Schaub, and Norman M. Sadeh. 2015. What do they know about me? Contents and Concerns of Online Behavioral Profiles. http://arxiv.org/abs/1506.01675. *Computer Research Repository (CoRR)* abs/1506.01675, arXiv:1506.01675 (2015). arXiv:1506.01675

[117] Andreas Reckwitz. 2002. Toward a Theory of Social Practices: A Development in Culturalist Theorizing. *European Journal of Social Theory* 5, 2 (2002), 243–263. https://doi.org/10.1177/13684310222225432

[118] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, and Florian Schaub. 2015. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. *Berkeley Technology Law Journal* 30, 1 (2015), 39–88.

[119] Tom A. Rodden, Joel E. Fischer, Nadia Pantidi, Khaled Bachour, and Stuart Moran. 2013. At Home with Agents: Exploring Attitudes Towards Future Smart Energy Infrastructures. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 1173–1182. https://doi.org/10.1145/2470654.2466152

[120] Rodrigo Roman, Jianying Zhou, and Javier Lopez. 2013. On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks: Special Issue on Security and Identity Architecture for the Future Internet* 57, 10 (2013), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

[121] Benedikt Römer, Philipp Reichhart, Johann Kranz, and Arnold Picot. 2012. The role of Smart Metering and decentralized electricity storage for Smart Grids: The importance of positive externalities. *Energy Policy: Special Section: Past and Prospective Energy Transitions – Insights from History* 50 (2012), 486–495. https://doi.org/10.1016/j.enpol.2012.07.047

[122] Cristina Rottondi, Giacomo Verticale, and Antonio Capone. 2013. Privacy-preserving smart metering with multiple data Consumers. *Computer Networks* 57, 7 (2013), 1699–1713. https://doi.org/10.1016/j.comnet.2013.02.018

[123] Ira S. Rubinstein. 2011. Regulating Privacy by Design. *Berkeley Technology Law Journal* 26, 3 (May' 2011), 1409–1456.

[124] Lalitha Sankar, S. Raj Rajagopalan, Soheil Mohajer, and H. Vincent Poor. 2013. Smart Meter Privacy: A Theoretical Framework. *IEEE Transactions on Smart Grid* 4, 2 (June 2013), 837–846. https://doi.org/10.1109/TSG.2012.2211046

[125] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub. In *Procceding of the Eleventh Symposium On Usable Privacy and Security (SOUPS '15)*. USENIX Association, 1–17.

[126] Daniela Schiek. 2014. The Written Interview in Qualitative Social Research. *Zeitschrift für Soziologie* 43, 5 (2014), 379–395.

[127] Ari Schwartz. 2009. Looking Back at P3P: Lessons for the Future. https://www.cdt.org/files/pdfs/P3P$_{\text{R}}$etro$_{\text{F}}$inal$_0$.pdf.

[128] Tobias Schwartz, Gunnar Stevens, Leonardo Ramirez, and Volker Wulf. 2013. Uncovering Practices of Making Energy Consumption Accountable: A Phenomenological Inquiry. *ACM Trans. Comput.-Hum. Interact.* 20, 2, Article 12 (May 2013), 30 pages. https://doi.org/10.1145/2463579.2463583

[129] Katie Shilton. 2009. Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection. *Commun. ACM* 52, 11 (Nov. 2009), 48–53. https://doi.org/10.1145/1592761.1592778

[130] Herbert Alexander Simon. 1997. *Models of bounded rationality: Empirically grounded economic reason.* Vol. 3.

[131] Daniel J. Solove. 2010. *Understanding Privacy.* Harvard University Press.

[132] Gunnar Stevens, Timo Jakobi, and Kai-Oliver Detken. 2014. Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme. *Datenschutz und Datensicherheit – DuD* 38, 8 (01 August 2014), 536–544. https://doi.org/10.1007/s11623-014-0180-z

[133] Gunnar Stevens, Volkmar Pipek, and Volker Wulf. 2009. Appropriation Infrastructure: Supporting the Design of Usages. In *End-User Development*, Volkmar Pipek, Mary Beth Rosson, Boris de Ruyter, and Volker Wulf (Eds.). Springer,

Berlin, Heidelberg, 50–69. https://doi.org/10.1007/978-3-642-00427-8$_4$

[134] Hamed Taherdoost, Mazdak Zamani, and Meysam Namayandeh. 2009. Study of smart card technology and probe user awareness about it: A case study of Middle Eastern students. In *Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology*. 334–338. https://doi.org/10.1109/ICCSIT.2009.5234410

[135] William Isaac Thomas and Dorothy Swaine Thomas. 1928. The methodology of behavior study. *The child in America: Behavior problems and programs* (1928), 553–576.

[136] Peter Tolmie, Andy Crabtree, Tom Rodden, James Colley, and Ewa Luger. 2016. "This Has to Be the Cats": Personal Data Legibility in Networked Sensing Systems. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM, New York, NY, USA, 491–502. https://doi.org/10.1145/2818048.2819992

[137] Shuang Wang, Lijuan Cui, Jianlan Que, Dae-Hyun Choi, Xiaoqian Jiang, Samuel Cheng, and Le Xie. 2012. A Randomized Response Model for Privacy Preserving Smart Metering. *IEEE Transactions on Smart Grid* 3, 3 (Sept 2012), 1317–1324. https://doi.org/10.1109/TSG.2012.2192487

[138] Willis H. Ware. 1973. Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems'. https://www.rand.org/pubs/papers/P5077.html. *US Department of Health, Education & Welfare* (1973).

[139] Samuel D. Warren and Louis D. Brandeis. 1890. The Right to Privacy. http://www.jstor.org/stable/1321160. *Harvard Law Review* 4, 5 (1890), 193–220.

[140] Rolf H. Weber. 2010. Internet of Things – New security and privacy challenges. *Computer Law & Security Review* 26, 1 (2010), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

[141] Mark Weiser. 1991. The Computer for the 21st Century. *Scientific American: Special Issue on Communications, Computers, and Networks* 265, 3 (September 1991), 94–104.

[142] Alan F. Westin. 1970. *Privacy and Freedom.* Bodley Head.

[143] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. http://www.usenix.org/events/sec99/full$_p$apers/whitten/whitten$_h$tml/index.html. In *Proceedings of the 8th USENIX Security Symposium*, Vol. 348. USENIX Association, 169–184.

[144] David Wright. 2011. A framework for the ethical impact assessment of information technology. *Ethics and Information Technology* 13, 3 (01 September 2011), 199–226. https://doi.org/10.1007/s10676-010-9242-6

[145] Volker Wulf, Markus Rohde, Volkmar Pipek, and Gunnar Stevens. 2011. Engaging with Practices: Design Case Studies As a Research Framework in CSCW. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work (CSCW '11)*. ACM, New York, NY, USA, 505–512. https://doi.org/10.1145/1958824.1958902

[146] Phillipp Wunderlich, Daniel Veit, and Saonee Sarker. 2012. Adoption of Information Systems in the Electricity Sector: The Issue of Smart Metering. https://aisel.aisnet.org/amcis2012/proceedings/AdoptionDiffusionIT/16. In *Proceedings of the Americas Conference on Information Systems (AMCIS 2012)*.

[147] Shan Zhou and Marilyn A. Brown. 2017. Smart meter deployment in Europe: A comparative case study on the impacts of national policy schemes. *Journal of Cleaner Production* 144 (2017), 22–32. https://doi.org/10.1016/j.jclepro.2016.12.031

[148] Mary Ellen Zurko. 2005. User-centered security: Stepping up to the grand challenge. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005)*. 14 pp.–202. https://doi.org/10.1109/CSAC.2005.60

Received August 2017; revised May 2018; accepted September 2018