Incorporating Usable Privacy into Connected Devices: A User-Centered Perspective

Dissertation von

Timo Jakobi

Zur Erlangung des Doktorgrades

Dr. rer. pol.

an der

Fakultät III: Wirtschaftswissenschaften,

Wirtschaftsinformatik und Wirtschaftsrecht

der Universität Siegen

Jahr der Fertigstellung: 2019

Erster Gutachter: Prof. Dr. Gunnar Stevens

Zweiter Gutachter: Prof. Dr. Volker Wulf

Abstract

Due to the popularity of the Internet and the networked services that it facilitates, networked devices have become increasingly common in both the workplace and everyday life in recent years—following the trail blazed by smartphones. The data provided by these devices allow for the creation of rich user profiles. As a result, the collection, processing and exchange of such personal data have become drivers of economic growth.

History shows that the adoption of new technologies is likely to influence both individual and societal concepts of privacy. Research into privacy has therefore been confronted with continuously changing concepts due to technological progress. From a legal perspective, privacy laws that reflect social values are sought. Privacy enhancing technologies are developed or adapted to take account of technological development. Organizations must also identify protective measures that are effective in terms of scalability and automation. Similarly, research is being conducted from the perspective of Human-Computer Interaction (HCI) to explore design spaces that empower individuals to manage their protection needs with regard to novel data, which they may perceive as sensitive.

Taking such an HCI perspective with regard to understanding privacy management on the Internet of Things (IoT), this research mainly focuses on three interrelated goals across the fields of application:

1. Exploring and analyzing how people make sense of data, especially when managing privacy and data disclosure;
2. Identifying, framing and evaluating potential resources for designing sense-making processes; and
3. Exploring the fitness of the identified concepts for inclusion in legal and technical perspectives on supporting decisions regarding privacy on the IoT.

Although this work's point of departure is the HCI perspective, it emphasizes the importance of the interrelationships among seemingly independent perspectives. Their interdependence is therefore also emphasized and taken into account by subscribing to a user-centered design process throughout this study.

More specifically, this thesis adopts a design case study approach. This approach makes it possible to conduct full user-centered design lifecycles in a concrete application case with participants in the context of everyday life. Based on this approach, it was possible to investigate several domains of the IoT that are currently relevant, namely smart metering, smartphones, smart homes and connected cars.

The results show that the participants were less concerned about (raw) data than about the information that could potentially be derived from it. Against the background of the constant collection of highly technical and abstract data, the content of which only becomes visible through the application of complex algorithms, this study indicates that people should learn to explore and understand these data flexibly, and provides insights in how to design for supporting this aim. From the point of view of design for usable privacy protection measures, the information that is provided to users about data disclosure should be focused on the consequences thereof for users' environments and life. A related concept from law is "informed consent," which I propose should be further developed in order to implement usable mechanisms for individual privacy protection in the era of the IoT. Finally, this thesis demonstrates how research on HCI can be methodologically embedded in a regulative process that will inform both the development of technology and the drafting of legislation.

Acknowledgements

I am deeply grateful to my thesis advisor, Gunnar Stevens, for guiding my research activities at the intersection between consumer informatics and usable privacy and for encouraging and supporting me in finding my way. His advice, creativity and analytical sense were, and remain, an inspiration, and he not only provided valuable input concerning my thesis but also provided me with guidance concerning my growth as a researcher and person.

I also wish to thank Volker Wulf for giving me the opportunity to work in such a positive environment and making me feel supported in everything that I did.

Special thanks also go to Dave Randall, who has often whom I often engaged in discussion and who provided feedback on research proposals and papers throughout the last few years. It was a pleasure engaging and co-authoring with such a well-versed and sympathetic scientist.

In addition, I would like to thank my many colleagues, most importantly Nico Castelli, Martin Stein and Corinna Ogonowski, but also all of those associated with the larger WiNeMe group, for the motivation, inspiration, cooperation, fun, tech support, countless discussions, team outings and productive lunch breaks. It has been a great ride.

I also wish to thank all of the participants in my studies for welcoming me into their homes and allowing me to make pictures and observations. Thank you to all of you for your time, effort and patience.

Last, but definitely not least, I would like to express my deep gratitude towards my family, namely Anja, Janne, Ute, Alfred and Tom who always pushed and supported me in my work and life.

Related Publications

Some of the research presented in this work has been previously published, presented and/or discussed with scientists in the field of human-computer interaction and usable privacy research, more specifically. The following list provides an overview of the material that was previously published as articles and the respective chapters in which they were used:

Chapter 4: Stevens, G., Jakobi, T., & Detken, K. O. (2014). Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme. *Datenschutz und Datensicherheit-DuD*, *38*(8), 536-544.

Chapter 5: Jakobi, T., Stevens, G. and Seufert, A.-M. 2018. Privacy-By-Design für das Connected Car: Architekturen aus Verbrauchersicht. *Datenschutz und Datensicherheit-DuD*. 42, 11 (2018), 704–707.

Chapter 6: Stevens, G., Bossauer, P., Jakobi, T. and Pakusch, C. 2017. Second Dashboard: Information Demands in a Connected Car. Mensch und Computer 2017-Tagungsband. (2017).

Chapter 7: Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G. and Wulf, V. 2017. The Catch (es) with Smart Home: Experiences of a Living Lab Field Study. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (2017), 1620–1633.

Chapter 8: Jakobi, T., Stevens, G., Castelli, N., Ogonowski, C., Schaub, F., Vindice, N., … Wulf, V. (2018). Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *2*(4), 28.

Chapter 9: Jakobi, T., Kropp, E., Stevens, G., Schmal, M. 2017. Providing smartphone data visualizations to support Privacy Literacy; Work in Progress Presentation at EuroUsec 2017, Paris.

Chapter 10: Jakobi, T., Patil, S., Randall, D., Stevens, G. and Wulf, V. 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 (2018), 43.

Other Publications

In addition to those presented above, there are other publications that inspired the research conducted for this thesis and thus contributed to the insights presented in it; as such, these studies should also be mentioned. While they are not fully presented in this thesis, for reasons of completeness, they are listed in descending order by date below. Papers in which the author of this thesis has first authorship are listed first:

Jakobi, T., Stevens, G., Castelli, C., Ogonowski, C., Vindice, N., Randall, Tolmie, P. and Wulf, V. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. ACM. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 4 (Dec. 2018), 28.

Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G. and Wulf, V. 2016. Smart Home Experience Journey: Über den Einsatz und die Wahrnehmung von Smart Home-Technologien im Alltag. WISSENSCHAFT TRIFFT PRAXIS. (2016), 12.

Jakobi, T. and Stevens, G. 2015. Energy saving at work - and when not working! Insights from a comparative study. *EnviroInfo and ICT for Sustainability 2015*. Atlantis Press, 2015.

Jakobi, T., Stevens, G. and Schwartz, T. 2014. Verhaltensbasiertes Energiesparen am Arbeitsplatz: Ergebnisse einer vergleichenden Studie. Proceedings of Multikonferenz Wirtschaftsinformatik 2014 (Paderborn, 2014), 76–88.

Jakobi, T. 2013. Always Beta: Cooperative Design in the Smart Home. Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication. ACM, 2013.

Jakobi, T. and Schwartz, T. 2012. Putting the user in charge: end user development for eco-feedback technologies. Sustainable Internet and ICT for Sustainability (SustainIT), 2012 (2012), 1–4.

Jakobi, T., Stevens, G. and Schwartz, T. 2011. EUD @ Smart Homes Smart refurbishment of rented apartments to improve energy efficiency. IS-EUD 2011, Workshop on EUD for Supporting Sustainability in Maker Communities, 2011.

Ogonowski, C., Jakobi, T., Müller C. and Hess J. 2018. PRAXLABS: A sustainable framework for user-centered ICT development - Cultivating research experiences from Living Labs in the home, Socio-Informatics. 592.

Stevens, G., Bossauer, P., Jakobi, T. and Pakusch, C. 2018. Mehrseitiges Vertrauen bei IoT-basierten Reputationssystemen. Mensch und Computer 2018-Workshopband. (2018).

Schwartz, T., Stevens, G., Jakobi, T., Denef, S., Ramirez, L., Wulf, V. and Randall, D. 2014. What People Do with Consumption Feedback: A Long-Term Living Lab Study of a Home Energy Management System. Interacting with Computers. 26, 3 (Apr. 2014), iwu009.

Hornung, D., Müller, C., Shklovski, I., Jakobi, T. and Wulf, V. 2017. Navigating relationships and boundaries: concerns around ICT-uptake for elderly people. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (2017), 7057–7069.

Table of Contents

List of Tables

List of Figures

1. Introduction

Against the background of the emerging data economy, the increasing tendency to digitally measure aspects of everyday life offers new possibilities for economic growth. An example would be the development of connected cars, by enabling cars to communicate the data collected by their many sensors: Both automobile and their suppliers may be interested in analyzing the performance data of vehicles and their parts after they are sold and under real driving conditions. Such tracking of hardware performance under real-life conditions may contribute to the development of motor vehicles and parts with more durable and efficient designs. Similarly, third parties such as insurance companies may wish to analyze driving behavior to make better offers to their customers. In addition to the potential for companies to profit from analyzing large amounts of data, consumers and society may also benefit from the digitalization of vehicles. For example, drivers may be interested in feedback on how to drive in a more eco-friendly manner or in reporting the locations of potholes anonymously based on data collected by their vehicles.

Similarly, beyond connected cars, digitalization and its associated networked devices are affecting an increasing number of aspects of everyday life. This ongoing development goes hand-in-hand with the success of cloud applications, data-based business models and personalized services. Many such technologies are already part of modern society. For example, smartphones have become permanent digital companions for many people, while networked devices in the so-called "smart home" promise comfort, security and automation. Likewise, fitness-tracking devices and smart voice assistants are examples of economically successful connected and data-based products. When it comes to more recent car models, people have less of a choice when it comes to digitalization, as many modern vehicles are connected to the IoT by default to provide data-based services and to support autonomous driving. In the European Union (EU), new cars are even required by law to be connected to the Internet via the so-called eCall system to provide assistance to drivers and emergency personnel in accidents [163]. Similarly, many nations have or are attempting to make smart meters obligatory to digitally manage their power grids and promote energy awareness [159, 415]. All of these products are regarded as types of cyber-physical systems with great market

potential. Their core service provision is typically based on storing and processing a wide range of sensor data concerning various aspects of people's lives.

Given the quality and quantity of modern means of obtaining digital data, questions arise concerning future approaches to designing privacy protection measures for cloud systems, particularly with regard to the design of such systems and the need for supporting digital privacy and individual self-determination. The challenges associated with providing usable privacy controls and information become even more pressing in view of the fact that digitization is not entirely voluntary in all areas: The previously mentioned rollout of intelligent metering systems and the European eCall system are examples of legally prescribed and basically unavoidable uses of cloud systems among large sections of the population of many countries.

Among essentially legal questions such as who data might belong to and whether data can actually be owned in a legal sense [138, 176, 216], given new technological developments, the concept of privacy in its current form has come into question. Some researchers have even gone so far as to proclaim the emergence of the post-privacy society [81, 233, 355, 467]. While one does not have to agree with this thesis, it nevertheless can be argued that, in accordance with Wittgenstein [464], privacy is a socio-historical, changing and vague term. Accordingly, theories of privacy are subject to constant change and exhibit a certain degree of uncertainty. This is necessary in order to be able to do justice to their equally dynamic subject—namely, a society that is changing, particularly with regard to technological developments—and to be able to provide answers to new questions. Since the end of the 19th century, theories about what privacy is and how it is negotiated have evolve, primarily due to technological developments such as the telephone, electronic data processing (initially primarily by state actors) and the Internet.

It is often proclaimed in the modern media that data is the "new oil" [426, 492, 520, 531], which suggests that data is a driver for economic growth. While this metaphor can be criticized in terms of its accuracy and adequacy [15, 125], it is undisputed that data can be ascribed a value insofar as user data are being traded and brokered legally, often for personalized

marketing purposes [61].[1] Beyond the criminal misuse of data (e.g., credit card information, addresses or passwords), personal information itself now has economic value. Particularly in the fields of social networks, e-commerce and, presently, smart metering, services making use of personalized data have proven to be valid business models. As a result, many ostensibly "free services" that claim to enhance and personalize user experiences on the basis of personal data come at the price of end users allowing service providers to process and further exploit this information to refinance their operations and maximize their profits. Simultaneously, misuse of data has been shown to lead to severe consequences for both individuals and societies, as discussions of how public opinion has been swayed prior to elections by the spreading of target information over social networks have shown [82, 118, 408, 497, 513]. Likewise, awareness has grown on the part of companies that even legal use of data might be perceived very critically if the data collection or analytical methods used to acquire such data are not perceived as legitimate or ethical by the public or if data are acquired without the public's awareness [56, 86, 87].

While protecting data against illegal third-party manipulation or access is typically one of the responsibilities of information technology (IT) security [518], managing and limiting the legal disclosure and use of personal data is the core objective of (data) privacy [161].

In a connected world, protecting data and communicating how data are used are critical for individuals, companies and society to protect their assets, communicate intended data use and maintain privacy. Most current approaches to making the implications of data protection measures in data-based services visible focus on the data and the recipient thereof. Much international legislation also focuses on providing statements on data rather than on clarifying consequences [165, 201, 509]. Such legislation, however, dates back to times when digital data processing was often reserved for a few large or governmental actors and was primarily a necessary secondary condition for processing than a business model on its own. In addition,

[1] For example, the Acxiom GmbH is one the most significant players in this regard; see https://www.acxiom.com/

the data collected were usually of relatively low complexity, such as address data, making them easy for consumers to understand.

Both the computing powers available and the types of data collected, however, have fundamentally changed as a result of the advancement of computer technology. Today, many areas of life can be captured by embedded and networked computers, and the resources required to handle and analyze large amounts of data are becoming increasingly affordable. Collected data are frequently hardly readable by humans both because of their abstraction and sheer quantity and the fact that they are collected over long periods of time. Thus, as increasing amounts of data are collected, the impact on the individual privacy of the end user becomes increasingly difficult for non-experts to assess. However, it is precisely this weighing of the effects and the added value provision that is core to consumer protection in both many (mostly economic) privacy models, such as the "homo oeconomicus" model [318] (and its corresponding privacy model) and the privacy calculus model [134], as well as in legislation, in the form of "informed consent."

In this regard, the EU's new legislation is no different. The General Data Protection Regulation (GDPR) [164], which came into force in May 2018, aims to provide a modern framework for the regulation of privacy throughout the EU and for European citizens around the world. The GDPR provides new rules concerning how data may be collected and must be stored and which rights customers have, including the rights to the erasure (famously known as "the right to be forgotten"), rectification, restriction and portability of and information about collected data [164].

In line with existing best practices for developing information technology, the GDPR propagates "privacy by design" [91, 311] principles to enforce the incorporation into the conception and design phases of technical systems.

However, the requirement that programmers implement privacy by design (PbD) is essentially based on the assumption that both designers (and users) know exactly what privacy means in the particular context of design and how to design for user needs in advance. However, non-essentialist privacy theories show that privacy is not a static concept but rather one that evolves

with the transformation of social practices [410]. This particularly applies to the development of novel technologies, which are often accompanied by a reciprocal transformation of social practices and privacy demands. Arguably, the introduction of connected devices in everyday life, such as the emerging technologies that fall under the broad category of "Internet of Things"" (IoT) technology, constitutes an example of such a technological and societal change.

In such cases, existing "best practices", whether at the legal, organization or individual level, must be reconsidered in light of changing underlying circumstances. In particular, instead of relying on an approach that attempts to solve privacy issues in advance, developing and maintaining an understanding of technology and its appropriation [135] in practice should be ongoing practices in the process of technology development.

From this perspective, understanding privacy behavior is not only relevant to the creation of more usable privacy management but also becomes of theoretical interest. Hence, this study addresses the issue of privacy practices in the context of some of the most relevant emerging IoT technologies using a Living Lab-based [157, 160, 185, 375] approach to obtain a more profound understanding of the situated practices [410] and their logics. The areas investigated include smart metering (see Chapter 3.3.1 for an in-depth discussion of the field), smartphones (Chapter 3.3.2), smart homes (Chapter 7, 8) and connected cars (Chapter 5,6).

The aim of this thesis is to investigate the potential of a methodological lens of practices [410] in privacy protection and data disclosure and the evolution of said practices as a result of technology appropriation. To do so, several design case studies [528] were conducted in the fields of smart metering, smartphones, smart homes and connected cars, and connected cars, with the emphasis being on investigating the privacy practices of households when collected data are fed back to participating households for evaluation. In this vein, the approach relied on a derivation of trace interviews [143] and is likewise heavily influenced by the idea of conducting "data work" [178, 495]. Overall, the studies typically aimed at uncovering privacy practices using IoT devices to inform usable design of individual privacy management systems.

2. Perspectives on Privacy in Information and Communication Technology

This chapter introduces the concept of privacy from a historical perspective, outlining its reflexive interdependence with technology and its evolving character, as well as conceptual understandings of this term. In addition, this chapter presents the three main perspectives on managing privacy (not only in the context of the IoT) and discusses research in the field of usable privacy.

2.1. Historical Perspective

The notion of privacy has evolved over time. Historical understandings of what "privacy" constitutes are closely connected to technological development and the appropriation of novel technologies by society. In particular, the development of privacy theories has largely been driven by the effects of new technology on societal contexts at particular times. As a result, there is no commonly agreed-upon single definition of privacy [463]. However, at least for Western societies, it can be demonstrated that societal consensus on privacy needs evolves when society is confronted with new technology. This section presents a few selected milestones; what follows is not intended to be an exhaustive discussion of the history of privacy but rather serves to illustrate the connection between changing notions of privacy and technological development.

A famous early example of privacy demands conflicting with technology can be traced back to the success of mobile photography at the end of the 19th century. Their emergence led Warren and Brandeis to write about the need to define the home as a private territory to be protected. In this period, privacy was understood as the "right to be let alone" [63] physically, for example in one's home, and securing buildings and private grounds was enough to protect their owners and/or inhabitants from being watched, listened to or tracked in any way of which they were unaware.

The introduction of telegraphy at the beginning of the 20th century, followed by the invention of the telephone, required an extension of these territorial privacy rights to the privacy of communication. Without having to enter anyone's home or property, third parties could easily

remotely wiretap early telecommunication. The notion of one's home being one's castle [453] thus needed to be extended to privacy of personal communications. Notably, however, in the United States, a bill intended to protect the privacy of telegram communication was introduced but never passed [451]. The next major trend, which is still ongoing, emerged in the 1960s with the introduction of electronic data processing, which was initially performed at the state level. The advent of IT led privacy theorists to characterize privacy as personal control over (digital) data flow [24, 517]. As a result, successive data protection laws were formulated to guarantee the informational privacy of the individual. These form the basis for today's legal measures for data protection, such as the Fair Information Practices, which protect individuals against the processing of their data [509]. At the time of entry into force and the following decades, the guidelines that were implemented largely limited data collection by governmental entities, as computers were still uncommon in the private sector.

With the success of IT in the following decades, however, computers with greater processing power and storage capacity became widely accessible and popular among organizations. Additionally, in the mid-1990s, data protection was confronted with another far-reaching technological breakthrough, as the dissemination and commercial exploitation of the Internet further enabled electronic data collection, sharing and processing in both the governmental and private sectors. In light of these developments, in 1995 the EU passed a directive on privacy and data processing on the Internet [165]. About 20 years later, a new technological upheaval arguably led to further important implications for data protection: First, computers started to become increasingly common and widely used, both at the workplace and in people's leisure time. Second, beyond traditional computers, a variety of everyday devices are now capable of measuring, communicating and acting without this activity being visible to humans. In 2016, the EU therefore renewed its efforts to regulate privacy on the Internet by issuing the GDPR [164], now including new or extended rights for consumers (e.g., to access, change or have data deleted by third-party organizations).

From a research perspective, understandings of privacy were traditionally thought of as entailing normativity or, to put it another way, as being bound up with issues such as trust (see [228] for an overview). Research into trust and privacy has investigated areas such as social

networking (e.g., [145, 183]), data mining (e.g., [321]) and mobile services (e.g. [231]), to identify only a few. Alternatively, privacy has often been seen as an economic function of decisions made by rational actors. A more specific theoretical perspective on privacy decision-making that has been widely adopted as a guiding principle for international legislation is that of the privacy calculus mental model [134]. This model focuses on individual behavior, considering privacy decisions to be the rational actions of an informed individual. From this perspective,

> *"individuals make choices in which they surrender a certain degree of privacy in exchange for outcomes that are perceived to be worth the risk of information disclosure"* [134].

The concept implicitly identifies a major prerequisite for making privacy decisions: People need to understand the social context, the roles and the behaviors of others and the potential future uses of the disclosed information. However, empirical studies have observed a "privacy paradox" in the form of a mismatch between stated attitudes towards privacy vs. actual user behavior [371].

Following this observation, research has shown that when people make decisions, the consequences and outcomes thereof are often not (or at least not completely) transparent to them [202, 459]. Theories opposing the rationalistic view are therefore often based on the notion of the "bounded rationality" of an individual [202, 459]. In contrast to strict economistic definitions of rationality, this concept emphasizes that rational decision-making is context-bound [227] and is dependent on (at best) partial knowledge of the social context and of the cost and benefits associated with data disclosure [382, 400].

Along the lines identified above, several conceptual understandings of privacy have drawn upon the concept of two contrasting spheres, namely the private and the public. Whereas some theorists presume the existence of static boundaries between both [400], others, such as Altman [24], have described privacy as a dynamic process that can be understood in terms of the boundary regulation theory. In this view, users engage in sophisticated practices to determine the appropriate level of privacy by continuous management of the disclosure of data and the flow thereof to third parties. Given the growing use of interconnected technologies in public

surveillance, the concept of "contextual integrity" [370] has been developed as an alternative benchmark for privacy and the challenges facing it. While not explicitly centering on the private and public spheres, both of the factors included in the model map on what is considered (non-)private by society in a specific context of data collection and use, as this concept considers both the context of surveillance and societal norms to determine whether government surveillance would invade citizen privacy.

Palen and Dourish [382] elaborated Altman's [24] view to fit new privacy implications and allow for privacy-sensitive design in networked systems. Their framework covers three dimensions: the disclosure boundary, the identity boundary and the temporal boundary. Each of these boundaries requires dynamic privacy management, in which disclosure decisions depend on the particular social situation at hand.

Focusing on privacy in the age of IT more generally, Solove developed a pragmatic notion of this concept that holds that human behavior in general must be understood from the background of historically contingent social practices in which privacy decisions are embedded in collective cognitive and symbolic structures that enable a socially shared way of ascribing meaning to the world. Hence, in order to understand and support privacy decision making, researchers should consider how these decisions are embedded in people's everyday understanding of the social context of data collection, the roles and the behaviors of the third parties involved and the potential future uses of disclosed information.

Crabtree et al. [117] built upon this notion of researching privacy for an ethnomethodological study of privacy practices to "repack privacy", resembling Palen and Dourish's paper title "unpacking privacy." [382] Crabtree et al. found that participants attempted to manage the "attack surface" [117] meaning the information that people expose using the Internet, which basically consists not only of IT security-related risks such as hacking and phishing but also of potential privacy incidents, for example disclosing data to third parties. Interestingly, for participants, the relevance of the "attack surface" to be managed manifested in terms of its potential impact on their everyday lives:

"The abiding concern is not with hardware, software, firmware or networks, but people *and the impact the networked world might have on their interpersonal relationships."* [117]

While maintaining privacy when interacting with technology has often been conceptualized as a technological task, Crabtree et al. show how humans make sense of privacy in their everyday lives. The management of an "attack surface" indicates a social phenomenon associated with how people relate to data and the sensitivity thereof that—after further exploration—may possess potential as a design resource for helping individuals in managing their privacy.

However, as the following chapter outlines, there are several perspectives on privacy, which are often interrelated.

2.2. Perspectives on Protecting Privacy

Protecting privacy is an endeavor that many fields are concerned with. The dominant perspectives on privacy and their foci are outlined in this chapter. Measures for safeguarding privacy are typically implemented with one out of four perspectives in mind:

1. From a regulatory perspective, legislation is the foundation for handling privacy, as laws codify societal consensus on norms and make them enforceable. The GDPR [164] put into effect in May 2018 is an example of such a measure.
2. A technological perspective emphasizes the use of means such as single technologies for anonymizing data [144, 148, 196, 279, 483] or sets of guidelines, such as PbD principles, [218, 311, 330] to support or grant privacy.
3. An organizational perspective seeks to protect the organizations' assets and manage risks and must comply with any relevant legal frameworks through the use of technology. In order to fulfill all of these requirements, such an approach often involves adopting frameworks encompassing technological, organizational or individual means. A widely adopted example of a norm that has been adopted to promote organizational security and privacy is the ISO2700x norm family [251].
4. Finally, some researchers have investigated individual behavior as a resource for designing systems intended to promote awareness of privacy and to support decision-making regarding privacy management.

I outline some key developments and research associated with all of the above perspectives to subsequently argue that they can only successfully protect privacy when they are combined and aligned and can thus function in a complementary fashion.

2.2.1. Legal Perspective

First, and most obviously, defining guidelines on what parts of life a right to privacy should include, is a matter of a country's legal system and judicial power. Almost all nations now have laws in place to safeguard privacy. Likewise, privacy has been acknowledged as a human right by the United Nations [491]. On a very basic level, laws codify and allow for the enforcement of societal consensus on those values and norms that should not be violated. Simultaneously, however, laws are to be non-discriminatory themselves. This is why, for example, laws such as the GDPR [164] are designed to be as neutral in terms of technology as possible: Doing so renders them adaptable to and interpretable in almost any circumstances. It also is meant to ensure that regulation can be applied to both today's technologies or those that might emerge in the foreseeable future. After all, laws should provide guidelines, but they cannot anticipate the complexity of every possible case. While the GDPR, for example, prescribes IT security measures for protecting data from being stolen, to be "up-to-date" in organizations, it will not describe concrete measures, as, for example, encryption methods that are currently considered to be secure may be broken by future technologies, as continues to happen [348, 476, 477, 508]. Likewise, guidelines such as "privacy by design" and "privacy by default" are demanded, but concrete methods for ensuring the anonymization of data or the require levels of such anonymization are not mentioned, as they will need to be determined in the context of each particular case. To meet these needs for neutrality and flexibility, new laws heavily depend upon being interpreted and "brought to life" by case law. Besides laws, there are other regulations that may be issued by government organizations that are binding, e.g. when operating in the context of infrastructures critical for society and/or state. With regard to IT security, for example, the German Federal Office for Information Security (BSI) has issued guidelines for smart metering based on the Common Criteria [104] that manufacturers must comply with.

From a legal perspective, privacy laws such as the U.S. Privacy Act of 1974 [504] or the GDPR [164] regulate how personal information should be handled. Originating in 1973 as a response to the emergence of the first digital data centers, the Fair Information Practices (FIPS) developed by the U.S. Federal Trade Commission [509] constituted the first widely adopted privacy-related "behavior" guideline for data collection to target enterprises rather than end

users. Additional regulation and standards such as the Common Criteria [104] play an important role in defining security requirements for the operation of systems that store and process private data. For instance, the BSI protection profile [73] outlines fundamental requirements for the secure and safe collection, transmission, storage, and processing of personal smart metering data. In addition, it defines basic consumer rights such as the ability to control the disclosure of data to third parties.

"Informed consent" is one of the core principles of most privacy legislation. It stipulates that the consumer, as data subject, must consent to the disclosure of his or her data for defined purposes through an active and conscious decision. Likewise, the GDPR is based on the model of the responsible and conscious consumer, who, in addition to "informed consent," now also has the explicit freedom to request data from providers to limit the processing thereof or—insofar as is (contractually) legally possible—to delete his or her data. Thus, the sovereignty over the personal or personal data generated by a consumer lies with him or her, as the existing practices of management tools (e.g., those used in social networks [215], organizational information systems [e.g. 16] or e-commerce [9, 134]) show. The need to obtain informed consent by presenting the data to be released to the recipient and the purposes for which that data will be processed was initially identified in by both the German Federal Privacy Law [52] and the previous data protection directive of the EU [165] and is included in today's GDPR [164].

2.2.2. Technical Level

Although the law should be technologically neutral, legislation, the jurisdiction of courts and technology have historically been intertwined. For example, hearings with technology experts are routinely held both when creating new laws and in court.

The field of IT security considers four main goals when attempting to safeguard digital data, namely preserving the confidentiality, integrity, availability and authenticity thereof [518]. From a technical perspective, the major goal is to embed privacy protection into the technology to be designed.

Essential privacy and security protection is provided via technical means such as encryption, authentication and anonymization [206]. The two main approaches to embedding privacy into technology by design attempt to limit personal identifiability by either manipulating the data to be disclosed or reducing the amount thereof. The first category includes statistical strategies such as distortion [433], data anonymization [325], random noise integration [507] and obfuscation via local buffers [271]. Another approach to ensuring privacy aims at anonymity through aggregation [427]. For example, in the case of smart meters, this aggregation, can be implemented in one of two ways [158]:

- spatial aggregation, which summarizes the readings of a larger grid segment (e.g., all of the households attached to one converter station), thus obfuscating each single household within the larger group; or
- temporal aggregation, which involves using longer intervals between data collection and transmission in order to avoid revealing fine-grained and potentially sensitive data.

However, these statistical aggregation techniques create additional overhead, thus potentially reducing the flexibility of and affecting service quality (e.g., eco-feedback) for consumers [206]. As a solution, Pallas suggested the introduction of a "data trustee" role, who should be responsible to store data securely and eliminate the necessity to fall back on having to trust non-neutral parties handling consumers' privacy [383].

Some of the approaches that fall under this umbrella include PbD, privacy-enhancing technologies (PETs) and privacy-preserving technologies (PPTs) [123]. These provide best practices, guidelines and schemes, such as preventing data spills, supporting data minimization and providing various levels of anonymity, unlinkability and control over individual digital identities. A common 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" [206]. These principles have been applied to many areas, including ubiquitous computing [309] and smart metering [92, 95], and have also been adopted as principles in more general legislation such as the GDPR [164].

2.2.3. Organizational Perspective

For organizations, safeguarding hardware and software assets is also of vital importance, as is compliance with relevant legislation. In organizations, security and privacy are often enforced not only by technological means but also by enforcing workers' compliance with

organizational rules or educational measures. Particularly since the beginning of the new millennium, interest in IT security for organizations has grown in the industry, resulting in a variety of frameworks targeting the implementation and verification of organizational security [151, 332, 399, 411, 505, 535]. Overall, risks are handled by minimizing them technologically, raising security awareness or establishing compliance rules, assigning or delegating them either to internal or external authorities or by accepting those that remain. The information security management system (ISMS) as codified the ISO2700x norm family can be considered to be a particularly important and successful framework. Based on organizations' information security requirements and the expectations of stakeholders, ISMS frameworks typically suggest to implement a continuous improvement process that follows a plan-do-check-act methodology.

Research on the delicate matter of IT security in organizations has proven to be challenging to conduct, as organizations have to outline their potentially insufficient security measures to outsiders [297]. When it is possible to find appropriate and willing partners, workers are often characterized as rational users by management and researchers themselves [26, 79]. As a result, identifying and modeling the parameters that may influence workers' (in-)secure decisions is a way commonly used for trying to improve workers' compliance to organizational guidelines [460]. However, it has been found that contextual factors such as top-management and organizational culture also influence compliance behavior, which is far more complex than that of rational users.

Information technology security cannot be reduced to ticking boxes or instantiating workflows. Furthermore, workers are not only passive instruments to be educated or sanctioned; they also need appropriate tools with which to manage IT security. Famously, Sasse et al. stated that "users are not the enemy" [16] and demonstrated that unusable passwords result in increased workloads for helpdesks. Other studies have found that the level of compliance in workflows is related to the effort required to comply with organizational guidelines [41, 236]. Given these observations, insecure behavior makes sense from an economic perspective. Therefore, organizations must provide usable tools to allow their works (even when it comes to IT professionals[99, 253, 452]) to work more securely.

2.2.4. Individual Perspective

Securing and minimizing collecting of personal data by system design is an important step to safeguard individual privacy without the user having to care about basic protection. Still, legal frameworks highlighting concepts such as "informed consent" and "informational self-determination" need the user to be aware of and actively approve data disclosure. Against this backdrop, it is an important question, how levels of exposure or secrecy, privacy or its absent, should be communicated and designed in an IoT context.

Therefore, also HCI has—compared to its young time being—a long history on designing for usable privacy. Due to the nature of the field, research on usable privacy, in both its development and focus, focuses on technological trends and their application. On the individual level, the main goal is to foster and support privacy-related user behavior. This objective is addressed in different ways, such as providing usable privacy features, increasing privacy awareness or providing support for privacy decisions.

The aim of usable privacy is to ensure that useful privacy management mechanisms are available and that these features are designed in such a manner that they are usable and understandable by non-tech-savvy users [198, 473, 519]. At the basic level, usable privacy begins with the application of general usability principles for designing technological systems and interfaces. More specific principles include enabling privacy practices as part of normal system usage and not inhibiting established usage practices [315], taking mental models of privacy and security into account [326] and supporting standard privacy-oriented access controls [475].

The primary aim of privacy awareness tools is to sensitize the user to various privacy-related concerns [33, 400]. Approaches that address privacy awareness attempt to increase individuals' attention, perception and cognitive capacity regarding which of their personal data are recorded and by whom, how these data are processed and used and what amount(s) of data will be stored and where [400]. This is challenging in ubiquitous computing environments, as it is often not readily apparent that data collection is taking place at all [311].

Instead of merely providing passive awareness, a privacy decision support system aids users in active decision-making on privacy-related matters [13] by facilitating informed choices [322]. However, there is no clear separation between passive and active techniques because studies have shown that providing contextual cues, making people aware of privacy issues and presenting appropriate privacy-relevant information have an impact on disclosure decisions [291]. In this vein, the potential of the justifications provided [293] and social norms [14, 386] have been widely debated. A salient and widely researched example of a PDSS is the interface for specifying privacy preferences for smartphones [33, 152, 173]. Felt et al. [172] conducted an extensive survey of the diverse strengths and weaknesses of design alternatives.

Further general guidelines addressed in the literature to support privacy decision-making include the provision of meaningful and suitable alternatives [437], improvement in the expressiveness of the available options without a corresponding increase in complexity [33] and increasing understandability by using straightforward and non-technical language [69].

While a significant amount of research is being conducted in usable privacy, it has not been integrated into many other fields. Although privacy is considered a key aspect of IoT and ubiquitous computing, human factors, usability and user experience (as relayed in user demands) are largely unaddressed when drafting technical legislation.

2.3. Designing for Usable Privacy: A Synthesis of Perspectives

When designing usable privacy, theoretical concepts of privacy do not serve just as analytic tool but also explicitly and implicitly shape the design space [123]. As outlined above, privacy-oriented design techniques also vary substantially depending on the perspective adopted. The perspective used in this work is primarily that of HCI. With research in this thesis spanning across several domains with products that incorporate IoT concepts, however, it is clear that other stakeholders also participate in the design of technologies. These may include governmental representatives and offices and public or private organizations that both rely on and implement IT security technologies.

Therefore, in this thesis, the outlined perspectives are considered not as mutual exclusive or parallel worlds but instead as being heavily intertwined and thus having to work in concert

with each other to identify sound solutions [516]. Privacy mechanisms at any level, this thesis argues, must designed collaboratively in respect of and complemented by corresponding counterparts on other levels to become truly effective. In this vein, this work not only provides a user perspective on privacy demands associated with some of the most widespread consumer IoT devices but also addresses methodological implications concerning how HCI must be adaptable evolve to be able to function alongside with regulative processes and domains such as IT security and law.

3. Study Outline

In this chapter, based on the current state of research, practice and legislation, the research perspective and, in particular, the research questions guiding this work are presented. Thereafter, some key characteristics of the fields of research addressed in this thesis follow. The chapter also features the demonstration of the setup and realization of the Living Labs in the research conducted. Additionally, the overarching methodological theme of the use of design case studies and the Living Lab methods of research as key frameworks in this thesis are described as the methodological underpinnings of subsequent studies that were conducted in different contexts. The thesis then provides a detailed account of each publication's contribution to answering the research question and motivating and steering further research.

3.1. Research Perspective

> *"Most PETs require advanced knowledge to use, are complex to configure and operate correctly, and ultimately fail to meet end-user needs."* [248]

Although the field of usable privacy has been gaining attention over the last years, users still suffer as a result of unusable hard- and software. Beyond the need to conduct research to address existing questions regarding how to design for usable privacy, however, new questions have emerged. In light of technological advancements, decisions concerning whether or not to disclose data are gaining both economic and social importance. Simultaneously, the same advancements lead to an increasing number of new products relying on the collection of (from a user-perspective) abstract data, as a) these data are typically configured to be machine-readable and b) products collect highly technical sensor data in vast amounts. Due to these new developments, it must be discussed whether practices that have been taken for granted— be they on the legal, technical, organizational or individual level—still hold up under the fundamentally new conditions brought about by the rise of the IoT and data markets for individual users.

Against the backdrop outlined above, this thesis aims to provide an understanding of how data disclosure information should be designed from a users' perspective.

Theoretically, the approach taken in this thesis was highly influenced by ethnomethodological thinking such as that of Garfinkel [189, 190]. Ethnomethodology has been frequently used as a form of inquiry in design research and as a method for analyzing interactive systems [405]. As research has demonstrated, ethnomethodological approaches are suited to grasping broad notions and situated effects associated with (not only technology) usage. Since ethnomethodological studies work with real-world actions, in contrast to, in contrast to quantitative studies, they are not as prone to be critically influenced by common pitfalls such as the attitude-behavior gap or the effects of bounded rationality [202, 458]. Instead, ethnomethodological research can focus on the ordinary flow of actions taken by actors in their everyday lives, which they generally do not realize are governed by certain structures.

To study these structures empirically, large parts of this research began with conducting trace interviews, which is a common practice in the study of posting behavior on social networks [143]. More specifically, this approach is closely related to the concept of "data work" [178, 495], resembling a softer version of breaching experiments [111, 113, 115] which intervene into and disturb existing practice with technical artifacts to make them explicit and visible to researchers.

This research is based on specific cases concerning the (partially prospective) privacy practices of ordinary people using IoT products in Germany (the characteristics of these products are outlined in Chapter 3.3). In certain ways, studying the practices of ordinary, non-experienced users may lead to bias, as their practices may change when people become more familiar with a technology. However, such a "bias" also has a strength: When actually buying a connected product or having a smart meter installed, users will have to make privacy decisions a priori. Asking non-experienced users questions about their perceptions of the privacy implications of technology is thus a helpful approach to identifying their actual practices.

In this regard, this research is driven by a strong practical orientation, which makes it possible to understand the issues related to the research question from the user's point of view, which is particularly useful when exploring and "sensitizing concepts" [55].

The social constructivists Thomas and Thomas stressed that if people define situations as real, those situations are real in their consequences [239]. Following this way of thinking, the evaluation of risks and advantages, as promoted by the concept of informed consent, is by no means objective but instead relies on how people define the riskiness of a situation. In this respect, the focus should actually be on perceived risks and benefits. As stressed by Thomas and Thomas, such a definition is not arbitrary, as it has consequences; for example, if leaving an apartment unlocked because the neighborhood is perceived safe, it makes it easier for others to break in.

With regard to information, it is also a priori not clear what meaning (also beyond concerns regarding privacy) is attributed to data such GPS coordinates because the individual's attribution of meaning to data significantly influences his or her decision as to whether something is classified as private or less sensitive [410].

In the case of privacy decisions, one would have to ask how data that are to be released or kept private are constructed and evaluated. What impression does the owner have of information or data, and what does he or she consider to be private about such information or data? What is the value of keeping certain data private? Using this approach, it is possible to determine which mechanisms are used in decision-making.

Part II of this dissertation focuses on answering the questions identified above. The five chapters of part II have been published previously and closely resemble the forms in which they were published as journal or conference papers.

3.2. Methodology[2]

This work generally follows a participatory design paradigm, subscribing to a design-case-study methodology, as described by Wulf et al. [528]. As a result, the majority of the research presented was conducted in a Living Lab setting, as this approach made it possible to conduct long-term appropriation studies on the research artifacts in question. Within this setting,

[2] Parts of this chapter relate to the previously published book chapter: Corinna Ogonowski, Timo Jakobi, Claudia Müller and Jan Hess 2018. PRAXLABS: A sustainable framework for user-centered ICT development - Cultivating research experiences from Living Labs in the home, Socio-Informatics. 592.

mixed-method studies were conducted. All of these studies contribute to an iterative, user-centered process for designing solutions for the management of privacy concerns.

In terms of concrete methods, this thesis relates to a mixed-methods approach. Randall et al. [405] suggest that qualitative methods in general and the ethnographic approach to studying practice in particular should not be understood as distinct approaches themselves, but only serve as suitable methods for distinct analytic commitments and interests. Such a view is in keeping with the broadly "anti-method" line found in much ethnomethodological work [331] and can be traced back, at the very least, to work of Paul Feyerabend [175]. The point here is that an understanding of practice does not require a specific method but rather a commitment to the idea of the "rationales" [227] of the members of the practice in question, especially if one considers the "individual" level discussed above seriously. In principle, rationales can be elicited in a variety of ways. Therefore, this thesis presents studies using a variety of methods either suiting explorative, ethnomethodological interests, as well as more evaluative, even quantitative means (see Table 1).

Table 1: Overview of methods used throughout the studies.

Chpt.	Paper Title	Methods used
4	Multilateral, Accessible Security of Smart Metering Systems	Scenario-based stakeholder analysis
5	Privacy by Design for Connected Cars: Available Architectures from a Consumer Perspective—a User-Centered Discussion	Scenario-based stakeholder analysis
6	Second Dashboard: Information Demands in a Connected Car	Design case study, participatory design, interviews, focus groups
7	The Catch(es) with Smart Home: Experiences of a Living Lab Field Study.	Design case study, participatory design, interviews, focus groups
8	Providing smartphone data visualizations to support Privacy Literacy	Breaching experiment
9	Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility	Design case study, participatory design, interviews, focus groups
10	It's About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering	Open-ended questionnaire, focus groups, design probe, post-task interviews, quantitative evaluation

By targeting some of the IoT systems most widely used by end users and carrying out design case studies in practice, the studies were intended to extend the understanding of how to design for usable privacy in IoT environments, taking into account technological, legal and individual perspectives. Consequently, the aims of this thesis are as follows:

- To promote the relevance of an integrated perspective of privacy by considering regulations, technological development and individual empowerment. More concretely, the thesis seeks to demonstrate how HCI (as a representative stakeholder of individuals in privacy regulation) can prove helpful in improving the security and privacy of IoT technology;
- To demonstrate the importance of information visualization for sensitizing end-users and promoting their privacy literacy; and
- To obtain insight into the inner workings of the phenomenon of data disclosure in IoT environments and identify means by which to inform design for supporting users in managing privacy.

3.2.1. Participatory Design

Participatory design (PD) aims to involve different stakeholders in the development process to reach a more democratic design [53] and, more generally, to develop software that will be accepted by users. Applying the methods and tools of PD aims at fostering a process of designing software that is, in some senses, grounded in practice. Traditionally, work in PD addresses the context of the workplace [57]. Bødker et al. highlight the importance of a design that is truly informed by the needs of actual users. Such a design process requires establishing a *mutual learning process* between designer and users (to address questions such as "what is needed?" and "what is possible?"). Instead of involving users as informants only, their *genuine participation* results in a shared understanding of needs, problems and options with regard to solutions.

With the wider distribution of new technologies, PD has increasingly focused on the domestic context. In the field of HCI, applying PD to applications related to the home has become equally popular, such as in the contexts of home care, ageing at home, family interactions around new media or energy management and sustainability [115, 381]. Several concepts intended to promote the transferability of findings from the work to the home context have proven successful to some degree, such as designing for social awareness [113]. However, the home context arguably features unique demands of the appropriation and use of domestic

technologies. Rather than designing for efficiency and utilitarian pursuits, home technologies aim to foster sociability, inclusion and social awareness. This prompts a need to take into account different underlying design aspects, such as designing for recreational or ludic experiences [195].

3.2.2. Design Case Studies

The multi-staged, action research approach [232] of design case studies [528] combines methods from ethnographically-oriented research into user behavior and its rationales [405] with those from design research, in which "probes" are used in a variety of ways, from the stimulation of creative ideas to the evaluation of prototype artifacts [111, 194]. The basic purpose of the design case study approach is to provide a means by which to relate the in-depth knowledge of current practice that an ethnographic orientation provides with a means by which to assess the viability and consequences of a technological intervention collaboratively with users. From this perspective, design is understood as an open-ended process that is informed by the context of a particular study and that has a transformative potential.

Design case studies serve as a means by which to structure and learn about practices in and through design [527]. In this context, practices are to be understood as part of the concept of praxeological practice [410, 528]. In my work, user practices with regard to data disclosure represent the starting point of my investigation into the social and socio-technical phenomenon of privacy management in IoT. In this context, a practice can be defined as follows:

> *"A practice is understood to be a mainly routinized pattern of human action which is not only encompassed by mental and physical forms of activity but that is also greatly imprinted by objects, especially by tools, media, and their usage. A practice is grounded in background knowledge that is both not entirely explicit and containing emotional as well as motivational elements. Practices, therefore, represent collective patterns of interaction that are reproduced in specific contexts. While the collective patterns of interaction are routinized, the concrete action is situated context-specifically and may deviate from them." [528]*

Three main phases can be distinguished within the design case study approach: During the pre-study phase, researchers seek to understand practices so as to then be able to frame a design space. During the technology design phase, the design space is mapped onto technologies and transferred into a design that is believed to have the potential to address the identified practices. Thereafter, during the appropriation phase, research aims at understanding how the usage of newly introduced artifacts interferes with and interacts in shaping practices and vice versa. Design case studies thus provide grounds for addressing a certain context and looking into user requirements and impact of intervention on practices in detail while also affording a basis for comparison. Design and evaluation can occur in different fields of practice, and the findings produced by such research can be used to learn how software is being adapted and to gain further insights into how a particular case (the design solution) might function in similar environments.

3.2.3. Living Lab Setting

The general approach taken to researching domestic contexts is closely linked to Living Lab studies in that the preference is to conduct long-term studies on households in naturalistic settings whenever possible. By collecting context-sensitive data, an in-depth understanding of privacy management and the issues associated with it, as well as user groups and their needs, can be established. Longitudinal field research holds a considerable if often unrealized potential in terms of the progressive refinement of design concepts and the evaluation of the artifacts that result.

Living Labs [157, 374, 375] have proven to be a suitable framework for long-term in situ research, especially when investigating the adoption of technology. They allow for researching appropriation processes in the wild, as participating households are able to integrate prototypes and tools into their domestic ecologies. Thus, study participants do not have to anticipate usage scenarios but can actually live and explore them. Furthermore, this long-term cooperation includes all stakeholders, including hardware and software developers, disseminators, vendors and third parties. In various scenarios investigated in this thesis, the Living Labs framework was found to effectively provide basis for and guide the development of participatory development processes.

In Living Lab settings, design and development thereof is informed by continuous feedback from (potential) users and represented in the form of mock-ups and other intermediate design products that support the ongoing negotiation processes among design teams, end users and stakeholder groups [375]. Similarly, evaluation of the products designed as a result of the process is another important element of Living Labs. In the ideal case, prototypes are given to households as early as possible to allow researchers to learn how technology is appropriated in a real-world environment and embedded into social practice [474].

Methodologically speaking, many different methods can be used to gain empirical insights, including interviews, workshops, observation studies, usability tests and online questionnaires (or combinations thereof). However, the approaches adopted by the many scholars who fall under the broad label of Living Lab research vary considerably, often because the proximity of such research(ers) to real-world practice varies considerably. The techniques employed to evaluate the use of IT artifacts in the home and how they are appropriated will be contingent on the degree to which the real-life circumstances of the representatives of the target group are investigated.

In this thesis, Living Labs are conceptualized as suggested by the PRAXLABS framework [375]:

> *"[...]an evolving systematic approach to the generation of a scientific corpus of practice-based design work, being described as Grounded Design [420] [..] in turn based on the Design Case Study" approach by Wulf et al. [527], reference by the author.*

Living Labs with a focus on domestic or private sectors conceive the notion of a "real-use" environment in different ways. Scholars who conduct Living Labs either collaborate with users in real-world testbeds or in controlled artificial environments within test centers. For example, MIT PlaceLab [250], Philips HomeLab [431], the Georgia Institute of Technology [3] and Fraunhofer Inhouse [78] have conducted both short- and mid-term evaluations in large-scale controlled artificial domestic settings by building "typical" apartments or houses in test centers and inviting participants for single-test or short-term studies over several hours or a few days. In these studies, the researchers placed great emphasis on the layout of the labs to make "the

environment aware of human activity" in the most supportive and least obstructive way possible [3]. In contrast to relatively controlled environments of this kind, Bergvall-Kareborn and Larsson [48], Mueller et al. [361], Wan et al. [506] and Schuurman et al. [443] conducted more longitudinal studiesdesign studies and evaluations in natural everyday life contexts and collected in situ feedback on user experience, usability aspects, technology acceptance and appropriation processes.

3.2.4. Methods

The following subsections briefly describe the methods used throughout the studies described in this thesis.

Multi-lateral Security/Scenario Analysis

Multilateral security is based on the view that security can only be defined from the perspective of particular actors and their justified (security) interests [391]. Hence, the goal is not objective security but finding a compromise that is acceptable to all parties. A multi-sided security infrastructure is intended to reduce the need for mutual trust, recognize conflicts between actors, permit equitable negotiation and enable each interest group to verifiably protect its security interests within the bounds of the negotiated compromise [391, 526]. In practice, this approach is often based on a combination of legal, organizational and technical perspective.

The international debate on IT-Security is increasingly recognizing the merits of a user-centered approach to security, which focuses on usability issues in security models, mechanisms and systems [539]. This approach shares many similarities with multi-sided security. However, while multi-sided security takes a bird's-eye view, user-centered security adopts an explicit user perspective, but not without considering the socio-technical preconditions that structure human behavior [307].

Multi-sided security has a special focus on the core security and usage requirements of various stakeholders and intends to harmonize these requirements in the planning and implementation phases of technology [424]. It usually highlights the tensions between the various actors' interests. A major contribution of user-centered security, however, is its focus on actors' internal conflicts of interest. It sees a user as a social subject who unites different interests,

many of which may conflict [409] ((in particular, there is often an internal conflict between security and usability interests). Empirical studies have shown that users often make case-based compromises between security- and usability-focused usage practices to achieve their aims [519].

Therefore, a user-centered approach to security attempts to assess the usability of security solutions, analyze the conflict(s) between overall system security and usability and identify viable compromises.

With regard to multi-sided security, first the usage scenarios and the (justified) interests of the relevant user groups need to be considered. These interests must be balanced on the basis of the data protection principles of purpose limitation and necessity and taking into consideration data subject rights [267, 274, 378, 423, 425].

Focus Groups

Focus group interviews represent a well-established methodology for exploratory research intended to obtain as wide a range of responses as possible [31, 67, 310, 342]. Originating in media analysis [354] and having been adopted by medical researchers investigating illnesses, focus group interviews have become a widely used method in user-centered design:

> *"The method is particularly useful for exploring people's knowledge and experiences and can be used to examine not only what people think but how they think and why they think that way."*

A key aspect of focus groups is the fact that what participants tell the researcher is inherently shared with other group participants as well. This calls for careful management of a group's atmosphere to ensure an open-minded and truthful discussion. Above all, participants must feel that they are able to freely interact with each other, and wide gaps in social background or lifestyle can defeat this requirement. Note, however, that the goal is homogeneity in background and not homogeneity in attitudes

For recruiting focus groups and in terms of seeking insights, it is often more useful to think in terms of minimizing sample bias rather than achieving generalizability. This shift in priorities calls for wise theoretical sampling [110].

One important strategy here can be the segmentation of potentially conflicting ideas to avoid destructive discussions or to ease social pressure. There are strong arguments [359] against mixing categories of participants across authority or status lines, either due to ethical issues or because of the high probability that the discussion will be uncomfortable at best and conflict-ridden at worst. The general strategy in using complex, segmented designs is to create a variety of internally homogeneous groups that capture a wide range of potentially distinct perspectives [288].

However, when participants are able to freely engage in a constructive discussion, especially with regard to creativity, the exchange of ideas can be fostered by collective and cooperative thought and action.

Interviews and Open-ended Questionnaires

Interviews are a widely used method for gaining insights into participants' lives and actions, as well as both the internal and contextual factors influencing them. In particular, narrative interviews seek to give rise to interview situations that are similar to everyday conversations and in which interviewees' comments at least partly drive the elicitation of topics [242] and the interview structure itself.

Throughout the studies in this thesis, interviews are a frequently used method, with slight variations and nuances for different purposes. During the explorative phases of the Living Lab research conducted for this thesis, interviews were largely framed as problem-centered interviews in a broader sense, rather than targeting specific sequences of events, they were intended to provide an understanding of the participants and their perceptions of the topics of investigation. While not as broad as a narrative interview and generally concerned with certain aspects of life, such an interview is likewise

> *"[..] based on interactionist and phenomenological sociological research traditions [442] with its principle concern to understand how the everyday 'life world' is constituted. In this respect, the phenomenological sociology of knowledge put forth by Berger and Luckmann [47] is crucial for the understanding of reality as a socially constructed entity."[439]*

Particularly in research within Living Lab settings, during the phases investigating the use of technological artifacts, which followed the exploratory phases, more focused questions regarding embedding of technology into everyday life became increasingly important in the research process. Such a combination of narrative and semi-structured interviews parts is common, particularly in social science research, and is often referred to as a problem-centered interview [522].

Weiss notes several drawbacks of interviews in general, most importantly he highlights:

> *"When respondents are asked about opinion, attitudes, appraisals, evaluations, values, or beliefs, shading responses to present a positive picture of the self is especially likely."[515]*

In particular, semi-structured interviews can be problematic in that researchers bring up topics, thus potentially imposing their ideas on the participants [439]. Therefore, a researcher should carefully reflect on the manner in which topics will be raised in interviews. In this regard, the problem-centered interview as developed by Witzel [522] provides some guidelines for balancing narrative flow and topics of interest.

Another challenge encountered in interviews is related to the temporal decoupling of a participant's experience and the reporting thereof to the researcher [515]. Due to this gap, and in contrast to methods such as observations (which are often used in ethnographic research), contextual information may be lost or reported in a distorted manner from the memory of interviewees. Moreover, critical aspects of the participants' interaction with the technological artefact could be totally forgotten and thus rendered inaccessible for the researcher:

> *"Despite all the ways in which interview material can be problematic, richly detailed accounts of vividly remembered events are likely to be trustworthy. Nor does apparent inconsistency always demonstrate invalidity. After all, people can act in inconsistent ways or maintain inconsistent feelings." [515]*

To counter this effect and to strengthen the connection between the collected data and past experiences, this thesis also used data visualization tools as a resource in many interviews.

Such an approach is common in, for example, co-analysis of social media posts [143] and is known as a "trace interview."

Weiss argues that besides planning and conducting interviews properly, the interviewing partnership ultimately is of crucial importance in terms of ensuring the validity of interviews. To manage these partnerships—especially over longer periods of cooperation—the PRAXLABS setting provides important guidelines [375].

Throughout the studies, open-ended questionnaires have been a means by which to understand respondents' hopes, fears and demands with regard to IoT technologies. While those questionnaires featured open-ended questions much like those used in interviews, in this case, the interviewer was unable to ask follow-up questions and thus had reduced flexibility in terms of adapting the interviews to individual statements or questions. However, this method was only used in case the scope of investigation was very clearly defined.

With regard to analysis, both the oral and written interviews were transcribed and analyzed them using thematic analysis by Braun and Clarke [66]. Responses were analyzed by at least two researchers, who paid attention to how the participants expressed their expectations, concerns and needs. Thematic coding is situated within the broad tradition of grounded theory [204] but allows focused research questions to be used. Therefore, its broad phenomenological orientation and lack of emphasis on theory building suited the research questions very well. Rather than generating theory, the primary research interest was in eliciting rich descriptions of phenomena. Using the MaxQDA coding software,[3] the coders (minimum two researchers, find more on that in the method sections of the respective papers) individually coded three randomly chosen questionnaire responses. Depending on the type of interview (whether it was more problem-centered and open or was more structured), a mixture of deductive and inductive coding was used. Each round of interviews featured various sessions aiming at consolidating codes identified. The resulting code set was subsequently applied to the analysis of the remaining responses and was critically and iteratively refined throughout the analyses

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

conducted by the coders iteratively. Newly identified codes within the remaining questionnaire responses were added to the individual code sets and were discussed in a final round of consolidation.

Breaching Experiments: Feeding Back IoT Data Individually and Collectively

By discussing IoT data and their semantic meaning through personalized visualizations, the data were re-contextualized and thus opened to exploration and reasoning about their character. With regard to more concrete methods, a wide variety of largely qualitative methods was employed, such as explorative and evaluative semi-structured interviews (both with and without technology, mockups and/or prototypes of varying degrees of maturity), creative and reflective workshops with both lay users and experts and observations.

Over time, the tools used also evolved alongside technological advancements. Early work, for example on smartphone data collection, relied on manual generation of visualizations. Throughout the course of these studies, however, a flexible web-based tool was developed specifically for the purpose of data exploration, which was subsequently used to visually depict the recorded data of the study participants. By providing actually collected data, this tool helped identifying the participants' privacy demands and preferences by making them explicit during the course of the interviews and thus accessible as a design resource for following design iterations.

This research takes an approach that involves collecting and visualizing data and feeding the visualizations back to users. Through data exploration sessions and design workshops, users' data literacy and ways of referring to data as a means of practicing privacy were investigated. Methodologically, this work is thus influenced by theoretical methods such as trace interviews [143], which were adapted to research users' relation to IoT data. In their theoretical framing and conduct, these studies are closely related to what was later referred to as "data work" [495], an approach which within the studies of this thesis has been applied to understand privacy demands of participants.

Design Probes

Probes are used in a range of ways, from the stimulation of creative ideas to the evaluation of prototype artifacts in user-centered design processes [111, 194]. Design probes are understood as "an approach of user-centered design for understanding human phenomena and exploring design opportunities"[339].

In HCI research, a design probe [58] can serve different purposes: First, a probe can serve as a tool for interpreting empirical design findings as a part of research through design [194]. Second, a probe can serve to make subconscious or taken-for-granted practices, values and norms apparent by irritating and possibly explicitly breaking with the "normal," as perceived by participants in a manner similar to that of breaching experiments [111].

From a methodological perspective, design probes can be characterized through three core features [339]: First, the user takes an active part in generating research data. Second, they are used to unveil the personal contexts and perceptions of users. Third, generally speaking, design probes are of an exploratory nature. In this regard, they are closely related to ethnographic approaches[112, 432] such as the ones outlined above. For supplementing qualitative findings, however, a probe can also be extended to feature a quantitative component by having a higher number of participants use the probe, which is how design probing was used in this thesis to explore data privacy practices in the context of smart metering (Chapter 10).

3.3. The Consumer IoT: Selected Fields of Investigation

During the 1980s, the private sphere became a prominent field for research on HCI. Empirical research, especially ethnographically oriented methods such as observation, was conducted on certain aspects of the role of technology within private life, focusing particularly on technology in the home. Television and video played a particularly salient role as a focus of research activities. Lull, for example, investigated the social use of TV within families [329]. With the mass adaptation of PC technologies in the mid-1990s, many new research interests emerged. New devices such as interactive TV sets changed the ways in which services were used and also influenced usage practices (e.g. those related to an early set-top box trial [373]) or led to or the emergence of new services for communication and individual media consumption (e.g., streaming providers such as Netflix and Amazon) on a variety of different devices (e.g.,

smartphones and tablet PCs) [238]. Today, smart home devices and wearables with smart functions are further shaping the consumer market and household practices. These devices reside around the home but are not limited to its physical space. For example, connected cars or wearable devices are often conceptualized as part of private life, but their use is not necessarily bound to the geo-spatial limitations of the home. In this regard, Living Labs are often used as a research framework for researching the home as a "place" and not limited to its "space", as discussed by Harrison and Dourish [229].

Therefore, researchers in HCI and related fields have investigated different aspects of private life at the intersection of technology and its use. A variety of empirical research work has focused on different aspects of how technology is used and managed within families (e.g., the use of computers to provide technical support or to assist in domestic chores [396], home networking [214] and home automation [72, 226]) and the routine nature of communication [115].

Broadly speaking, there are three different ways in which consumer IoT devices find their way into society: First, there is the sector of new, market-driven IoT devices and services. An early, but particularly noteworthy, example of the spread of IoT products through the market arguably is the smartphone. More recently, smart home systems, fitness trackers and smart assistants have become part of this stream. The introduction of these devices was and still is driven by consumer demand for innovative technology. For these technologies, new regulations are not being issued. From a privacy research perspective, bearing in mind the reflexive nature of society, technology and privacy, it is important to determine how new technology can relate to societal and legislative interpretations of privacy, protective and informational needs, and how to design privacy management accordingly.

Second, and less common, is the case of legally prescribed digitalization. For example, the use of smart metering devices is mandatory for citizens in many countries and will soon become obligatory for millions of other people globally. In the case of "IoT by government," specific new regulations are often involved. Smart metering, for example, was one of the first technologies to be subject to PbD in Europe. In addition, the German government classified smart meters as part of the critical infrastructure of the country's power grid and thus issued

IT security guidelines based on the Common Criteria. In such contexts, it is important to develop legislation also from a user's perspective in order to implement security and privacy mechanisms that balance the interests of state actors, companies and consumers.

Finally, as a third option, existing devices, tools, and services are connected to the Internet as part of product innovation, driven by manufacturers, often without new specific regulation being emplaced. In contrast to genuinely new products, the "sensorization" of existing products has a major difference: Consumers have already appropriated these products and embedded their use into their everyday lives; indeed, they often rely on them. While using them is ostensibly voluntary, practically speaking, consumers may have no alternative. A prominent example of such "inevitable IoT" is the connected car. Millions of people rely on their cars as a key part of their mobility, as their vehicles allow them to travel to work, take their children to school or get from point A to point B in non-urban regions. Arguably, in scenarios where using devices is non-negotiable and basically essential for everyday life in society, regulations should consider consumers' need for protection more closely. This notion is also supported by the German Ethics Committee on Connected and Autonomous Driving [80]: A recent report published by the Committee states that a purely market-driven introduction of technology, as occurred with smartphone ecosystems, search engines and social networks, should be avoided for future IoT devices that are or may become essential for users:

> *"Vehicle owners or vehicle users generally decide on the transfer and use of their vehicle data. The voluntariness of such data disclosure presupposes the existence of serious alternatives and practicability. A normative force of fact, such as that which prevails when data is accessed by the operators of search engines or social networks, should be counteracted at an early stage." [80]*

To ensure the existence of effective privacy measures for the IoT, the three levels described in Chapter 2.2 need to be put into effect collectively. These levels therefore are at the core of privacy research. This thesis addresses all of these levels by including studies on usable privacy from the areas described in the following subsections.

Table 2: Overview of selected fields of investigation, demonstrating a continuum of voluntary and obligatory adoption depending on the products' socio-historical context

	Voluntary IoT			Obligatory IoT
Selected Field	Smart home	Smartphone	Smart car	Smart metering
Ownership	Voluntary/may become quasi-obligatory	Has become quasi-obligatory	Will be quasi-obligatory	Obligatory by government
Driven by	Market	Market	Market	Legislation
IT/Privacy Protection Measures	Basic	Basic	Mid	High
Usability	Varies	High	Unknown	Low

3.3.1. Smart Metering

The German roll-out of smart meter systems is one of the supporting pillars for the implementation of the smart grid and the energy revolution [17]. Intelligent measuring systems (smart meters) record, collect, process, send and display current energy consumption data to allow intelligent management of the power grid (smart grid). In addition, they issue tariffs and control decentralized feed-in of energy producers into the grid and local energy consumption. Digital data collection offers various advantages for different interest groups (i.e. end consumers, electricity suppliers, network and metering point operators, providers of innovative energy services and society as a whole, as represented by politicians) [521]. Simultaneously, new threats are emerging, against which protection measures need to be implemented to ensure the security of supply and the resilience of smart grid infrastructure [146, 181, 363]. In addition, the operation of intelligent electricity meters poses new challenges in the area of data protection and data security.

The special need for privacy protection derives from the implemented and planned technical abilities of intelligent metering systems (a) to be able to remotely control devices in the future and switch them off if necessary and (b) to record consumption on a fine-grained basis, which allows for the development of personal or household-related behavior profiles that permit detailed conclusions to be drawn about the daily routines of end consumers [187, 267, 362,

445, 448]. Thus, the installation of intelligent measuring systems in a household will affect several fundamental rights of the respective residents simultaneously, including the right to informational self-determination, the fundamental right to guarantee the confidentiality and integrity of information technology systems and the right to the inviolability of the home [245]. Due to the potential for far-reaching invasions of privacy, there is broad agreement in the literature that, for smart meter systems, in addition to the general protection goals of IT security (i.e. confidentiality, integrity, accessibility and authenticity), the specific need in terms of data protection of ensuring the transparency, intervenability and non-linkability of organizational activities must also be considered [425].

The special need for protection is also reflected in the extensive legal requirements for the operation of intelligent measurement systems [274, 314], as well as for the storage and dissemination of data collected by third parties [267, 362, 413]. The protection profile of the BSI which was developed in accordance with the Common Criteria and technical guideline TR03109.1 should be mentioned here [314]. These regulations lay down binding minimum standards for the protection of recorded and transmitted consumption data, as well as the control and information options of the final consumer with regard to his or her data.

While the subject matter in the literature has mostly been examined from legal, technical and organizational perspectives [186, 187, 245, 267, 274, 314, 362, 423], there is thus far hardly any work that has explicitly dealt with questions concerning the usability of protective measures. User-centered security research [539, 519] shows, however, that, in practice, protective measures can lead to a reduction in the level of security if they are not suitable for everyday use and barrier-free. In addition to technical safety, it is therefore also important to consider the analysis, design and evaluation of practical safety. In this context, one frequently encounters a tension between the demand for greater safety on the one hand and greater usability on the other. Against this background, our contribution aims to formulate and evaluate the various usage and implementation scenarios when it comes to intelligent measurement systems.

3.3.2. Smartphones

Smartphones are arguably one of the most widespread devices carrying embedded sensors. In a broader sense, they can be understood as very early incarnations of IoT devices. Rapidly gaining popularity with the launch of the first iPhone in 2007, within a decade, smartphones evolved from a luxury to a ubiquitous companion in modern societies. The many sensors of a smartphone make it possible to determine its location, meaning that users of location-based services are constantly locatable. In addition, events such as key strokes, switching a smartphone's screen on or off or loading states can be used to infer activities [328].

With regard to privacy risks associated with smartphone use, previous research has employed mechanisms of IT security and privacy known from other fields on all three of the levels outlined in Chapter 2.2. PbD approaches [94, 311] and privacy regulations such as the GDPR [164] have been evaluated with regard to their potential to provide guidance for designing privacy protection mechanisms into said systems. Technical means include research into means of safeguarding privacy using obfuscation [71, 144], anonymization [196] or spatial and temporal degradation [305]. On an individual level, privacy management support is typically researched addressing questions that reflect legal requirements: (1) *who* the recipient of location information is, (2) *what* the location to be disclosed is, (3) the *purpose* of disclosing and (4) the *level of detail* [105, 385, 486].

It is also understood, however, that, in different situations involving location sharing, users may have different preferences regarding whether or not location information should be shared with others [317]. As part of said context, the physical location also carries individually and socially ascribed meaning [229]. While there are studies that acknowledge the role of contextual and situational factors in location-sharing practices, specific aspects of a particular context are typically focused on: For example, Tang et al. focused on the purpose of location sharing [487], while Patil et al. [385] and Tang et al. [486] considered the type of context in which location sharing occurs.

Another stream of research on the individual level targets consent for sharing data with providers of mobile applications, especially ways of raising awareness and and how to design effective privacy notices [33, 34, 46, 437].

In a similar vein, questions arise as to the extent to which individuals' data protection settings correspond to their data protection requirements and whether unwanted insights into the privacy of users can be obtained through consent. It is known, for example, that users are often not in a position to understand the technical (communication) connections of the Internet or to identify ways of protecting their own privacy on the Internet, let alone to explain them [272, 407]. In addition, privacy is generally assigned a higher value in theory than it is in practice [19]. Against this background, questions arise as to what extent the mechanism by which an application accesses a smartphone's sensors fits the privacy needs of users and what information needs to be obtained to achieve a better fit with the privacy practices--and thus the protection needs--of users?

The smartphone privacy study builds upon and extended the existing work of Tang et al. and Patil et al. [385, 486] by collecting real-world data from the everyday lives of participants using non-obtrusive technology. The focus, however, extends beyond location disclosure, thus widening the analytic lens.

3.3.3. Smart Home

Smart home solutions are a technology trend that is considered to hold major market potentials [461]. However, smart homes collect data from and gauge a completely new environment, namely the epitome of privacy: the private household with its ecologies and practices. Comprehensive smart home systems feature a large variety of sensing and automation technologies and can thus provide detailed insights by controlling and monitoring, for example, air conditioning, lights, windows, garage doors, energy consumption and smart appliances such as TVs or washing machines. The sheer number of sensors used in such systems offers new opportunities for and levels of detail in profiling. Many providers of smart home services offer cloud storage solutions that provide remote control over smart homes but also send private data to external parties, thus posing potential security threats to the user. From an IT security perspective, these developments are not fundamentally new but rather represent a new field of application for old problems. For HCI, however, this new arena raises questions with regard to how to design privacy-supporting interfaces for such a broad range of sensors in the large variety of intertwined and complex usage situations that households imply.

As early as 2003, Eggen et al. [150] stated in a survey on smart homes that it is crucial that people maintain control over devices and build trust in them: "Intelligence is not the same as autonomy. This means that decisions and activities are the domain of the family" [150]. Instead of acting autonomously, smart home must adapt to the living environment, contextual conditions and individual preferences of residents, which can change over time. Still, actions can be grounded in highly complex algorithms, potentially making it hard for home inhabitants to understand results. Therefore, particularly in the field of ubiquitous computing, the challenge of ensuring the comprehensibility of actions for the user is posed against the background of ever smaller, less visible and better embedded systems that are intended to act independently to a certain extent:

> *"One fear of users is the lack of knowledge of what some computing system is doing, or that something is being done 'behind their backs'. "*[4]

In distributed and embedded systems such as smart homes, in which many sensors work independently, system states can usually only be retrieved via the central software interface. This includes the provision of effective mechanisms for clarifying the data protection implications of smart home services. Most users are unaware of the consequences for privacy of sharing data measuring their households and act against their actual intentions, as various studies on the attitude-behavior gap have shown [96, 223, 466]. Providing usable mechanisms that support system state transparency for the end user could make smart home environments could lead to them being perceived as more trustworthy and understandable, thus increasing the perceived and possibly actual competence of the user.

Beyond transparency, multiple studies have shown that perceived and actual control over automated technologies such as context-sensitive or ubiquitous IT systems plays an important role in user acceptance [39, 42, 43].

3.3.4. Connected Car

In Germany, more than 46 million motor vehicles [27] covered 246.1 billion kilometers of road on motorways alone in 2018 [167].

Already today, a large number of different sensors and communication modules, as well as an Internet connection, are installed in individual premium car models. Since 2018, an eCall system that automatically dials the European emergency number 112 in the event of an accident and transmits basic vehicle information (such as position and direction of travel) to an emergency recording system has also been mandatory for new cars. In addition, service platforms will also be developed that make the data obtained from the cyber-physical systems of automobiles accessible to Original Equipment Manufacturers (OEM) or third-party providers, for example. Through the availability of continuously updated information systems (e.g., maps with additional information), which are formed by the diverse data provided by automobiles, completely new interdisciplinary benefits can be exploited.

Already identified examples of such benefits include real-time road condition data for maintenance tasks, hazard identification and automatic alerting of emergency services in the case of accidents. The opportunities offered by easily obtainable information and the new insights that result should rapidly become clear to most users. However, in addition to the loss of privacy, analysis may also lead to false assumptions regarding causality and predictions, as well as unfavorable outcomes for drivers, e.g. through profiling driving behavior for car insurance tariffs.

In order to overcome these obstacles, IT security seeks to ensure the confidentiality, integrity, availability and anonymization of data throughout the entire processing chain by either organizational or technical means [518]. In addition, the relationship between benefits and risks must be made transparent to those involved in an understandable way so that they can make their own decisions regarding the release of their data or part thereof.

Legal and scientific research in the field of connected card data is only just beginning. Thus far, it has primarily dealt with the classification of different processes of data disclosure by highlighting the differing legal implications in relation to different areas of law, such as data protection law [9], [10] and [11].

Ergonomic designs for data protection management in connected cars also contribute to increasing the security and acceptance of IT systems by making their security mechanisms

comprehensible for the user. The field of user-centered security therefore investigates aspects of the usability of software for users in order to guarantee technical security and, in practice, to resolve the alleged antagonism between security and usability [16, 538]. In particular, designing in the context of trends in ubiquitous and mobile computing [36], as well as in cloud systems [485], represents open challenges to combine usability, privacy and security due to the abstract nature and invisibility of the data colleting systems. To optimally protect consumers in their privacy practices while allowing for the exploitation of the market potential of connected car data to be exploited, it will be necessary to conduct user-centered research on privacy management in the context of the connected car.

3.4. Aligning the Publications with the Research Questions

Initially beginning in 2011, Living Lab-based research on eco-feedback, both in the smart home [255, 259, 264, 445, 447] and in office environments [261, 265], shows how users and organizations raised privacy concerns when data were stored externally. Similarly, work on a project to design IT solutions intended to support the integration of the elderly in their local communities revealed considerable privacy concerns [244]. Due to a trusting relationship between researchers and participants using the co-developed PRAXLABS approach [375], those concerns were managed successfully, and suitable ways for maintaining privacy were identified. Still, it became clear that storing energy consumption data in a university cloud or sharing data via the Internet more generally to render them accessible to users (for their convenience) and to researchers (for the development of feedback systems) was perceived as a sensitive matter.

The research agenda that was set up, followed a project-driven logic and included four phases which covered the use cases of smart metering, smartphones, smart homes and connected cars. Throughout all of these phases, the research process was generally informed and guided by the framework of design case studies as proposed by Wulf et al. [528]. While each study subscribed to the practice-based approach, they varied in their comprehensiveness and depth depending on the research question defined.

As a follow-up to the initial findings regarding the sensitivity of energy monitoring data, in 2013, a study to explore human factors in smart metering security and privacy kicked off. At

that time, in Germany, governmental agencies were in the process of defining security and privacy requirements for smart meter gateways [131, 289, 366], which are understood to be key to establishing a smart grid environment [102, 168, 169, 338, 422]. Analyzing the process revealed that in this process, the input of users was largely not taken into account, resulting in a highly unusable definition of the interfaces for using the smart meter gateway ecosystem, as described in Chapter 10. In a similar manner, Chapters 5 and 6 outline the incorporation of the user perspective in the case of connected car. Whereas the former chapter 4 is stronger focused on informing regulation of smart meters with a user perspective on privacy and usability, the latter chapter 5 and 6 present users' information demands with regard to connected cars. Taking the use case of computer-supported car sharing, the potential to improve interpersonal reputation systems using connected car data and the corresponding privacy demands were investigated [472].

To look into the appropriation of new technology and information demands, the thesis also includes a smart home appropriation study to understand hurdles to appropriation in distributed IoT devices (Chapters 7 and 8). Besides learning about limitations of ecosystems, as well as about designing user experience for hard- and software [257], also guidelines for designing feedback for lay users of embedded systems in home environments were identified. More specifically the guidelines included usability factors for designing feedback of measured data and guidelines for maintaining system intelligibility and privacy awareness in smart home environments [263].

Targeting privacy more closely, the thesis then presents a subsequent intervention study on smartphone privacy (see Chapter 9). In a first step, data from a participant's smartphone was collected over the course of several weeks using a self-deployed sensing framework. Feeding back this data in a workshop in which other participants attempted to investigate the meaning of the collected data resulted in an enjoyable approach to exploring data and increasing perceived privacy awareness for participants. It also demonstrated the crucial role that data visualizing plays in terms of increasing data literacy. Finally, chapter 10 presents a multi-staged design-case study in the area of smart metering- It was conducted to gain a detailed understanding of how users relate to abstract IoT data when it comes to maintaining their

privacy by unveiling information needs, privacy demands and ways of ascribing meaning to abstract data.

In Chapter 11, the major findings of the above studies are discussed with a focus on their theoretical and practical implications for HCI as a research field and regulative processes. Believing in the value of a more integrated perspective on privacy across levels as discussed in chapter 2.2, however, it is further argued that the findings in this thesis on designing more usable privacy for IoT can only truly put to effect if they were to be embedded in a co-depending design process involving technology, law and the user perspective, as represented by HCI research.

4. Multilateral, Accessible Security of Smart Metering Systems

The rollout of Smart Metering systems also brings a strong intrusion into end consumer privacy. This article analyses potential implementation scenarios from an explicit user perspective. To avoid the risk of a privacy divide, we propose that protective measures and regulation focus more on socio-economic aspects to promote secure, accessible, and usable mass-market solutions.

> *"The more secure a system is, the harder it is to use. The harder it is to use a system, the less secure it will be." Krause, quoted from [Krause, zit. nach 304]*

4.1. Introduction

The roll-out of Smart Metering systems is one of the pillars of the energy transition [17]. Smart Metering systems measure, record, process, transmit, and display electricity consumption data. Furthermore, they adjust tariffs and control local energy consumers and producers. Digital metering has various benefits for stakeholders (end consumers, electricity providers, grid and meter operators, providers of innovative energy solutions, and the political representatives of society as a whole) [521].

However, there are also new threats which require protective measures to ensure supply security and resilience of the smart grid infrastructure [146, 181, 363]. Smart meters also pose new challenges to data protection and privacy.

These special challenges arise from the planned and realised technical ability of Smart Metering systems to (a) control and switch off devices, if necessary; (b) perform fine-grained metering, which permits creating personalised or household-based behavioural profiles and gives insight into end consumers' daily routines [187, 267, 362, 445, 448]. Hence, installing smart meters affects several basic rights of the inhabitants at once, such as the right to informational autonomy, the

basic right to guaranteed confidentiality and integrity of information technology systems, and the right to inviolability of the home [245]. Since these are severe intrusions into user privacy, the literature largely agrees that Smart Metering systems must be subject to specific data protection requirements – namely transparency, intervenability, and non-linkability of data – that exceed the general principles of IT security – confidentiality, integrity, authenticity.

These special requirements are also reflected in the extensive regulation of Smart Metering systems [274, 314] and of third-party storage and processing of collected data [267, 362, 413]. Examples include the Protection Profile of the Federal Office for Information Security (BSI) based on the Common Criteria and the BSI Technical Guideline TR03109.1 [314]. These set mandatory minimum standards for the protection of collected and transferrable consumption data and for end consumers' rights to control and disclosure.

While the literature usually treats the issue from a legal, technical, or organizational perspective [186, 187, 245, 267, 274, 314, 362, 423], there is a lack of publications dealing explicitly with the usability of protective measures. User-centered security research [519, 539] shows that protective measures can decrease

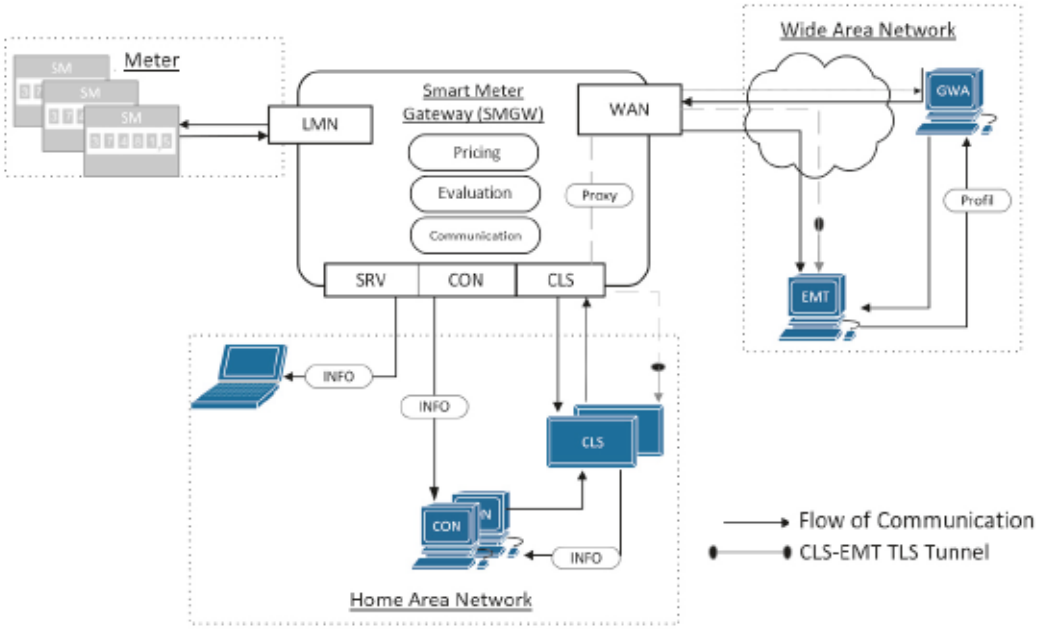


Figure 1: Simplified Chart of BSI-compliant Smart Metering Infrastructure

the security level in practice, if they are not accessible and fit for everyday use. Technical security concerns should therefore not exclude the analysis, design, and assessment of practical security. Here you often find tensions between security and usability. To develop systems that are secure in practice, not just in theory, these tensions must be analyzed seriously and without bias, and both concerns must be seen as legitimate. This article therefore aims to evaluate the various usage scenarios and implementations of Smart Metering systems.

4.2. BSI Protection Profile

The new requirements for energy grids can only be achieved by coordinating energy production and consumption and ensuring secure data transmission between all stakeholders. This will require two new components in smart energy grids: smart meters (SM) and smart meter gateways (SMGW) as central communication units. These two components are the foundation of the Smart Metering system.

The components and areas shown in Figure 1 and the security requirements for Smart Metering systems are detailed in several BSI specifications, cp. [73, vgl. 74, 75].

The SMGW is the central unit for processing and secure storage of the data produced by the connected metering systems. It is intended to ensure secure data transmission between the participants of the connected networks. According to the BSI, these network types are:

- **Local Metrological Network (LMN)**: Network for connection of local devices (electricity, gas, or water meters) of end consumers.
- **Home Area Network (HAN)**: Network for local connection and controlling of energy producers and energy consumers (controllable local systems (CLS)) in households; also serves to provide information to end consumers and technical operating staff (service technicians (SRV)).
- **Wide Area Network** (WAN): Network for connecting both gateway admins (GWA) for SMGW administration and external market participants (EMP) for data transmission.

The SMGW also works as a firewall separating these networks and their participants. In addition to this logical separation, all networks are also physically separated [74] .

The SMGW receives metering values from smart meters connected to the LMN. The main differences between smart meters and regular metering systems are that they use encryption to communicate with the SMGW and that the transmission of metering values by the SMGW can be controlled [74].

The BSI's guidelines also specify which data may be sent through the wide-area network. The BSI also defines property rights for each role. The end consumers, both as natural and as legal persons, own the metering data from their metering systems and any derivative data. External market participants are stakeholders and users of this data, since they use it for billing, pricing, and monitoring the network condition. Electricity providers are also considered external market participants, although they are usually the customer's first contact for problems and questions about metering systems. Gateway admins (GWA) usually have no access to this type of data. They receive system-relevant information, like configuration data, system logs, or calibration logs. The service technician is tasked with diagnostics and is therefore allowed to access system-relevant data. Unlike the GWA, however, the service technician may not store this data. Each participant may access the SMGW only through the network assigned to them, as shown in Figure 1 [74].

One technical requirement is that the HAN and WAN ports must be physically separated and use an Ethernet interface. Operating interfaces and accessibility options are not specified in detail. Although there are position papers implicitly requiring visualisation media [366], the BSI Protection Profile no longer requires a mandatory display unit to be provided free of charge.

4.3. Theoretical Background

4.3.1. Multilateral Security

The BSI Protection Profile is shaped by the heterogeneous actors involved in developing secure smart grid infrastructures and their sometimes conflicting interests [511] (cp. section 2). The multilateral security approach has proven itself in similar constellations [424].

Multilateral security is based on the idea that security can only be defined for particular actors and their justified (security) interests [391]. Hence, the goal is not objective security, but finding a compromise acceptable to all sides. A multi-sided security infrastructure is intended to reduce the need for mutual trust, recognise conflicts between actors, permit equitable negotiation, and enable each interest group to verifiably protect their security interests within the bounds of the negotiated compromise [391, 526]. In practice, the approach is often based on a legal, organisational, and technical perspective.

4.3.2. User-Cantered Security

The international debate is increasingly recognising the user-centred approach to security, which focuses on usability issues in security models, mechanisms and systems [539]. This approach shares many similarities with multi-sided security. But while multi-sided security takes a bird's eye view, user-centred security takes an explicit user perspective, but not without considering the socio-technical preconditions that structure human behaviour [307].

Multi-sided security has a special focus on the core security and usage requirements of various stakeholders and intends to harmonise them in the planning and implementation phases [424]. It usually highlights the tensions between the various actors' interests. A major contribution of user-centred security, however, is the focus on actors' internal conflicts of interest. It sees the user as a social subject which unites different interests that may conflict [409] (especially the internal conflict between security and usability interests). Empirical studies have shown that users often make case-based compromises

between security- and usability-focused usage practices to achieve their aims [519].

Therefore, user-centred security tries to assess the usability of security solutions, analyse the conflict between overall system security and usability, and point out viable compromises.

4.3.3. Accessible Security

Accessible security is a special case of usable – or practical – security. It addresses the issue that security measures do not just prevent third parties from accessing information and functions, but may also create new hurdles for users. This usually reduces user acceptance, and in the worst case may even reduce the degree of security in practice.

The narrower meaning of accessibility refers to systems allowing disabled people access and use in the customary manner, without special difficulty and, as a rule, without external help (cp. section 4 Behindertengleichstellungsgesetz [51]) . The wider meaning does not differentiate between "able-bodied" and "disabled," [282] but instead implies universal "design for all." So the aim is to consider the needs and abilities of all people, so that nobody is excluded from using a system due to physical, cognitive, social, or technical restrictions (cp. ISO 9241-171:2008).

This wider sense of accessibility means that users, regardless of their disability status, can pursue their security interests and needs in their everyday lives without external help or additional technical measures. This definition adds a specific, internal user perspective to the general demand of multi-sided security.

4.4. Scenario-Based Analysis

With regard to multi-sided security, we are first looking at the usage scenarios and the (justified) interests of user groups. These interests must be balanced on the basis of the data protection principles of purpose limitation, necessity, and consideration of data subject rights [267, 274, 378, 423, 425].

4.4.1. Usage Scenarios

Billing and Variable Tariffs

Automatic meter reading for consumption-based billing is an important usage scenario [186]. However, it does not require fine-grained consumption data.

This need will likely arise only as controlled load or time-of-use tariffs emerge due to rising volatility on the electricity market. Promoting such tariffs makes sense for the general economy, since they can increase overall grid efficiency by optimizing the rate of electricity production to consumption. End consumers also benefit, if cost optimization leads to cheaper tariffs. There is also a data-saving solution without fine-grained usage data transmission: If the electricity providers' latest tariffs are stored on the device, each smart meter can perform its own decentralized tariff adjustment [187]. This will make it enough to transfer personalized consumption data only once per billing period.

Remote Controlling and Remote Shutoff

Smart Metering systems will allow remote controlling of systems and devices and targeted disconnection of meter points from the grid. This results in two major usage scenarios from an electricity provider's perspective:

In the first, dynamically optimized controlling of producers and consumers will avoid peak loads and allow activation and deactivation of decentralized electricity producers on demand. Similar as with controlled load tariffs, end users may benefit, for example, by charging their electric vehicles when the price of electricity is lower [363].

The second scenario permits fast remote disconnection of late-paying end consumers from the grid [363]. Hence, Müller [364] demands that end users retain control over remote control and disconnection. However, it remains vague, how less tech-savvy end consumers may properly and effectively exercise this control while ensuring sufficient protection against unauthorized third-party access.

Smart Grid and Production Management

Electricity providers are also interested in fine-grained consumption data because, compared to standard load profiles, it allows more precise forecasts. This would allow optimized grid feeding and minimize risky short-term purchasing from the energy exchange [186, 362]. Creating reliable consumption curves, however, does not require that data be assignable to individual households [363]. Mass data collection would also be unnecessary, as anonymized data samples would be enough [187]. Various technical approaches to anonymization have been proposed, for example, using collectors [388] or group signatures [363]. As a compromise between consumer and supplier interests, Müller [362] further proposes a smaller temporal resolution of metering data and aggregation of intermediate values and data from multiple households. Smart Metering systems also allow closer monitoring and management of the distribution grid's condition. Metering values at local substations seems sufficient [378], but this aspect has not been researched much.

Consumption Feedback

This is currently the largest incentive for consumers to use smart meters [479]. Feedback allows them to learn more about their consumption, to better control it, and to identify potential savings [445, 448]. Studies show that savings of 5-15% are possible [124] – this also motivates legislators to promote a broad roll-out of Smart Metering and more conscious energy consumption [17]. Effective consumption feedback should support real-time visualization, comparative consumption display, and a detailed reconstruction of users' consumption behavior. This places high demands on fine-grained real-time collection, processing, and storage of data over extended periods. It also creates a tension between effective consumption feedback for research purposes and data minimization for preventive data protection. The literature prefers a local solution for consumption feedback to ensure transparent data protection [187, 362, 378]. The consumption data would remain on the end consumer's device and not be sent to third parties [187]. Ideally, the data should also be processed and visualized

using free software to avoid dependence on commercial providers and to verify data protection compliance in the source code.

4.4.2. Implementation Scenarios

Each usage scenario comes with a list with technical and organizational measures to ensure that data protection and other interests are ensured to various degrees [424].

From an end consumer perspective, the protection measures should not restrict the benefit provided by the consumption feedback. As stated above, this creates a tension, which will not easily dissolve in the future. Therefore, we need viable compromises under the current social and technical conditions. In the following, we analyze several derived usage scenarios.

Electricity Provider's Proprietary Portal

In this scenario, the end consumer can access consumption data through the electricity provider's portal. This scenario is similar to the YelloStrom solution: "Customers receive new meters which record consumption by the second and transmit it to headquarters every 15 minutes over the Internet. Users can access their data on the YelloStrom website" [313]. One problem is that users must trust in the provider not to abuse their data. The data also needs to be sent through the public Internet, which has more risk exposure than local data transmission.

Despite these drawbacks, the portal solution has the significant advantage that most people have Internet access, so that after closing the electricity contract, end consumers can directly see their consumption data in the portal without any additional costs or hardware. Yet, according to the Federal Statistical Office, a quarter of all private households had no Internet connection in 2011. So an accessible alternative access point is needed in order not to exclude this group. The usability and accessibility of the portal also depend on its actual implementation. For example, the Accessible IT Ordinance (BITV) or the guidelines on website accessibility (WSAC 2.0) should be observed [282].

Another restriction for users is the risk of vendor lock-in [307] in proprietary IT solutions. Although the data legally belongs to end users, they remain tied to the vendor and cannot freely store, process, visualize, or share their data.

In summary, the proprietary portal solution offers the least degree of data transparency compared to other scenarios. In particular, users have no influence on the protection of their security interests and no way to trace or control the use of their data. Usability depends heavily on the specific implementation, but can generally be rated as medium to high, especially if mobile device visualization of consumption is supported. The solution also offers good accessibility, if the user has Internet access (which is not always the case). In this case, installation efforts and additional costs would be negligible.

Standardized Smart Energy Cloud Services

Standardized cloud services are one alternative to proprietary portals. Here, end consumers send their recorded consumption data to an external provider of their choice for evaluation and visualization according to their wishes. These services can be provided by commercial providers (e.g., Verivox, Google, Facebook), non-profits (such as Stiftung Warentest), or governmental institutions (e.g. Energy Agency, Federal Statistical Office). Services can range from simple consumption feedback to personalized comparison portals to new, smart electricity services.

In terms of technical security, the provider portal solution and proposed cloud services share many similarities (e.g. data transfer over the Internet.) However, the cloud solution would require sending of private data to previously unauthorized providers. This requires additional measures for transmission and storage and causes new security issues.

Furthermore, cloud services raise new consumer concerns about specific use, especially to what extent private data may be shared with third parties for non-restricted purposes. Some secondary use scenarios for big data are already based on non-restricted sharing of data [341]. Information asymmetries between providers and users make this particularly problematic, since users can hardly

estimate the consequences of their decisions [20]. A related issue is the case-based distinction between desirable information (such as ways to save energy at home) and unwanted advertising (such as information about savings with the intention to sell energy-efficient refrigerators).

Consent-based sharing of data is crucial, as it would allow end consumers to decide – at least formally – whether to trust a provider and to protect their justified interests. The BSI Protection Profile covers cloud services as "external market participants." However, it should be considered whether the different services should be standardized further and placed in separate categories of purpose and protection. This would increase transparency and allow end consumers to make more informed decisions. There should also be standardized data formats and protocols for the individual categories to minimize transaction costs when users switch providers (due to changed terms and conditions or privacy policies, for example).

Another issue is free access by external market participants. Here there is a latent conflict between the wish for a broad range of third-party solutions and protection of individual end consumers and the meter operators' overall infrastructure. There is a danger of the metering infrastructure provider citing security concerns to exclude unwanted competitors.

Transparent rules and protection requirements are needed to verify when it may be justified to exclude a provider and to ensure free market access. The key goal should be to enable end consumers to make free and informed decisions about what happens to their data and for which purposes it is shared.

Since cloud scenarios are very complex and their implementation is often still unclear, it is hard to make a general assessment. However, this scenario is likely to share some similarities with the provider portal solution, which is why we are focusing on the differences. For example, the additional parties involved are likely to reduce the overall level of data security. Yet, the choice between various providers should increase end consumers' informational autonomy. It can also be

expected that the wide reach and usability expertise of large software producers like Google will result in their cloud services offering good overall usability. Accessibility will depend strongly on external market participants' infrastructure. A major factor will be, if finding and installing suitable services is as user-friendly as in the Android Marketplace or the Apple App Store. Since the software solutions would be cross-funded by advertising and similar means, additional costs for end consumers should remain low.

Single-Purpose Display

The single-purpose display visualizes energy consumption data locally, so that the data does not have to leave the end consumer's location. The display can either be integrated into the smart meter's housing, a smart gateway, or an external display, which is installed in the home.

The local display offers high technical security by design. The single-purpose display can also be customized to provide user-friendly and accessible consumption feedback. However, it does have some drawbacks, such as higher costs for development and production costs for Smart Metering systems. Version 0.9.2 of the BSI Protection Profile made an integrated display mandatory and required manufacturers or operators to bear the costs [364]. However, these rules were dropped from later versions, so the higher costs would now be passed on to end consumers.

Another drawback of integrated displays is that meters are usually installed in the basement with varying ease of access. The practical barrier of accessing the information adds to the financial one. This would also undermine the politically desirable effect of giving users a steady overview of their (energy) consumption behavior.

Stationary or mobile single-purpose displays do not share this drawback, but the financial barrier remains. Overall, a single-purpose display would offer the greatest data protection transparency among all the scenarios. However, a display installed in the meter would not be usable. Good-quality mobile or stationary

displays would not have this drawback. They would also be the most accessible choice, because they require no internet access and, if properly designed, could be used by non-tech savvy users or people with mental or physical impairments. One big drawback are the high extra costs for end consumers, which exceed the costs for the other presented solutions.

Home Energy Management System (HEMS)

As an alternative to single-purpose displays, data could be displayed on existing home display devices (TV sets, PCs, tablets, smartphones) [364]. Since these display devices are not directly connected to the Smart Metering system, the data must be securely sent to the end consumer's home/device, as in the single-purpose display solution. Here there are several scenarios:

Today's smart electricity meters have an Ethernet port, which, though unsecured, makes consumption data accessible. In the future, SMGWs are intended to have an Ethernet port, which allows encrypted and password-protected access to the HAN interface. Here, too, it is the end consumers' task to download the data to their home network. In a Living Lab with seven households, we were able to transfer the data from the basement to the apartments using power line communication (PLC) [9].

Apart from the extra costs, there are other practical problems specific to multi-party homes: Overlaps with existing PLC modules (such as baby cameras) may create issues that require technical knowledge about the devices. Most of all, however, the PLC adapter in the basement needs an accessible wall socket that is connected to the end consumer's electrical system.

As a second variant, the SMGW could provide the data not just via Ethernet, but actively transmit it into the home network. Integrating the transmission function greatly reduces costs and work for end consumers to connect the smart meter to their home energy management systems (HEMS). Technically, both wired and wireless transmission are possible. Wired transmission would be possible by integrating a PLC adapter into the SMGW, for example. This would also avoid

the communication and security issues of wireless solutions, such as HAN interface attacks through wireless signals. PLC also permits transmission of data from shielded meters or outdoor meters, which in our experience tend to be the rule rather than the exception.

From a technical and financial perspective, WAN and HAN could use the same PLC adapter, even if the BSI Protection Profile does not offer this option for security reasons.

For this implementation, however, it must be ensured that no data sent through the HAN interface can be accessed over the Internet.

To prevent proprietary island solutions, the related file formats and transmission protocols must be standardized, especially to avoid vendor lock-in. It would also promote the medium- to long-term development of a market for routers, smart TVs, set top boxes, etc., which would give users plug & play access to their real-time, local electricity data. Here the same HAN protection measures from the BSI Protection Profile must be implemented for authentication, encryption and authorization.

Overall, the HAN interface shares many security features with the single-purpose display. At a closer look, it has two variants: "data transmission via Ethernet interface" and "data transmission via integrated PLC adapter". The usability of both variants depends heavily on the provided third-party software, which is likely to be of high quality, if we look at cloud services. Nevertheless, third-party software opens the door to data abuse. However, abuses would be easier to reveal than in the cloud scenario, since the data would be stored and processed on third-party servers.

The practical barrier for feeding data into the home network and the incurred costs are a major difference between these solutions. In our experience, the Ethernet interface comes with high barriers and with medium to high costs due to the additionally required hardware adapters. The integrated PLC adapter, however, will likely cause few additional costs, because HEMS devices with plug & play

will probably become established in the medium to long run. However, these benefits come at the security-related cost of the PLC adapter having only a logical, not a physical separation between the HAN and WAN interfaces. Still, data protection transparency is higher in the case of local transmission via PLC adapter than in the case of data being stored and sent through the public Internet.

Table 3: Preliminary assessments of smart metering implementation scenarios. A more reliable assessment would depend on the actual implementation and must be case-based.

	Transparent Data Protection	Usability	Accessibility	Costs
Proprietary portal solution	Low	Medium-high*	High	Low
Standardised cloud services	Low-medium	High*	Medium-high	Low
Single-purpose display	High	Low-medium	High	High
Local Ethernet data transmission	High	High	Low-medium	Medium-high
Integrated PLC adapter for local data transmission	Medium-high	High	Medium-high	Low-medium

** if real-time feedback supported*

4.5. Discussion

A wide, mandatory roll-out of Smart Metering systems brings a strong intrusion into end consumer privacy [245]. This is why YelloStrom won the 2008 Big Brother Award. Ever since, the privacy and security discussion and regulatory measures have significantly improved the situation. One important outcome is also reflected in the BSI Protection Profile, which states that end consumers must continue to have secure and privacy-friendly alternatives for receiving electricity consumption data. Our analysis shows, however, that various decisions result in a trade-off between security and usability (cp. Table 3). We also see a tension between security and costs, which we will address in the following.

4.5.1. Privacy Divide

The tension between protective measures and costs bears the risk of a privacy divide. This term is deliberately based on the digital divide, which refers to access to information and communication technology being unevenly distributed and strongly dependent on socio-economic factors. We see a similar tendency in digital security technology, due to access and use being increasingly influenced by socio-economic factors. As a rule, the decision whether or not to use security measures is cost-driven [199].

Due to the increasing importance of digital privacy, we see this divide not just as a personal problem, but also as a threat to our democratic society. Considering how far smart meters intrude into our private sphere [245], it should worry us that usable security is only realizable at a high cost to the end consumer. Under these circumstances, we fear that less secure WAN-based solutions will win the mass market. Although officially there are alternatives, in practice, only a small segment of wealthy, educated, or technophile users will (be able to) use HAN-based solutions.

There have been voices in the debate around the digital divide, which demanded accessibility for all [1]. We can formulate three demands for accessible security in Smart Metering systems to avoid the privacy divide:

- The user interface should comply with BITV and/or WSAC 2.0 Level III standards. This also includes the information users need to make informed security decisions. The information should be presented in a language and form accessible to users, which should not exceed the basic secondary education level [282].
- Additional costs to end consumers should be considered in the development of protective measures [1]. It should also be evaluated if the added security justifies the added costs.
- The security measures should integrate into users' everyday routines to avoid practical barriers [479]. Local displays integrated into smart meters, for example, meet high security standards, but lead to an unjustifiable loss of overall usability.

4.5.2. Regulatory Measures

Right now, how to access data is left mostly up to users. There is no regulation on the design of the user interface. There seem to be no efforts to also make the Barrier-Free Information Technology Ordinance (BITV) mandatory for Smart Metering systems (for example, by adding a clause guaranteeing end consumers barrier-free access to their data.)

This lack of regulation grants SMGW manufacturers, operators, and buyers a lot of flexibility to agree on their own solutions in response to technical developments. The legislature is thereby meeting its duty to ensure the highest possible degree of technological neutrality. However, this bears the risk of operators and manufacturers sacrificing end consumers' accessible security interests to cost considerations. The BSI Protection Profile may have the opposite of its intended effect. Unlike 2008, end consumers now have the formal choice of accessing their data locally without first sending it to third parties. This formal choice allows critics of the German data protection regulation to frame low user acceptance as a free, individual decision. However, this conceals the socio-economic context and disconnects the challenge of privacy-friendly Smart Metering from the critical, political debate around security and privacy.

Therefore, we suggest some more regulation of the HAN interface, in order to ensure usable privacy for the masses. In particular, the SMGW should not just share data through the Ethernet interface, but also through the HAN. The PLC could be a good compromise between technology neutrality, usability, and technical security. The alternatives discussed in this article are mutually non-exclusive and blend in with the existing regulation. Although technical security would be slightly below the current requirements (cp. Table 3), the improved local acceptance would probably increase the average degree of security on a mass scale.

4.6. Conclusion

This article has shown that secure Smart Metering systems should not be seen as separate from usability and accessibility. From a user perspective, security

measures should not interfere with the benefit of direct and informative consumption feedback. Practical barriers and additional costs should also be considered, if data protection and security are to be more than promises on paper. Here our analysis has identified the threat of a privacy divide, which should find more attention in the political debate around IT security and smart data.

5. Privacy by Design for Connected Cars: Available Architectures from a Consumer Perspective – a User-Centered Discussion

There is currently a great need for design and regulation in the Connected Car Cloud, as underlined especially in the report of the Ethics Commission on Automated Driving set up by the German Federal Ministry of Transport and Digital Infrastructure. Unresolved questions also have far-reaching implications for driver and passenger privacy. Yet, the consumer perspective is underrepresented in the current debate. Therefore, this paper analyses infrastructure decisions from the perspective of consumers and other stakeholders, looking especially at expected effects on service quality and data protection.

5.1. Introduction

While self-driving cars have been a staple of futurology and science fiction writing, the industry has only begun in recent years to define concrete strategies to make this vision come true. Facilitators include the advancing miniaturisation of information technology, sinking hardware prices, as well as advances in machine learning [471].

The terms "Connected Car" and "autonomous driving" are often seen as one and the same technology. While it is true that Car2Car or Car2X communication can support autonomous driving, there are other data services apart from self-driving vehicles that offer promising market opportunities. Any regulation should therefore consider alternative usage scenarios right from the start.

While the mandatory eCall function adds a degree of connectivity to all new cars, companies are also offering upgrade kits (Pace, TankTaler) that plug into the mandatory OBD II service interface of older models. Typical services include vehicle logbooks, fuel consumption optimisers and trackers, service station finders, and similar geodata services, or telematics-based insurance plans. These

services analyse various parameters of a driver's behaviour, such as kilometres driven, braking action, hours driven (day/night), or similar. This vehicle-specific and user-specific data is sent to the cloud of the relevant service provider, either through a SIM card in the OBD plug or using a smartphone with Bluetooth tethering.

The Connected Car is a vision that promises to integrate such services into every vehicle. Of course, cars are not the first everyday device permanently connected to the Internet. Smartphones started spreading around 2005, while smart meters for power usage metering were made a mandatory target for 2022 in Germany, as in many other countries [131].While legislators did not develop any data retention requirements beyond the GDPR for smartphones [164], they did so for smart meters. After discussing various options [473], the German federal government decided to set up a neutral agency to manage the collected household data. The Ethics Commission on Automated Driving has now given some initial suggestions on how to ensure data protection in Connected Cars [80].

Legal implications of the Connected Car concept on autonomous vehicles [234] and Car2Car communication [286] have been studied, and "privacy by design" [224] has been demanded as a remedy. But while security technology [302] and legal questions [77] dominate the debate, consumer information concerns are often neglected. It therefore seems appropriate to discuss various infrastructure models from a consumer perspective, how data collection in Connected Cars could look in the future, and the implications for data & service quality, passenger privacy, and data protection.

5.2. Data protection in Connected Cars

In June 2017 the Ethics Commission on Automated Driving presented a catalogue of guidelines especially for developers of self-driving cars [80]. It discusses classical dilemmas, sources of discrimination, as well as damage to objects, people, and animals from accidents with self-driving cars. Finally yet importantly, it points out that cars of the future are machines that collect and may disseminate private data. Once stored, this data may be used for purposes that may not even

be foreseeable right now. In principle, data could be used for applications with or without personally identifiable information. The first could be used to calculate personalised insurance contributions, while the second could be used in anonymized crowd sensing applications to detect potholes.

The enormous success of Alphabet (formerly Google), thanks to its integration with the Android mobile operating system, has alerted stakeholders in the automobile market to the high value and possible exploitation of vehicle data. Currently available upgrade solutions typically demand far-reaching permissions to analyse the collected data. Various research projects are already testing cloud environments, which usually follow IT security approaches to protect consumer privacy.

Should the Connected Car become established, it begs the question which view consumers have on the processing and storing of their personal data, but also to which extent consumers are able to understand the personalised nature of their abstract data collected by the car. This is no easy task, as shown by existing products for the so-called Internet of Things, such as smartphone data transmission [33, 481], or studies on information demands in Smart Homes [258].

In addition to concrete tools that allow consumers to protect their privacy when using IoT devices, the underlying system architecture of Connected Cars also matters. How to ensure that consumers can make their own informed decisions which data to share? Under this aspect, who should primarily manage the data? Which data should be transmitted at all? How can system architectures integrate the privacy by design principles stated in the General Data Protection Regulation (GDPR) [164]?

These are topical questions, since car manufacturers are working hard to establish Connected Cars, and a solution acceptable to consumers is needed. The report by the Ethics Commission pointed out that a situation similar to the rapid advance of smartphones should be avoided. This development had taken legislators by surprise and was left mostly to market forces [80].

Smart Metering is an example of a technology whose introduction in Germany was not left to the market [473]. Meters are officially considered a critical part of the infrastructure, which needs extra protection, especially against cybercrime. Therefore, they were subjected to additional security and data protection requirements, which benefitted consumers. The measures include creation of the "data trustee", an additional market player who stores electricity consumption data in a professional, secure cloud, where consumers can decide which other recipients may use the data.

Considering this continuum from market-driven to highly regulated connections of infrastructure to the Internet, this article discusses possible architectures for a Connected Car cloud. Factors include the degree of data protection, usability, non-discrimination / accessibility, and costs to consumers. For each scenario, we study the implications for the data economy surrounding Connected Cars.

This helps give an overview of current developments and available Connected Car technologies. We also want to highlight consumer interests in data control and the usability of cloud solutions for providing value-added services.

5.3. Discussion from a consumer perspective

This section reviews the four presented solutions for data storage in Connected Cars for exploitability by third parties, usability of services, and data protection options.

5.3.1. In the Vehicle

Cars often come pre-equipped with so-called event data recorders, for example, in airbags. Voluntary black boxes are also available, as insurance companies have recently introduced pay-as-you-drive plans [450]. One user benefit of keeping the black box inside the vehicle is that the data stays in the car instead of being sent to an external storage. This means that only vehicle owners have initial access to the data, which significantly lowers the risk of hackers accessing it. One drawback of black boxes is manipulation by users. It would need to be ensured that the owner of the vehicle and the black box could not easily delete data to conceal events from

the police or insurance companies. Data services could be provided in a way similar to smartphones, by downloading modules that use external data to the car. The vehicle data would not have to leave the car. Limited storage and computing power in the vehicle and the costs for upgrades are one current challenge. On the other hand, data services do not require much bandwidth, and only anonymized data would need to leave the car. Configurations could be stored online to economize data. However, ensuring backups and data synchronisation when users change vehicles remains a challenge.

5.3.2. In the Car Manufacturer's Cloud

In a cloud solution, however, the data is not stored in the vehicle, but transferred wirelessly to an external storage. Users have access to the manufacturer's ecosystem and can easily register for and use authorised services.

Automated backups and changing vehicles should also be easy, as long as the manufacturers ensure interoperability. If not, it could lead to vendor lock-in. In any case, this approach would not permit service users to choose which cloud system to use, as it would be tied to their brand of car. This bears the risk of manufacturers covertly undermining data avoidance and data economy rules and thereby the privacy by design principle. The upload by default approach also permits easy exploitation by manufacturers and third parties. By consenting to the cloud provider's terms of use, consumers could risk ceding far-reaching rights. This option also requires high data throughput. On the other hand, users would not have to pay for this service. As established in smartphones, the vehicle's usage data would be the means of payment.

5.3.3. In a Cloud of the User's Choice

The prerequisites are similar as for In the Car Manufacturer's Cloud5.3.2, but with higher freedom for consumers. The argument could be made that more choice of providers allows consumers to better adjust services to their needs. The services could also be connected to other offers and personal data, which would improve customisation. Although usability will likely be high, the problems of the manufacturer cloud scenario remain: liberal data transmission and a resulting

lower degree of data protection. This could be changed if there were cloud services explicitly offering better data protection. However, these providers would require significantly higher payments by consumers. This scenario also leaves unanswered who pays the costs of data traffic; these might be passed on to the consumer. However, the argument could be made that not offering access would be a competitive disadvantage for the manufacturer, and therefore the market would regulate this issue.

5.3.4. In a Trustee Cloud

One variant for storing personal consumption or usage data is the so-called data trustee model, which was intended for Smart Metering. In this scenario, the cloud is hosted by a third party, ideally the state or a trusted institution. They should not follow a profit motive, or at least be required not to analyse the data. Consumers can grant authorisations to third-party providers, who can then access the trustee's database.

Here, the architecture would not undermine the privacy by design principle, and privacy would be subject to the wishes and needs of the consumer. The trustee could function as a reliable intermediary, especially for those services requiring only anonymised data. Usability would be comparably high, as in the free choice of cloud scenario, and possibly even higher, if there is only one trustee. In this case, users would not need to select a provider, and the car could come connected to the trustee. As long as manufacturers pay for data traffic, there would be no costs to consumers. A standardised interface for all manufacturers could ensure high safety standards for communication and reduce development costs to service providers. Anonymised or synthetic data could also be freely provided to developers in order to promote innovation. Regarding data protection, this solution ranks just behind the local storage scenario, since cloud architectures are structurally more vulnerable to attacks.

5.4. Assessment of the Architectures

The individual factors of each option must be assessed according to data protection, security, and costs to manufacturers and consumers (Table 1).

Maximum data protection requires minimum storage of data. However, only double storage at separate locations can ensure maximum protection against unauthorised access and deletion. The Internet is especially full of attack vectors. However, offline storage, while offering maximum security, also raises costs. As the most viable alternative, cloud storage must ensure adequate data protection. Local storage would also make it difficult to guarantee the authenticity and integrity of data, since the storage medium would need to provide a physical interface. All cloud infrastructures, however, will send high data volumes through mobile connections.

If privacy by design is taken seriously, and the technical and organisational measures are observed – which according to the GDPR must be state-of-the-art – cloud infrastructures provided by manufacturers or free market participants would have difficulty meeting strict data protection requirements. Such infrastructures undermine informational autonomy "by design". If data is "shared by design", i.e. uploaded into a cloud, even the best safety measures will not protect consumers against unwanted, albeit legal, profiling.

Table 4: Preliminary assessments of connected car implementation scenarios. A more reliable assessment would depend on the actual implementation and must be case-based.

	Data protection	*Usability*	*Accessibility*	*Costs*
In vehicle	+ +	+ +	-	- -
In car manufacturer's cloud	- -	-	+ +	+ +
In cloud of user's choice	-	+ +	+	+
In trustee cloud	+	+ +	+	+ +

On the other side are social and political expectations of extracting additional value from data and hence using it for commercial purposes. Therefore, each option has its pros and cons. To satisfy all interests, any solution would have to be a compromise. Data management by a trustee seems to be the means of choice to find a balance between data protection, exploitability, and usability. It offers an

open platform, but can also protect consumer interests and give them control over the services to share their data with. The Ethics Commission recommends that the government should play a central part in designing the trustee role.

5.5. Outlook

Much will depend on the implementation of the GDPR and whether and to which extent legislators see a specific need for regulation (as demanded by the Ethics Commission). The challenge, however, is not legally compliant data storage, but consumers having no alternative services to choose and curtailment of their informational autonomy, unless data protection-friendly solutions are provided. The discussion around users' data ownership and their exercise of property rights will also be futile, if data usage rights are hidden deep in providers' terms of use, as often seen in other areas.

The state's active role in the development of the automotive cloud will help protect user data and produce an infrastructure that offers lower costs for manufacturers, usability for consumers, and innovation-friendliness for developers.

Furthermore, this article presents an example where the regulation of an IT infrastructure explicitly considers consumer interests. This matters, because the basic degree of data protection will be hard to change after the infrastructure is set up. In our view, usable and future-proof infrastructures require that the consumer perspective also join the dialogue between technical security and legal reliability.

6. Second Dashboard: Information Demands in a Connected Car

Traditionally automotive UI focuses on the ergonomic design of controls and the user experience in the car. Bringing networked sensors into the car, Connected Cars can provide additional information to car drivers and owners, for and beyond the driving task. While there already are technological solutions, such as mobile applications commercially available, research on users' information demands in such applications is scarce. We conducted four focus groups to uncover what kind of information users might be interested in to see on a second dashboard. Our findings show that besides control screens of todays' dashboards, people are also interested in Connected Car services providing context information for a current driving situation and allowing strategic planning of driving safety or supporting car management when not driving. Our use cases inform the design of content for secondary dashboards for and especially beyond the driving context with a user perspective.

6.1. Introduction

The classic focus of the automotive HMI is on design of in-vehicle interfaces. The aim is to inform the driver more effectively, providing ergonomic control and car-assistance systems matching humans' physiognomy and mental models to improve road safety and relieve drivers [203, 365]. In the last years, car experience design became a vivid research topic asking how to provide positive in-car experience to improve the quality of time e.g. by entertainment systems, in-car gaming or promoting social interaction [22]. In this vein, also innovative modes of interaction are researched [393]. The technological and societal progress towards Connected Cars offers new possibilities for automotive HMI [482].

Making a car a *Connected Car* is typically understood as a way of enabling car-to-car or car-to-infrastructure communication. Apart from new cars coming with such functionality, there are also upgrade modules / hardware to provide a remote access for current and older cars [35, 107]. Mostly they use the OBD/CAN interface to access vehicle-specific data. In addition, such devices often have GPS

and accelerometers to provide additional data on car movement and position [23]. Similar to what is planned for cars connected by default, data is then transmitted via GSM or LTE to be processed in a backend and finally visualized on common consumer devices.

By connecting the car and its multiple sensors to the internet, it becomes a cyber-physical system in the hand of non-experts, similar to what Smart Home systems. Research shows, that such systems both provide means for improved management capabilities and knowledge about self-behavior, but also spark a need for awareness, such as for setting levels of privacy [258]. Given that the Connected Car will soon be the default for newly built cars, we similarly expect that today's in-car dashboards will not be able to – and from a security and driver distraction point of view should not – display all data of interest to car owners. Instead, a second screen could extend the primary dashboard and provide additional car-related information. Similar to dashboards provided in Smart Homes or the second screen concept in media research, where users can receive additional information about a TV program via other devices [237], we define a second dashboard as follows:

> *The second dashboard is a device or application that allows extensions of the primary automotive experience on a second screen (e.g. smartphone or tablet).*

Whereas there are technological and market-driven commercial solutions such as smartphone applications available, research on what information users believe a Connected Car should provide, is scarce. We therefore conducted a user study to gain insights on how a second dashboard could support car owners in driving itself and make use of digitally available car data otherwise, such as improving car management or reflecting on their (driving-)behavior.

6.2. Designing for the Connected Car Data

Automotive UI is a research field, which investigates efficient visualization of relevant data for drivers [441]. Research in this field typically aims at choosing and visualizing data in a way such that distraction from driving and thus potential

dangers for road users is minimized [394]. At the same time, HMI [283, 441] and interaction modes [393] in the car are targets of current research efforts.

In recent years, this challenge grew by a manifold of sensors, which are positioned in cars in the light of providing new features for drivers. More recently, manufacturers have started to put efforts in connecting the local sensing infrastructure within a car to a cloud backend [220]. The so-called "Connected Car" is not only foreseen to improve manufacturers' knowledge on car or vehicle parts performance [50], it is also often connected with the promise of autonomous driving, car-to-car and car-to-infrastructure communication becoming possible [200]. Also, from a technological point of view, cloud-based platforms for car data are researched [50, 220]. The user largely profits from gaining higher comfort and security of driving by e.g. navigation services, automatic lane keeping, adaptive cruise control or other driver assistance systems [299]. Research also investigates the potentials of integrating context information into HMI [392].

In light of increasing data visualization and potential distraction, Automotive UI seeks for an answer for the increasing gap between the visualization of potential and actual data [210]. Similarly, extending the car dashboard with nomadic devices when driving or integrating them into in-vehicle information systems is investigated from a technological perspective [465]. For example, Kranz et al. built a tool to improve driver awareness via car-to-car communication [301]. Nomadic devices are also investigated to find out of how users can benefit from such devices in the Connected Car [312].

Designing for informing drivers beyond the actual driving task itself, however, has gained far less attention so far. Several manufacturers already provide mobile applications for their cars, such as the "BMW CarData", the "Mercedes me" or Volkswagens "Car-net" portal. However, the "Second Dashboard" lacks a systematic research of potential benefits from a user perspective: What would users want to know from their car? What do they need for handling a Connected Car? What do they envision to gain from car data becoming available to them? These are the questions, we turned to in our user study to better inform and

motivate the design of applications extending the primary dashboard in Connected Cars.

6.3. Methodology

The aim of this study was to explore what information might be useful while using a second dashboard in general. Therefore, we conducted four focus group interviews as a well-established methodology for exploratory research to obtain as wide a range of responses [342]. Each focus group interview lasted on average about 30 minutes, based on the following script:

In the first phase, we as moderator introduced the topic Connected Car and the second dashboard. Then the participants were asked to write down on cards their ideas, information needs, and requests that might be of interest to them. To stimulate the discussion, the moderator gave some examples of possible ideas. Sometimes these ideas were taken by participants and inspired them to elaborate own ideas. This kind of trigger was often necessary as most participants had no relation to the Connected Car concept, some of them do not own a car, or rarely drive a car. In the second part, the cards were presented and discussed among the participants. In the last part, participants were asked to group cards that are closely related from their perspective. We asked them to give each group a title that summarize common issues and give it an expressive name.

The focus groups were quite heterogeneous in terms of age and gender. The age ranged from 24 to 57, with the majority of participants between 25 and 30 years old. The selection of the participants was deliberately chosen to be younger due to the high affinity to mobile devices. We interviewed participants with a different intensity of car usage and different household situations, meaning how many people live in a household. The car usage reached from several times a month to daily use and we interviewed people who live alone and up to four people in the household, this is particularly interesting in terms of car use or sharing and opens up new demands for Connected Car services. The mentioned ideas and categories were often similar and largely matching each other. This indicates a kind of data saturation [205] – even if the mentioned list of ideas and information needs is

certainly not exhaustive. To achieve a common category scheme with a greater interpretative strength, we comparatively analyzed and joined the results of all focus groups. This analysis was guided by the qualitative content analysis methodology [342].

6.4. Findings

Our analysis reveals a set of information themes as well as presentation themes. Information themes are about the content our participant mentioned in the focus group interviews, means the information they would like to see on a second dashboard on i.e. their smartphones. Presentation themes are about how the information should be presented, means how can specific types of information be presented to the consumer, how they can be visualized and how can the car relevant data be combined with other applications.

6.4.1. Information Themes

Defective Parts

An important theme often mention by participants was the desire to get informed immediately about vehicle defects or damages similar to existing car warning displays. In addition to the single information that something is broken, some participants suggest to get more information about the problem, the severity, and how it could be repaired. Concerning this, various options were discussed, how a second dashboard could support the *car repair literacy* e.g., by giving clear instructions for repairing the car by locating and giving detailed information about the defect part (e.g., with pictures, videos, and text), providing recommendations for buying or changing defect or wear parts. In addition, it was seen as helpful when information about spare parts, repairers, and approximate cost of the repair was provided. A recurring issue was that such information helps to feel safer driving a car and to save money by self-repairing.

Wearing Parts

Another often-mentioned theme was to get informed about vehicle components that are wearing off substantially when driving. In contrast to defective parts, they are not broken, but taking an eye on them is important for two reasons: (1) Legally

binding safety requirements, such as a minimum tire profile, and (2) wearing components such as brake discs must be fixed or replaced in future.

Currently, the wear condition must be checked manually and periodically, on suspicion, or on certain upcoming occasions, such as longer drives. In future, most participants perceive it as an advantage, when the conditions are checked automatically to display the information in the second dashboard. Besides the tire pressure, participants mentioned the condition of brake discs, clutches, spark plugs, starter, wipers, and level of oil, coolant, and washer fluid.

Being informed when to replace, repair, or refill them *before* a defect occurs, could help to avoid both stress and potentially repairs that are (more) expensive caused by collapse of one component while driving or prevent dangerous driving conditions. The primary demand of most participants was therefore a second dashboard to provide drivers an overview of the current state and evaluate the vehicle condition without having to rely on expert knowledge. Especially for older cars, such information was mentioned to increase the perceived safety of the driver. Overall, wear awareness was understood to allow planning ahead car maintenance. Being potentially critical, also the option was requested to get an alert when e.g., the brakes or cooling water has reached a critical state. In addition, such incidents should also made a corresponding entry in a task list (see below).

Remote Awareness and Remote Control

Remote car awareness refers to get informed about the car status nearby or outside the car. For example, information on whether the lights left on, a released handbrake, unlocked doors, or a detected intrusion attempt. On the one hand, this information was demanded for reassuring everything was okay with the car. On the other hand, knowing something was wrong before using the car the next time, could reduce or prevent damage.

Additionally, some owners share their car with others– e.g., with their children, friends, or via private car sharing. These persons had an interest in various *surveillance* features. First, participants mentioned demands for controlling

driving behavior as a means for assuring the car was being handled with care or driven economically. Another use case rather targeted what the driver did when using the car, by following its GPS location. For example, entering or leaving geo-fenced areas could be defined to raise a notification.

For some participants, it was enough to get notified. Others also were interested in remote control the car with their smartphone. This was either for reacting to a car-related issue, for example locking an unlocked door, or for comfort-purposes such as regulating the heating before entering the car.

Task List

Participants reported that keeping track of different checkup intervals for a car was burdensome. Primarily, most cars notify when e.g., inspection is due, instead of providing awareness in the run-up. The Connected Car could generate a task list to support a long-term car management. This list could contain tasks such as the next general inspection or oil change, as well as externally defined tasks such as the next MOT-test, or dates to check insurance.

Some participants suggested that the task list should include information about the nature of the task (repair a defect, regular or on-demand inspection), provide explanation, and inform when and where the work could be done or has to be done (e.g. replacement of brake discs due next week in an authorized workshop). Besides forthcoming inspections, wear and defect information should be integrated in the task list. Most participants like the idea of the Connected Car generating such a task list automatically. A perceived benefit was that such a list helps to get an overview of all upcoming dates, repairs, and tasks around the car easier. In addition, the tasks should be ordered by urgency and recommendations for the best time and place to take action.

In addition, the idea was mentioned, to synchronize the task list with the personal calendars to better be able to match dates with other appointments. The list should be linked with the financial overview (see below) to be able to forecast, plan, and evaluate future costs.

Overview about Financial Issues

Financial overviews were desired to provide past and future expenses related to the car. Issues requested were gasoline costs including average fuel consumption, tax payment, car repair costs, insurance costs, but also current market value of the car. Two ways of presentation were suggested: chronologically and in relation to the driven kilometers. The goal for the users should be to recognize at a glance what the car costed about the last quarter. The hope is that Connected Cars could collect data of wear parts, defects, kilometer state, and other issues to make valid prediction about future costs. In addition to the costs, participants liked the idea of getting feedback about the current market value by comparing the actual state of the car with the price of related cars in online sales portals. Further, some participants consider that the car data could be used to get personalized recommendations about used cars and tuning products.

Several ideas were related to the connection with other applications, like logbook, tax, or business software. The data exchange, for instance, could be used to fill out forms, adapting depreciation to the actual residual value, and allow better financial planning. For car-sharing and carpooling, the car data can also be used for calculating fair, evidence-based, and transparent costs.

Location-based Information

Another request was related to location-based information taking the car status and location into account. Among others, the second dashboard should inform about events, places, and services located in the area of the car. Mentioned examples include information about congestion, gas stations, car repair shops, free parking, speed trap warnings, upcoming construction zones, tractors, and heavy loads. Further information about the weather near and at the destination, and a kind of friends-radar were called. The collected data should be displayed in an enlarged map.

It should also be possible to retrieve details about the entries on demand. While such information can already be provided by map applications on mobile systems, advantages to provide live messages to the driver were discussed e.g., sending a

push notification when a parking spot is getting free. In addition, the information could be improved, when the car context is taken into account (e.g., showing gas stations only if the petrol level is low).

Further Topics

Participants also mentioned other areas like environmental information including emission values, but also hints for ecological driving. Another topic refers to statistics like fuel consumption, speed, and most visited places, etc. One focus group also discussed the option of including communication channels to manufacturers, repairers, and insurances to make it easier to ask questions, make suggestions, or provide feedback regarding the level of satisfaction with the car.

6.4.2. Presentation Themes

Information Relevant for Driving or Security

There is a number of information over which our participant would like to be directly notified, to immediately react to certain conditions. By large, these circle around the actual driving context, but may extend the driving situation. Most importantly, when leaving the car, alerts should inform when the light was not switched off, a window is left open, etc. The same goes for attempted burglary and other suspicious events around the car. In contrast, important that refers to the actual driving, such as excessive speed, were deemed less important. This might be because these issues are already well supported by the first dashboard. Further, use cases for push notification had a stronger focus on other driving or location based information, e.g., leaving or entering a geo-fenced area.

Car push notifications could be characterized by three factors: (1) They are triggered when the car or one of its components reaches a pre-defined critical state or a user-defined state (2) they are pushed to raise the users' awareness, as (3) they usually call for immediate action.

Overall, users wanted to have control over pushed events. For instance, some car- or component states are pre-defined as critical in terms of driving or car security, while others may be defined individually, e.g., as soon as the fuel level drops

below 30%. These subscription techniques, which are also used for RSS feeds, might be a useful design concept.

Information for Car-Related Management

We also found that the Connected Car can support management activities of car-owners that go beyond the actual driving. Similar to other Smart Devices, such as Smart Homes and Smart Meters, users also seek to gain an overview about what the system is doing and what its state is [258, 447]. Moreover, a car needs explicit management, such as regular checkups or can be considered in tax declarations. Information regarding these management purposes. Such information should not be pushed, in order not to distract the user from ongoing activities. In particular, participants only called for specific information for a certain task such as planning a longer trip. Thus, the data is requested actively instead of being pushed. The presentation of such data should consider: (1) whether the data is retrieved regularly or on demand, (2) whether an overview about the most important indicators is needed or whether details about an actual issue, or the history of an issue is explored, and (3) to what extent informational demands vary depending on the particular context and task of the user.

Providing an overview, the dashboard design could adopt the long history of dashboard design in HCI [174]. To include tools for analyzing Connected Car data, existing InfoViz-techniques like "overview first, zoom and filter, then details on demand" [455] should be adopted. This especially holds for the visualization of times and distance oriented data like fuel consumption, wearing parts, etc. For instance, common methods such as bar graphs or scatter plots could be used, but also more advanced visualizations such as a spiral-shaped time axis or ThemeRiver technique might be used to support the detection of patterns and aesthetics of the graph [18].

Providing Interfaces to other Applications

Finally, including data from the Connected Car into existing software was a feature desired by participants. For example, while the cost overview was considered interesting, some participants remarked, that there already is software

for managing a households' finances. The integration of the task list into a personal calendar is another example for the need to embed digital data of the Connected Car into the digital life of drivers and their loved ones.

6.5. Discussion and Conclusion

The Connected Car creates new possibilities to visualize enriched car-related information digitally. The concept extends existing research on telematics [220] by a new perspective: It does not only seek to provide relevant data for the current driving situation, but also allows to take a management perspective considering the outside-car context. In this regard, we outlined a preliminary framework of categories for sensitizing designers in terms of what type of information users are interested in. Our study shows that the concept of the Second Dashboard needs a triangulation of data stemming from both within and outside the driving context to create innovative and useful Connected Car services from a user perspective. Processed data should 1) improve the driving experience, 2) improve management capabilities for owners, and 3) support reflection of driving behavior. Understanding the Connected Car as a complex cyber-physical system similar to Smart Home Systems, make apparent how these systems need transparency for the end-user in terms of what the system does and how it performs. Additionally, for security reasons, such newly available information will, when to be used during driving, spark new research demands regarding driver distraction, too. There are various attempts of business models for such services besides the solutions of car manufacturers, i.e. Pace (www.pace.car), which sell the OBD2 plug for a one time price or TankTaler (www.tanktaler.de), which raise a yearly fee for the usage of the OBD2 plug and the app. There are a lot of conceivable Second Dashboard business models like gamification or premium models. Moreover, especially data driven business models could be explored in further studies in terms of privacy and transparency.

Of course, our study is not exhaustive but rather open-ended, which is why it seems useful to understand the Second Dashboard as an ecosystem of related applications in the car context, that needs further research. Concerning this, we

plan to validate our findings by a survey and deepen the understanding of what information is relevant for different use cases and target groups. Further we are going to conduct user studies where we equip test households in a living lab infrastructure with car sensing technologies, to develop user-centered Connected Car-applications, data visualizations and usable privacy management systems. What services are needed both in and outside the car? Which information should be pushed and which should be pulled? What is the role of privacy within these systems? For answering these questions, we plan to conduct a design case study [528] to shed light on different design concepts and outline basic design guidelines for visualizing Connected Car data not only, but especially in non-driving contexts.

7. The catch(es) with Smart Home: Experiences of a Living Lab Field Study

Smart Home systems are becoming an integral feature of the emerging home IT market. Under this general term, products mainly address issues of security, energy savings and comfort. Comprehensive systems that cover several use cases are typically operated and managed via a unified dashboard. Unfortunately, research targeting user experience (UX) design for Smart Home interaction that spans several use cases or covering the entire system is scarce. Furthermore, existing comprehensive and user-centered long-term studies on challenges and needs throughout phases of information collection, installation and operation of Smart Home systems are technologically outdated. Our 18-month Living Lab study covering 14 households equipped with Smart Home technology provides insights on how to design for improving Smart Home appropriation. This includes a stronger sensibility for household practices during setup and configuration, flexible visualizations for evolving demands and an extension of Smart Home beyond the location.

7.1. Introduction and Background

The Smart Home seems to be the exemplar *par excellence* of possibilities inherent in the Internet of Things. Currently, both established companies such as Apple, Samsung and Google, and newcomers are positioning their own Smart Home products in the market. The idea of the Smart Home is not new and several researchers have already investigated challenges of making homes smart from a feasibility [284, 360] and user interaction [147] point of view and highlight the substantial 'work to make a network work' [213] for users. However, in recent years, advancing technology (i.e. the introduction of mobile and ubiquitous computing devices paired with low-power wireless communication protocols) has massively changed the way Smart Homes can be, and are, equipped and interacted with. For example, Harper's study [225], which dates back more than ten years, took place at a time when wireless affordances were not available, and where interconnected devices were rare.

This evolution has sparked more recent 'in the wild' Smart Home research that focusses on identifying challenges which Smart Home users face [72, 350]. Mennicken et al. [353] provide an overview of the literature and conduct an interview study with 22 participants, concerning themselves in the main with the relationship between user concerns and those of system builders. What we need, according to Mennicken et al. [351] is to '…stimulate both actionable insights and design artifacts that better capture the evolutionary nature of users and their home contexts'. Some challenges for users, then, are identified, though perhaps not in any great contextual detail. There remains, that is, something of a research gap. We aim, then, to report on the appropriation processes associated with Smart Home technology, covering the whole customer journey of system setup, installation and configuration, use, reconfiguration and extension, as a first step.

We therefore ask: how do Smart Home systems perform under real-life conditions? What are current challenges for successfully embedding the Smart Home into households' everyday practices, both from the system's and the users' perspective? While these questions have been raised in a user-centered manner, so far, there has been no recent long-term study on the Smart Home, one which actually accompanies households in their struggle to make their homes smart for a longer period of time.

The remainder of the paper is structured as follows. We first further motivate our research question by outlining related work and the current Smart Home product landscape. Subsequently, the methods and the Smart Home research artefact are introduced. The results from a case study with 14 households based on qualitative data from interviews, workshops, regulars' table meetings and mobile feedback application input collected in the past 18 months are then presented. Finally, we discuss design guidelines to help non-expert users to be able to manage their Smart Home adequately. Based on our findings, we suggest three main strategies: (a) To further hide technological detail in systems and instead make systems visible in a way that reflects how users construct their demands to make installation and configuration more user-friendly. (b) To acknowledge the individuality of users' information demands and provide flexible visualization solutions for evolving

needs. (c) To support flexibility for extending Smart Homes beyond the home as a place.

7.2. Related Work

Researching the Smart Home has a long, if slightly technology-driven, history. Several commercial and research-driven projects have explored various use cases and the potential of technologies for Smart Homes [225, 249, 284, 296, 360] from a feasibility point of view. In the following, we introduce design-oriented research for the home. Thus, we outline the concept of appropriation for informing Smart Home design and point towards a lack of long-term appropriation studies of technology in this context.

7.2.1. Informing Smart Home Interface Design

Studies relating to technology design for the home deal with a large number of different issues. For instance, in recent years, smart energy systems have received attention in research [5, 532], with a lively community studying Smart Metering, and with considerable efforts also focussing on privacy [92, 417]. In Sustainable Interaction Design [54], much research has focused on how to design energy monitoring systems from a user perspective [6, 188, 447]. It typically aims at making the consumption of the abstract resource "energy" – mostly electricity – visible and understandable as feedback to the consumer. Those working on Ambient Assisted Living technologies (AAL) [108] are very active in supporting comfortable and independent living for older people [129, 235, 337]. Amiribesheli et al. [25], for example, present a literature review for AAL and conclude with general design guidelines, supposedly also applicable when designing Smart Home technology. The role of security for the home has also been researched, e.g. within the field of access control [475] Ur et al. [501], for example, have shown that many Smart Home systems feature their own login system, thus fragmenting user flow and hindering a positive UX. Yet another issue identified is that of designing eco-feedback. For example, Froelich et al. stress, 'it is critical for the HCI community to step back and define an approach and theoretical foundation for the design and evaluation of eco-feedback technology' [188]. Strengers [478]

also critiques the models underpinning eco-feedback systems and argues for an approach embedded in daily life. Such positions, as we argue below, have wider ramifications. Other studies focus on single aspects of a Smart Home, such as automation [106], activity recognition [489], privacy implications [109, 287, 498] or certain parts of Smart Home user interfaces, such as the use of calendars [352].

Smart Home systems, however, promise to include a multitude of uses, including but not limited to the ones outlined above. For these complex systems, user-centered research deals, at least to some extent, with challenges posed, drawn from interviews with experts or people living with a Smart Home. For example, Brush et al. [72] have investigated the user acceptance factors of home automation technology. They identify high costs, inflexibility, bad usability and security issues as the most important barriers to the success of Smart Home platform systems. Similarly, Mennicken have found barriers to succesful Smart Home integration, identifying *a better support for routines as one central aspect* [353].

7.2.2. Understanding the User: Designing for Appropriation

A more comprehensive view on the use of technology can be developed by researching its appropriation in everyday life. This process is understood to include not only interaction with technology itself but also collecting information about it, envisioning possible use cases and developing an overall attitude towards it [84]. Generally, designing for appropriation means taking into account that users will make use of technology in unanticipated or even unintended ways in their everyday life. Design of technology thus should support flexibility in terms of adaptability to different environments, evolving (user) needs and environment as well as ownership [135]. In this vein, Carroll et al. [84, 85] have investigated what younger people do with technology, especially mobile phones. Stevens et al. [474] suggest ways of designing for individualized use of software engineering tools. Similarly, Dourish [140] outlines guidelines for supporting appropriation of document management systems in terms of important features to be included within a solution.

When aiming at reducing barriers to the appropriation of Smart Home platform systems, it likewise stands to reason that a broader view on a product's lifecycle, ranging from the system setup phase, over installation and routinization to reconfiguration can be beneficial. Such an comprehensive approach calls for long-term in-situ investigation into how users ascribe meaning to Smart Home technology and how this technology evolves in association with social practice and vice versa [457].

However, our inquiries reveal no recent long-term studies, investigating different phases of Smart Home interaction. As a notable exception, and as mentioned, Harper and colleagues [225] specifically researched the home from the users' perspective, looking closely at the appropriation of technology in the social space of the home. One chapter [404] specifically focuses on what it is like to live with and in a Smart Home, outlining design guidelines and possible futures. In contrast to most other research, the people in that research actually lived in a Smart Home, thus entailing a longer term approach to technology appropriation. However, as we have pointed out, the setup had limitations. Participants were not actually living in their own homes and technology at that point did not encompass cloud systems, smartphones, or new low-power wireless protocols, which allow battery-powered sensors and actors to become independent of wall sockets and thus to be installed more flexibly in unelectrified areas of the home. Therefore, more than ten years after Harper's study, it seems reasonable to revisit the appropriation of Smart Home technology.

7.3. Background on Smart Home Systems

In principle, Smart Home systems have existed ever since computers found their way into the home during the 1980s. At that time, hobbyists put huge effort into wiring up their homes. Such "wired homes" [225] were highly customized and characterized more as individual solutions rather than ones with the quality and scalability of a commercial product. Recent advances in low-power wireless communication protocols as well as miniaturization and decreasing costs of hardware have turned Smart Homes into a main stream and lifestyle product, and

they are considered as soon becoming the next digitalized part of daily-life. Currently, in addition to established home automation solution providers, many other IT companies, illumination manufacturers, telcos or even power supply companies are positioning their own Smart Home products, not to mention start-ups' attempts at gaining a market share.

Under the general term Smart Home, products vary greatly in terms of the technology used and the use cases covered. For our purpose, we distinguish between Smart Home systems along two dimensions, similar to Brush et al. [72]. First, there are products that only serve a single use case, such as smart thermostats, and second, platform solutions spanning across use cases and allowing greater flexibility. The latter systems either call for expert installation or are do-it-yourself solutions based on the principles of plug and play.

7.3.1. Single Product vs. Platform Systems

While there are no limits to the heterogeneity of hardware offered for the Smart Home, components can generally be categorized by use cases supported. Here, four trends can be identified. (1) Systems for supporting comfort, such as by sensing temperature, daytime or brightness and automating shutters, light, and air conditioning, entertainment and related appliances. (2) Increasing security in the home by installing internet-linked or networked cameras, motion detection, sirens, remote control of lights for simulating presence and control as well as alarm notifications via text messages or push notifications on mobile devices. (3) Monitoring and saving energy by avoiding standby consumption, automated switching off of devices and appliance-based measurement of energy consumption as well as visualization of consumption. Here, generally, smart plugs are used, placed between the device's plug and the power outlet. (4) , enabling more sustainable self-determined living through AAL technologies.

While Smart Home products may consist of only one sensor, platform providers, offering a set of hardware and software, are becoming more popular. These systems typically feature a hardware gateway and address more than one of the aforementioned main use cases with their set of sensors and actors. The multitude

of protocols and vendors, however, make the current market highly fragmented. Interoperability between the devices of different vendors is rarely supported even when they use the same protocol. Some systems, however, have a whitelist of products using the same protocol; others allow for extending their system with dongles to enable other protocols to be used.

Smart Home systems have three main ways of interacting with and controlling the system. First of all, many systems enable basic interactions via the hardware interfaces of their sensors and actors. For example, simple on-/off switches are provided. Moreover, there are switches dedicated to triggering predefined actions on other actors. More sophisticated controls are sometimes provided by dedicated displays. In most cases, however, Smart Home platform vendors provide controlling and monitoring mechanisms via mobile or desktop applications. Here, dashboard-styled control dominates, allowing direct manipulation of sensors and actors. Furthermore, these interfaces typically support (1) gaining an overview of the current and past state of the home (2) managing existing and adding new devices, and (3) managing automation rules and groupings.

7.3.2. Expert Installation vs. Plug and Play

For a long time, Smart Home systems required wired connections between control panels and sensors or actors. Installing and configuring such systems is often accomplished by professionals, and users without expert knowledge can only perform basic configurational settings. Wired connections for the Smart Home have several benefits. Typically, flush-mounted, they are well integrated into the home and can be almost invisible. Additionally, wired connections guarantee a good connection to control and monitoring stations. On the other hand, using wired connection makes "smartness" very inflexible in relation to evolving demands. Additionally, including a wired Smart Home into a building – be it new or retro-fitted – requires complex planning and significant investment.

More recent products in the Smart Home rely on low power wireless communication protocols. Emphasizing their plug and play character, these systems are surface-mounted and battery-powered and thus can be positioned in

remote sites within the home. This way, such systems are more flexible in terms of being adaptable for users. They are less cost intensive than wired systems and easier to integrate into existing home infrastructures. However, the burden at present is on the user to setup and manage rules and configurations.

7.4. Setting up the Smart Home Living Lab

Against the backdrop of quickly evolving technology, we believe it is appropriate to investigate the appropriation of Smart Home technologies in everyday life. Following Stevens et al. [474] and Wulf et al. [528], we seek to inform the design of Smart Home systems through understanding user behaviours throughout the process, thus informing UX design in future Smart Home products.

The work described in this paper was conducted as part of a 3-year research project focusing on the development of new concepts and strategies for Smart Home systems with a specific focus on UX. We applied a Living Lab approach [157, 185, 376] to address the complexity and situatedness of these systems over different stages, namely (1) system setup (2) installation and configuration, (3) use and embedding into practice and (4) extension and reconfiguration in real life environments. Living Labs allow different stakeholders from research and design to be brought together with users and technology in an open-ended design process in real life environments [185] as far as possible, given that they are predicated on the introduction of new technology into the environment in question, Living Labs are intended to be 'naturalistic'. Such frameworks are specifically suited to supporting long-term cooperation, co-design and collaborative exploration among researchers, users and other stakeholders. Involving users in the design process from the very beginning in sensing, prototyping, validating and refining complex solutions in multiple and evolving real life contexts allows a continuous formative evaluation of the designed artefacts and uncovers appropriation phenomena at early stages in the technology life cycle [49]. The advantages of the Living Lab approach lie in its flexibility, allowing for creative spaces for discussions on new concepts, long-term observational studies and, where necessary, lab-based

interventions, designed to assess the long-term appropriation of new IT-artefacts [376].

7.4.1. Recruitment and User Sample

We recruited our user sample through a four-staged selection process. From November 2014 to January 2015 (see Figure 3), we placed information about the study in the local press and via radio stations. We did not offer any compensation for participation. The only incentive we provided was the free provision of a Smart Home system used as the central research artefact and active participation in the project. Via an online platform, interested people had to provide basic information concerning their households' technical infrastructure, motivation for participation and expectations of the project. At this stage, more than 100 households applied to participate in the project.

Second, we checked all applications in terms of accuracy of fit for our project's demands. We decided to only include households within the postcode of the city of Siegen, Germany. This restriction allowed us to get in touch with them easily, e.g. for home visits, interviews and roundtables. As technological requirements, we defined two more criteria, which we believe are not critical but are worth mentioning. First, only households with a reliable internet connection with at least 2 kbit/s download according to the carrier contract were included. Second, due to budget constraints, only households in possession of at least one smartphone could participate, so households could be provided with tablets.

In a third stage, telephone interviews with each of the remaining 63 households were conducted to gather an impression of the motivation for participation, willingness to actively participate in the project and technical- and Smart Home-related foreknowledge. Additionally, these interviews served to get to know participants' self-reflectiveness, articulateness and understanding of the character of soft- and hardware prototypes compared to products.

Finally, we characterized all households and chose a sample, varying in terms of age, sex, household size, rented or owned home, house or flat, rural or urban

residential area and tech-savvyness as well as educational level. Finally, 14 households with 23 participants were selected. The sample consists of two single-person households, five multi-person households without children and five multi-person households with children. Four households lived in flats, while ten were owner occupied. Participants were aged between 27 and 61 years. Motivation varied, ranging through dissatisfaction with existing Smart Home systems, technological interest, to curiosity about being part of a research endeavor. Based on this qualitative user sample, we started the longitudinal Living Lab study.

7.4.2. Study Design and Data Collection

In March 2015, we first conducted a kick-off event to brief households regarding our overall research agenda. This was the first opportunity for households to get to know each other. Following this event, we set up an exploratory on-site study with a semi-structured interview guideline. We mainly aimed at a better understanding of the participants' homes, their daily routines and habits as well as their ideas for using a Smart Home. We also used the initial interviews to get to know each other and to establish trusting relationships. At this point, we also distributed wish-lists for Smart Home equipment. Households were allowed to pick any combination of available sensors and actors. To avoid a mental overload and to help participants to start thinking 'small', we suggested equipping only one room at the beginning and decided to set a maximum of ten hardware components. However, some households were allowed to order more than ten components if they were able to explain which use cases and scenarios they wanted to realize and what they wanted to achieve with them.

Based on these wish-lists, we provided an out-of-the-box plug and play Smart Home platform system released on the German market in May 2015 to the households. The installation and configuration process was either observed and video-recorded by researchers on-site (seven households) or self-reported by participants (seven households). To subsequently collect experiences in-situ and maintain a close relationship to households, a mobile feedback application was provided and integrated into the companion app of the Smart Home system. An informal regulars' table and an instant messenger group were initiated and

maintained to foster exchange of experiences, ideas, problems and their solutions between users and researchers. More formal communication about invitations to design workshops, technical announcements or updates about the project's progression was carried out via email by a university staff member who was responsible as central contact person for participating households and was a communication node between all project members. After this initial setup phase, households used their Smart Home over 15 months and participated in four design workshops focusing on information collection and interface design for new Smart Home concepts.

As a first evaluative intervention, in September 2015, after three months of use, we conducted a second interview study gathering experiences, demands and limitations when using the system. We focused on ways of appropriating the system into everyday life and reflections on the installation and usage routines in terms of usability und UX problems. We also asked for examples of best practice and implemented use cases. In August 2016, after 15 months of use, a third interview study was conducted where we asked again for best practices and desired or implemented use cases but also for changes in system configuration based on changed user needs or seasonal influences or based on the integration of new third-party components. We also noted changes within routines and daily habits in the course of using the system. All interviews, workshops and home visits were audio-recorded and videotaped where it was deemed to be helpful for data collection.

7.4.3. Smart Home Infrastructure

We chose a Z-wave based Smart Home platform system from a German provider. It is marketed as a plug and play solution with surface-mounted components only. Apart from manual control, the system also allows for automated control: setting up rules (if this, then that), scenes (setting a defined state for a number of components) and timers. Devices also can be grouped, for example, by room or by any other custom aggregation. A customizable dashboard serves as a homescreen where all chosen components are presented in widget-style fashion. Additionally, a weather-widget and a text-based home logbook are included. The

latter provided information regarding the system state (starting and stopping the gateway, connection to cloud, updates etc.) and listed every event (sensed motion, input, changed settings, triggered switches, rules, scenes or timers) of the smart system.

The sensors and actors were organized via a gateway, which was connected to the home router and thus the vendor's cloud. All existing settings were executable without internet connection, but changing settings and – naturally – remote control out of the home network depended on an internet connection. Controlling the system was possible via sensors and actors themselves (switches, remote control, thermostats and smart plugs), a companion app and a web portal.

While third-party sensors were not officially supported, there were user-generated whitelists in forums. When the project started, the Smart Home product included the following sensors and actors which households could pick: room thermostats (14 picks), radiator thermostats (31), motion and brightness detection (14), door-/window contacts sensing openness or closedness (29), smart plugs for measuring electricity consumption and switching appliances (45), remote controls (6), freely positionable switches supporting two or four different positions (11) and a smoke detector (10). While the product is offered in typical starter sets and sets focusing on a certain use case, such as heating, we allowed households to freely choose a constellation of sensors and actors for their Smart Home.

7.4.4. Data Analysis

To identify challenges and experiences of Smart Home from a user perspective, our analysis is based on all data (interviews, workshops, field notes from home visits and regulars' table, text histories from instant messenger group) collected during the 18-month period of the Living Lab research. All audio-taped material was transcribed. Each document was processed by two researchers individually using thematic analysis with an inductive coding process [66]. After each empirical phase, the codes were consolidated and developed iteratively. We discussed gained insights internally with researchers who were not involved in the project as well as with our industrial partners in the consortium.

For the analysis, we searched for common patterns and categories related to how participants find and select appropriate Smart Home solutions, how they used Smart Home components (sensors and actors) as well as looking at software design, interactions and information provided through the system and how households tried to include Smart Home components into their lives and how everyday life changed through the Smart Homes. The analysis enabled us to identify four central categories relevant to the successful appropriation of Smart Home technology within four stages of use. Based on Silverstone and Haddon [457] we have ideal-typically organized these categories into four phases of Smart Home appropriation: (1) system setup, (2) installation and configuration, (3) routinized use and (4) demands of reconfiguration and extension. All quotes used in our findings section were translated from German by the authors.

7.5. Findings: UX Challenges for the Smart Home

In this section, we present results of our qualitative Living Lab study. We broadly assigned them into the phases of system setup, installation and configuration, routinized use and demands for reconfiguration and extension.

7.5.1. System Setup: Choosing Hardware Components

Product innovation literature shows that there can be a considerable mismatch between the functionalities on offer and the expectations of consumers (i.e. [340, 537]). Our initial interviews showed that most of the households already had informed themselves about Smart Homes via the internet or magazines. However, participants planning to include Smart Home technology in their newly built or modernized home were overwhelmed by the number of existing products and their implications for future interoperability. Most common reasons for abandoning the search were a lack of market transparency and helpful information about use cases and best practices as well as an overly technical presentation of Smart Homes. Here, especially different communication protocols raised uncertainties. A male participant from a more tech-savvy multi-person household describes the assessment of existing Smart Home technologies as follows:

"I haven't decided on anything yet because I know there are many solutions. It is well known that [product A] is pretty expensive. [product B] is more for hobbyists [...]. Maybe those plug and play systems are better. [...] Investing hours of time reading through forums, writing scripts – which I cannot do myself – or programming something via copy and paste, I simply don't have the nerves for that right now."

While Smart Home technology is evolving fairly quickly, as far as the integration into home infrastructure goes, items need to be future proof, especially (but not only) when flush-mounted and thus more permanently installed. Additionally, the variety of more sophisticated product packages, and varying payment models requiring considerable financial investment, further discouraged households from deciding to buy.

When households were picking components for setting up their future Smart Home, it became obvious that many had very little knowledge of the various features of sensors and actors, as well as of their potential for combination. Except for tech-savvy households, participants had problems in articulating their needs and translating them into use cases or more complex scenarios with several hardware components beyond the ones that had sparked the interest in a Smart Home. Here, households often oriented towards use cases that researchers or other households provided e.g. via the instant messaging group or the regulars' table meetings. This complexity problem for the Smart Home user is reflected in several comments from participants, such as the case of a couple with grown-up children who have already moved out of the house:

"It has got to stay easy. Not everyone has daily contact with IT. We have seen people standing in [a consumer market] in front of Smart Home products, and I literally saw the question marks in their eyes."

The core problem our participants had in making their choices was to be able to identify routines to be supported and then map how the system might support a certain use case. While, in respect of hardware, this was unproblematic for use

cases where only a single (kind) of sensors was needed, such as heating, the complexity grew strongly with the number of different sensors included in a scenario. Moreover, sensors often have secondary features, such that a motion detector, for instance, also senses brightness. These hidden features made it very hard for households to actually understand what possibilities existed.

7.5.2. Installation and Configuration

In the phase of installation and configuration, households came in first contact with hard- and software. The system setup which households chose needed the hardware components to be installed and paired with the gateway. Additionally, households had to register with their email addresses to gain access to the vendor's cloud portal. Components were used to define rules and relationships on a software level. The installation routine was either accompanied by a researcher or self-reported by the provided in-situ feedback function of the companion app. Even so, households ran into problems getting the system running without considerable support from researchers or the vendors' support channels (hotline and live chat support).

The most common problem touched on that of pairing devices with the gateway – a necessary step for Z-wave based components. The whole process raised serious issues and was a task many participants felt uneasy accomplishing.

> *"For me, installation was very ... complicated. I mean you always think its like plug and play. Meaning: I will just try before reading the instructions. And that didn't work at all. Then I read the manual and thought I had understood it. But this still wasn't the case and looking closer to the manual, you found half a sentence you missed and then it worked." (multi-person household)*

Moreover, the reason for having to undergo the process was unclear to participants unfamiliar with the technology; they expected the Smart Home to be plug and play compatible.

> *"Retrospectively, I would prefer to simply put the devices where they should be and then they should make themselves visible automatically somewhere and*

then you just ascribe them instead of having to wait and do all these steps." (multi-person household)

Introductory screens and overlays, described with highlights, arrows and text boxes, were deemed not especially helpful. The overlays were often quickly removed and, in fact, not read at all. When the overlays' informative character was subsequently described, reactions were more positive:

"If you haven't ever done this before and you don't know [how to], you would probably search, search, search. In this way, it is prescribed to you: Oh yes, you have to click here, to start the timing. I think that actually is quite okay." (multi-person household)

For pairing devices, in ordert to include them into the system, rules for automated behavior in an if-this-then-that style needed to be defined by users. Identifying these concrete procedures necessitated considerable reflection:

P1: *"I find it especially hard to set up rules…And setting them the way I want them to work. I don't manage to do this myself."*

Interviewer: *"So what did you do?"*

P2: *"I always try. Let's look [into the system]. A rule is for example: In case the thermostat measures 23 degrees Celsius, shut down the heating. That's a rule, right?"*

P1: *"If one thing happens, the other thing must follow. That's a rule. I never manage to do this."*

P2: *"When the window is open, I get an email. We tested this down here: opening and closing. Then I tried to include that it would only write an email after 10 minutes or so, because we only need a reminder when we have forgotten it. And I didn't find it and eventually gave up."*

Noticeably, households typically defined rules in a step-by-step manner. For example, when wanting a light to switch on depending on sensed movement: First, coupling the motion sensor with the smart plug was set and tested as a rule by moving in front of the sensor. After success, the period of time where the light was to remain turned on was set and tested again. Finally, the restriction that light should only be turned on when ambient light is low was added. In one case, darkness was simulated by putting the sensor under a cushion or covering it with a hand to get immediate results. This example makes two challenges explicit: First, users had a need for immediately testing rules due to either lack of trust in their own accurate understanding of rules or in the system's interpretation. In other instances, automatic timers were defined to trigger certain actions during testing. Households explicitly used fake times to get feedback about whether their idea of implementing the rule was correctly reflected in the system. Second, and more importantly, the problem of thinking about daily routines in algorithmic structures is not an everyday task for many households, resulting in inconveniently having to set up rules incrementally to make them work and fit actual needs.

> *„But the rule, such that I can say: 'The door sensor measures certain brightness and it should turn on the lights.' I still don't know how to get there. But I have followed the chat in the group and Dave is really good at this."* (multi-person household)

Tech-savvy households with basic experience in configuring IT-systems and pairing processes often figured out troubleshooting for themselves and supported others, for instance, by setting up rules or suggesting use cases, with hints in meetings and within the instant messaging chat group.

7.5.3. Domestification and Daily Use

In the following months, participants used their individually configured Smart Home in more routinized ways. Within this phase, participants reported a considerably reduced interaction on the software interface level, due to having found their optimized configuration.

Regular and permanent home awareness demands

Despite households' general desire for background automation, we also found various demands for explicit information and awareness. In particular, permanent demand for historical data was mentioned. One household, for instance, which already manually kept track of gas and electricity consumption on sheets of paper wanted to digitalize and improve monitoring:

> *"For example, when I have invested let's say into my heating, I want to know: Does it pay off? Or when changing my heating settings. [...] I want a conclusion: Did it pay off or not? Therefore, I need to measure. If I don't, I can't change anything. I am not a control freak, but I want to know." (multi-person household)*

This permanent home awareness mechanism targeted not only support consumption optimization, but also security aspects regarding the whole home:

> *"When I'm on vacation or just gone for a week, then you want to know what has happened." (multi-person household)*

In particular, instead of having an interest in every single event, households tended to look for groups of events, which they were able to identify as a "normal" amount or sequence. Identifying patterns such as activities and times of absence, one could assess whether everything was okay at home or not.

Coming or leaving home were two very common scenarios in which households wanted to check on things or set devices to a certain state. For example, the same household with cats had installed a safety mechanism for their pets:

> *"It is dangerous for our cats if we let the window open when we leave the house because they could get hurt by getting stuck in a partly opened window." (multi-person household)*

For this purpose, they connected a small light to a smart plug next to the entrance door which switched the light on when windows are open. Similarly, another households set up an awareness system for the dryer which was positioned in the

basement, by connecting a smart plug to the machine and defining a rule that a smart plug in the living room should make a light blink when power consumption of the dryer dropped. After presenting his idea at a regulars' table meeting, this solution was adopted by others, too. Other demands for information related to security issues, such as checking for open windows or making sure all electronics were switched off.

A second kind of permanently demanded information related to system awareness:

"I check the system to see if something has failed, like my heating control at the beginning?" (multi-person household)

Related to system awareness, users showed relatively little concerns in privacy, though some users wanted to know what information was being transferred to the vendor (or 3rd parties). That is, they demanded a degree of awareness:

"For now, I don't see any way of misusing my data that could turn out to be my downfall. [...] It would be nice, however, to see what data is transferred or stored. If I can control this, its on me to decide what may be transferred or used." (single-person household)

Moreover, we found that most households did not understand the potential of information that could be deduced by third parties analysing data. However, if users understood, e.g. that Smart Home logs provide strong hints as to whether anyone was at home at a given time, awareness and caution grew:

> *"After looking at the diary widget, I realized what information the Smart Home collected. Especially, in terms of motion profiles, because these are safety-critical information." (multi-person household)*

One-time and temporal home awareness demands

During summer, in particular, a set of temporal or seasonal information demands became apparent. With longer daylight and higher temperatures during the summer season there was simply less to be managed in the house and interest in checking the temperature for heating was less sought. During the summer,

however, a two-person household with cats for example wanted to check the room temperature while they were abroad:

> *"[...] We could control if it was too hot for the cats at home." (two-person household)*

Several information demands were limited to a special event or timespan. This could be due to activities of members of the households or due to a change of infrastructure: for example, to gain an understanding how much energy the new washing machine consumed. After tracking the machine for a while, there was no further interest in a long-term consumption evaluation.

Controlling the home

The physical Smart Home switch was considered a great way of controlling the home, and many households appreciated the possibility of simply positioning switches whenever a Smart Home command was used regularly. For example, several households positioned a switch, which was supposed to be put on a wall, on their living room table to change light settings when sitting on the sofa despite aesthetic considerations. The switch was only available in white, since it was built for wall mounting, and was seen as intruding on the interior decoration.

Although also a frequently used interface when at home, the mobile application was primarily used abroad. Here, use cases serving a demand for security awareness prevailed. Simulating presence by switching on and off lights manually was especially considered a benefit. While traditional timers were already used by some participants, their static programmable time slots were perceived as a limitation and easily detectable by potential burglars. Either random timers or randomized timeslots were mentioned as possible solutions.

While core use cases seemed to be identified, the routinization phase points towards the complexity and heterogeneity of households' ecosystems. Even though comfort, security and energy savings might motivate households to have an interest in a Smart Home on a global level, concrete use cases are highly individual and changed noticeably depending on seasonal factors, changing

infrastructure or (irr-)regular events and households' evolving routines. Many use cases only arose in a later phase after households had the systems installed.

7.5.4. Becoming an Expert: Reconfiguration and Extension

In our first reflective interviews after four months of Smart Home use, participants told us about having integrated their Smart Home into their households to varying extents. Upon asking about the system's cost and its relation to the market price, however, the Smart Home was valued more as an expensive 'nice to have' gadget, rather than as a vital part of the home. However, no household took the offer to remove the system; they all wanted to participate further.

With households getting used to the system, its limitations became more evident. These, in part, stemmed from the sensors and actors not included within the system. For example, flush mounted switches or IP cameras were not available. While disappointing in principle, households understood that the product was still new and its landscape was to be extended. Other limitations of the Smart Home, however, were less anticipated and less accepted.

First, many users perceived Z-wave as a strictly standardized protocol and thought that any Z-wave-based sensor or actor was supposed to work with the system, too. Therefore, as an alternative to missing sensors and actors in the system, more technology-experienced households themselves tried to include third-party devices into the system. In most cases, and to varying extent, this failed due to differing interpretation of the communication standard. One participant found a third-party device that included several sensors which he wanted to be shown on his dashboard. Although compliant to the Z-wave standard, including the sensor was hard work and only partially worked:

> *"Well this (...) small bowl [I got] (...) It was kind of a jack of all trades device including earthquake sensor, motion detection and temperature (...). After four weeks, I managed [to include] it, but it only offered me the motion detection function." (multi-person household)*

The only way to know whether a product would work, even within the same standard, was to either find out by word-of-mouth or by trial and error. Throughout the Smart Home market official whitelists are seldom to be found.

Second, users found limits in the product itself, posing a barrier for their intended use. For example, some configurations of includable sensors were not possible, e.g. defining the sending rate of a light detector was not possible because of the vendor's battery saving intentions. This however, limited adaptability and led to feelings of helplessness and frustration:

> *"I guess you have to think twice whether it is the right component to fulfill your wish? [...] But I think it is kind of an issue, when expectations of users differ from what the vendor was thinking." (single-person household)*

Users also naively thought that other systems they used would be interoperable with a Smart Home, especially the ones promising "smartness". For example, some households had smart meters installed, which they thought would easily go with a Smart Home system – in fact they were considered a vital part of it. Similarly, other smart systems such as smartphones or audio systems were expected to be able to have an interface for sensors and actors, such that e.g. the Smart Home would be able to react to the GPS of the phone or the battery of an electric vehicle.

7.6. Discussion and Conclusion

In the 18-month Living Lab study, we identified 3 potential ways of fostering appropriation of Smart Home technology. We provide significant empirical detail, showing not only that users experience certain kinds of barriers but also *in what circumstances and when* they are likely to do so. Second, the extensive qualitative research undertaken demonstrates how these barriers are significant at particular stages of the appropriation process and suggests that designers need be mindful of this evolving set of conditions. Thirdly, we have shown, in and through the Living Lab study, that the various barriers to use should not be treated as separate matters, but need to be addressed in a holistic manner. In particular, the heterogeneous

ways in which households demanded configuration forms, and the degree of knowledge required in order to do so, was identified. Throughout the study, the most common and severe problems arose in the fields of (a) a disconnect between users' expression of demands and the systems' capability to understand and process them. This became visible in the system setup phase and during installation and configuration, (b) maintaining awareness in routine use and and finding suitable visualizations for feedback demands, and (c) system extension beyond the home as a place. We discuss these practice-based phenomena and outline promising ways of addressing these issues.

7.6.1. Setup and Configuration with Practices and Routines

Despite being interested in buying a Smart Home product, all households in our Living Lab mentioned having experienced problems identifying a suitable solution. The market is evolving quickly, and new products are being continually offered, making it hard to gain an overview. Most importantly, a Smart Home system was understood to be a significant investment, thus requiring it to be extendable in the future [72]. Here, the implications of choosing a particular system were not transparent in relation to future extensibility of the communication protocols and third-party sensors or actors. In this regard, our observations here were similar to Mennicken et al. [350]. Our findings go further, however, in highlighting that households actually did have ideas of what a Smart Home is supposed to provide, but often failed to map their interest to suitable technological setups. When asking, what could be improved or automated in the home, households often came up with what Smart Homes already offer. However, the step towards choosing the right technology was where our households reported feeling undecided and lost. We believe that orienting towards practices, routines and use cases to be supported will help users better understand what kind of technological setup they might need.

This disconnect between what users desired and how to map this to the system also was a major theme during installation and configuration, too. Although in the past even experts struggled to get distributed digital systems to work [494], new interfaces and web technologies promise plug and play even for "ordinary" users.

This is in line with several attempts to make the Smart Home plug-and-play compatible [2, 60, 285, 377]. Taking into account the individuality of user demands, End-User-Development (EUD) is known to pose a promising strategy for making complex systems work for non-experts, and should be relevant to the Smart Home [259, 523].

We now argue that it is especially useful to support the operationalization of behavior and routines into events measurable for sensors. Smart Homes, we argue, should be sensitive to local and changing, routines by affording more obvious and flexible (re-)configuration possibilities [353]. The typically proposed if-this-then-that style posed major challenges to households not familiar with algorithms in their everyday life. Reflecting on household practices in such a way that they could be matched to technology behavior was a serious challenge. Here, systems could more actively support users, e.g. by being pre-paired and preconfigured [377]. For example, products could be adapted to users during the buying decision by them reporting about routines. This way, the workload of algorithmically reflecting about daily routines would be transferred into a non-technological language, while still allowing rules and dependencies to be deduced and use cases to be suggested. This would allow the vendor to include rules into the system upfront, thus relieving the user of a task and fostering the plug and play character.

7.6.2. Design for Evolving Visualization Demands

During sustained and routine use, households checked up on their Smart Home, in the main for three reasons: (a) Maintaining control and awareness of what has been going on in the home and how it performs (i.e. in terms of energy consumption), (b) system check (i.e. whether the Smart Home does what it should), and (c) for temporary or specific event-driven information demands. Although, generally, the system worked in the background autonomously, usable means for maintaining sovereignty in the home were demanded. Regardless of the reason the concrete requirements on what exactly households wanted to check were highly individual and changed over time. In the field of energy consumption, these are known phenomena [448], calling for software to allow for continuous change and adaptability [259, 264]. EUD [40, 323] could support the users'

journey from a novice to an expert user by allowing for adaptable information dashboards and information widgets for evolving or temporary demands.

7.6.3. Extending the 'Home'

After getting used to their system, some households explicitly tested boundaries or came up with new use cases that included other electronic devices, such as smart meters, photovoltaic systems, smartphones, IP-based gardening equipment, cameras or car-mounted GPS-sensors. The isolation of these smart systems was counterintuitive to users and often led to frustration when different smart systems were not interoperable. This separation was not reduced to single appliances and protocols [72], but rather spanned across ecosystems. On a UX and usability level, the single access points to the systems lacking coherence in wording, style and control.

Households increasingly perceived their Smart Home interface as the central point for managing their home and wanted a single management system that also included e.g. their garden electronics and connection to external sensors and actors such as the smartphone. In this regard, the home is more than a location [126]. One promising solution is unified dashboards and control centers of distributed information sources from cyber-physical systems in household environments, similar to what Few [174] describes for business dashboards. For respective measures to be effective, this also calls for action on the middleware level [136]. If respective APIs and interfaces for protocols are provided, user interfaces may make use of them.

7.6.4. Limitations

Our findings might in part be due to system peculiarities. Even so, having conducted a market analysis and lab-based test of several platform-based systems we believe that most findings are not bound to a specific product. For Smart Home systems, Z-wave is a widespread standard, as are dashboards and IFTTT mechanisms for rule definition. All of which have implications for setup, running and maintenance that our system shares with many others. Also, market complexity and limitations in interoperability are not product-related. More

sensors might have improved the Smart Home experience. However, at least for surface-mounted solutions, an evolving growth of the Smart Home system better represents the actual way of buying such systems. Moreover, most inexperienced participants ran into major problems making their Smart Home work with about ten existing sensors. In limiting the amounts of sensors, we supported a steady appropriation and found newly developed use cases over time. Finally, our research was of a qualitative nature, which also sparks typical limitations. For further evaluating validity and classifying the relevance of each problem dimension identified, further quantitative research could and should be conducted.

7.7. Conclusion

Our Living Lab-based case study has identified design guidelines addressing challenges during the process of Smart Home appropriation. Overall, we argue that Smart Home so far has targeted the home primarily as a technological space, rather than a place formed by routines and interaction [229]. By becoming more sensitive to the routines and practices of users, four challenges could be addressed: Regarding the challenges of setting up and configuring the Smart Home, we stress the importance of daily routines as a metaphor which households can cope with, in contrast to technical detail or algorithmic patterns. For supporting operation and maintenance of a Smart Home, evolving visualization demands call for flexible user interfaces, adaptable to both temporary and permanent information demands on home and system awareness. Finally, Smart Home systems could unlock more of their potential when going beyond typical place-related boundaries, incorporating floating and interweaving practices which are not limited to the home as a building.

8. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility

A key issue for Smart Home systems is supporting non-expert users in their management. Whereas feedback design on use cases (such as energy feedback) have gained attention, current approaches to providing awareness on the system state typically provide a rather technical view. Long-term investigations of the practices and resources needed for maintaining Do-It-Yourself Smart Home systems, are particularly scarce. We report on a design case study in which we equipped 12 households with DIY Smart Home systems for two years and studied participants' strategies for maintaining system awareness, from learning about its workings to monitoring its behavior. We find that people's needs regarding system accountability changed over time. Their privacy needs were also affected over the same period. We found that participants initially looked for in-depth awareness information from the dedicated web-based dashboard. In the later phases of appropriation, however, their interaction and information needs shifted towards management by exception on mobile or ambient displays – only focusing on the system when things were 'going wrong'. In terms of system accountability, we find that a system's self-declaration should focus on being socially meaningful rather than technically complete, for instance by relating itself to people's activities and the home routines.

8.1. Introduction

With the increasing proliferation of Internet of Things (IoT) technologies for consumers, the 'Smart Home' is emerging as a domain for significant potential market growth [462]. Enabled by energy-efficient networking technology [414], such as ZigBee or ZWave and reduced hardware costs, new Smart Home sensors, devices and services continue to emerge, thus constantly increasing the variety of technologies that might be integrated into today's Smart Home. To be adaptable to the individual physical and social character of specific homes [229], many Smart Home systems have adopted a do-it-yourself (DIY) paradigm. The Smart Home's inhabitants can set up, configure, and automate system behavior

themselves in accordance with their individual (or family) needs, e.g., having lights switch on in case of detected movement in a hallway, or remotely controlling heating and air conditioning before people arrive home.

However, flexibility in choosing hardware and software setups comes with increased complexity. This complexity, we argue, will magnify as systems develop. The DIY Smart Home is arguably one of the first IoT-systems that also relies on configuration and management by non-programming users. This non-programming user population cannot be expected to be tech-savvy, or even interested in technology [72, 147]. In this vein, Brush et al. have identified poor manageability as a key barrier to the successful adoption of Smart Homes [72]. Users need clear and unequivocal methods for understanding what is going on with their systems and for making decisions about how they might best fulfil their needs. Such methods, for the reasons we have outlined, have to have a relevance to various user needs and need to service the provision of useful data monitoring devices.

In this paper, we therefore argue for adopting an end user development approach as a means of overcoming some of these challenges. End user development (EUD) has emerged as a way of enabling non-programming users to handle complex systems. Due to its emphasis on self-configuration, EUD is particularly applicable for the DIY 'Smart Home' [264]. We will discuss how intuitive and simplified user interfaces can be constructed so that they make much of the opacity of current Smart Home systems more transparent. Moreover, the flexibility of the approach provides for more individual management and, associated with this, greater possibilities in respect of reconfiguration over time. Some progress has been made in this regard. Trigger-action programming [502, 503], for instance, and rule-based systems have both been studied extensively [68, 264, 276]. In addition, flexible visualizations as a means of providing users with individually tailored feedback about what is being sensed in the Smart Home have been considered [43, 352]. In a long-term living lab study to understand the demand and potential for EUD in Smart Homes, Castelli et al. [89] found that, aside from understanding what is going on in the home, participants also wanted feedback on the system's

status. Their findings underscore the presence of the research gap addressed in this paper. For some of the more prominent use cases regarding Smart Homes (such as can often be seen in advertising), there are already very active research communities. Thus, designing energy consumption feedback has received a lot of attention [6, 124, 188, 447], including from an EUD perspective [259]. Designing for ambient assisted living has also generated a lot of interest [108, 252, 266].

Conveying *system status*, however, is not typically oriented towards informing a user about her/his performance, but rather towards making a system's behavior more transparent. Such system awareness has been shown to be an important feature in end-user configuration, especially for embedded systems [38, 372]. In an argument that echoes Dourish's discussion of system accountability [139], Lim et al., have also shown that limited system awareness may hamper user acceptance of context-aware systems [324]. Another user acceptance barrier is that people do not trust that Smart Home technology will be safe, secure, and privacy-preserving [100]. In this paper, we argue that system awareness helps users to build an understanding of data disclosure by helping them to learn about a systems' behavior and operations. Abu-Salma et al. [8], for instance, have shown that a lack of user understanding, compatibility issues, and lack of motivation rooted in a lack of understanding together contribute to a reluctance to use secure systems. Ruoti et al. have explored the reasons for this reluctance and have subsequently shown [430] how various trade-offs determine user policy.

However, so far, little research has focused on investigating Smart Home system awareness and how it evolves from a user's point of view. Woo et al. [523] have investigated ways of fostering understanding of rule hierarchies, suggesting ambient feedback as a possible solution. Yang and Newman have demonstrated how users demand Nest thermostats to provide incidental intelligibility in terms of their behavior and options [530]. The problem of exploring options and possible commands is particularly likely to increase with the onset of voice assistants. Mennicken et al. [349] have provided users in professionally maintained Smart Homes with system feedback embedded in a calendar. Despite these endeavors, supporting users in making sense of current and past system states remains an

under-investigated topic. Moreover, with the notable exception of Oulasvirta et al., who investigated surveillance by smart devices in the home [379], there is a gap in research relating to the longer term appropriation of (not only Smart Home) technology [351]. Evolving practices, changing levels of expertise and establishing routines around the use of Smart Home systems over time [395], all make designing for system awareness in DIY Smart Homes an ongoing challenge. The Living Lab approach we used constitutes one possible way of dealing with this lacuna.

Using a living lab approach [157, 185], we investigated evolving user demands regarding Smart Home system feedback for supporting system maintenance over time. Through a process of iteratively co-designing custom visualizations, we found that information demands and practices shifted significantly once the Smart Home system became embedded into the participants' everyday lives. By describing and analyzing these shifts, this paper makes a number of contributions:

- We report on and analyze perceived user needs for system awareness in DIY Smart Homes by examining the use cases pursued by participants and their respective information requirements.
- We identify event data structures and aggregations that participants relied on when trying to find information that could improve their Smart Home awareness and we demonstrate their potential application in Smart Home awareness interfaces.
- We examine an observed shift in information seeking practices towards "management by exception" in the later phases of Smart Home use and discuss opportunities for supporting this gradual shift through adaptive visualizations and interfaces.

Our findings can inform the design of DIY Smart Home systems to support both novice and experienced non-programming users in maintaining their Smart Homes. We conclude that this should involve the use of awareness mechanisms that consider how the relationship between users and their home technology evolves over time.

8.2. Background: Making the Home "Smart"

The first "wired homes" [26] were built by hobbyists during the 1980s and were highly customized and almost impossible to reproduce. The ongoing trend of

ubiquitous computing brought about a miniaturization of sensors and an increased energy-efficiency in wireless communication protocols and hardware. This, in turn, led to a new generation of commercially available Smart Home products. Low-power wireless protocols now enable these products to reach the most remote places in the home, often at some distance from power supplies, thus providing greater flexibility in the positioning of components. Some products clearly serve a single use case (e.g., IP cameras, light bulbs). Others (e.g., openHAB) adopt a platform approach. Such platforms allow the inclusion of a multitude of sensors, actuators and applications and sometimes support several protocols, thus enabling greater flexibility and interoperability. These Smart Home hubs can be tailored by their users according to their individual demands. The vast majority of advertised use cases, however, focus on certain key areas such as security, comfort, and energy saving [64].

Modern Smart Home systems fall into two basic categories: First there are professionally-installed and managed solutions. These dominated the market in the early days and typically featured wired connections between flush-mounted sensors and actuators (e.g., using the KNX protocol). Although wired systems benefit from greater stability and high bandwidth and are well integrated into the home, such systems call for higher investment and changes in the home infrastructure both at the point of installation and subsequently when users want to change the hardware configuration.

With the development of more energy-efficient wireless communication solutions, surface-mounted Do-It-Yourself hubs and sensors have entered the market (e.g., Samsung SmartThings, Wink Hub). They offer more flexibility when installing, (re-)configuring and extending the Smart Home and are especially designed to be maintained directly by users. As a result, both the opportunity, but also the burden of configuring the Smart Home has fallen to the user.

8.2.1. Understanding Everyday Life in Smart Homes

Home automation technology has been studied for well over a decade. For example, Zhang et al. [534] have investigated how to add context awareness to

Smart Home technology. Similarly, security and privacy research has recognized the Smart Home as a relevant domain [32, 109, 287, 498]. Several studies have focused on access control in Smart Homes [285, 343, 501]. Early work in this area was particularly focused on the technical feasibility of home automation and only relatively recently has attention to the relationship between technical and social aspects become more paramount [3].

A key part of the Smart Home vision is the notion of embedded technology. The associated challenges have been studied at a general level by multiple researchers, though few have tackled it specifically in relation to Smart Homes. Kranz et al. [300], for instance, highlight the tension between wanting embedded systems to blend in with their surroundings and the evident need for some human interaction with the system. For Smart Home systems, in an echo of Mark Weiser's original vision of ubiquitous computing [514], Davidoff et al. found that, rather than demanding control and information from users, the system should unobtrusively support them in their lives [126]. While we agree with this general point, we will show that the actual degree to which this is true varies over time.

Studies researching actual interaction with Smart Home technology "in the wild" are still limited in number and scope [350]. However, one challenge that has been commonly identified is controlling and managing the Smart Home. Randall et al. [404], provided an early ethnographic account of using and living with Smart Home technology where they found that control in the Smart Home was not merely a technological, but also a social matter in multi-person households. Jakobi et al. [258] studied the issues faced by users in a living lab when adopting Smart Home technology. Along four phases of appropriation, they identified challenges regarding information for making purchasing decisions, configuring the Smart Home to individual demands, designing information for evolving demands, and extending the system. Brush et al. [72] found that manageability and unreliable behavior were major concerns for Smart Home users. A particular problem has proven to be enabling non-programmers to successfully control and manage what amounts to a complex cyber-physical system. This remains one of the key challenges confronting the successful adoption of Smart Home technology.

8.2.2. Designing Feedback for Configuration, Context Awareness and System Awareness in the Home

The design of user interfaces that provide feedback from embedded consumer technology, including Smart Home technology, can roughly be divided into three main strands of concern: supporting users to configure a systems' behavior for individual use cases; feedback mechanisms as a means of gaining useful information about specific use cases; and informing users about the status and performance of the system itself.

Enabling non-programmers to adapt software to their needs is a core concern in end-user development (EUD) research [25,48]. EUD particularly aims to support users engaged in system (re-)configuration [142]. This is increasingly important as systems become more complex and interconnected [469]. Thus, the design of tools supporting system configuration constitutes a large part of the Smart Home EUD research [350]. Both configuration and individualization are known to be major success factors for Smart Homes [21]. Existing systems for configuration often use rule-based approaches, such as action trigger programming mechanisms, to implement automation and reactions to sensor states [128, 132]. A recent study by Brich et al. [68] suggests that process-oriented approaches may also be fruitful in supporting non-programming users in Smart Home configuration.

Providing feedback based on data sensed by ubiquitous computing technology is a commonly used mechanism across numerous different fields of research. For example, there are user-centered feedback design studies for life-logging [153] and self-tracking of physical activities [488] where the goal has been to try and design and structure sensed data that is meaningful for the user. For the specific design of feedback technologies in the home, there is also plenty of research covering different areas, such as the consumption of electricity [6, 188, 447] or water [155, 273, 478] and ambient assisted living [108, 252]. Here, EUD can provide a means of adapting dashboards and visualizations to individual needs by equipping end users with ways of modifying views on information without requiring programming skills.

While the above research focuses on harnessing and processing data to inform users when dealing with the case at hand, users are also face the task of controlling, maintaining, and potentially debugging systems. Research suggests that for these kinds of tasks, different information and modes of presentations are demanded. There is a difference in perspective regarding how to use the information provided. In contrast to Eco-Feedback, for instance, which seeks to support a households' energy consumption practices using sensors (and which could constitute or be a part of a Smart Home system), designing for the maintenance of complex systems requires the support of system awareness and intelligibility by making their health and performance accountable. Design addressed to a specific use case in what might be a Smart Home is conceptually different to supporting Smart Home system awareness, which addresses the administrative level of the system. So, in the case of energy-feedback, this might mean checking whether all the plugs are in working condition and that relevant rules for switching have been triggered correctly. Design for this kind of system awareness, however, has received less research attention to date [59], although prior work does highlight the importance of supporting the accountability of data in context-aware systems [43, 352]. Castelli et al. [89], for instance, have conducted a living lab study regarding information demands in the Smart Home and have found that the option to individualize visualizations was used frequently, to serve the purposes of both regular monitoring and short-term situational requirements for specific kinds of information.

A third major research topic in this area, aside from providing feedback and facilitating configuration, is making system behavior transparent so that users can explore a system's potential [246] and reason about its behavior effectively, thus facilitating its acceptance [324]. Research on *system* awareness typically does not target specific use cases directly, but rather seeks to provide meaningful support for understanding what the system is doing, what it is capable of, and potential anomalies. Frequently, this can also serve as a resource for maintenance and troubleshooting in case of breakdowns. Intelligibility [43, 324], in this respect, calls for providing ways of understanding current and past system states, e.g., to

debug potentially flawed configurations or check the system's current and past performance.

As Smart Home systems are among the first distributed cyber-physical systems to be managed by amateurs, there is a particular need to provide support for management of the system without any particular technical expertise. In relation to this, Woo and Lim [523] found that their participants had trouble understanding their Smart Home system structure. They therefore suggested providing ambient feedback regarding what rules were currently being applied to system components via the hardware itself. Looking at wired non-DIY Smart Homes, Mennicken et al. [352] found a calendar metaphor useful for visualizing sensor states and triggering rules in households where some familiarity with a Smart Home had already been achieved. It remains the case, however, that designing for system awareness in the domain of DIY Smart Homes is under-investigated with regards to (1) the instances in which system awareness matters to users and the kind of information they need; (2) how to support users in verifying system status, exercising the practices associated with awareness and disambiguating potentially complex feedback such as log data; and (3) the evolution of both users' expertise and interaction with Smart Home systems for maintaining system awareness over time, especially with regard to making systems more manageable, as well as facilitating management of data disclosure (i.e. privacy) in increasingly externally-addressable (i.e. IoT-based) environments.

So far, little research has focused on user behavior with respect to tracking and monitoring [379]. Epstein et al. [154] identify a variety of behaviors that inform self-tracking. Although this work was focused on people who actively self-track, it captures the range of motivations, reasons and review procedures that such users adopt. Epstein et al. also examined the various reasons why self-tracking behavior lapses, noting, for instance, forgetfulness, difficulty in managing upkeep and deliberate suspension. They recommended that design should incorporate features that encourage the avoidance of inertia, that support a variety of goals and that support resumption after a lapse. Van Kasteren et al [37] point to sensor technology that could automatically track user activity, using probabilistic

models. However, as this is predicated on data collected via Bluetooth headsets and, moreover, based on activities taking place in a single person household, such data can inform about behavior but not about the reasons for it. In line with Tolmie et al. [495], we argue that understanding the reasoning that informs behavior is important. To uncover users' requirements regarding Smart Home system awareness, we accompanied households in their struggle to set up and configure their Smart Homes (as well as their lives) in the way the wanted them by using DIY Smart Home technology. This covered both early and later phases of use. Our goal was to provide an account of what information users sought to obtain and how they maintained system awareness throughout the different phases of their experience of living in a Smart Home.

8.3. Method

In our study, we followed a design case study approach to inform the design of our Smart Home interfaces, as proposed by Rohde et al. [420] and Wulf et al. [527, 528]. This approach advocates a long-term view of the investigation-design-appropriation cycle. In our application of this particular approach, our broad interest was in the appropriation [84] of Smart Home technology. However, one particular analytical lens was focused on investigating the resources and means participants require when monitoring their Smart Home system and how they maintain awareness of it in real-life contexts. This is the theme that we have specifically sought to examine in this paper. Overall, we used a living lab approach to understand users and their contexts and to investigate how they used Smart Home systems in real-life environments [157, 185, 320, 376]. Living Labs allow different stakeholders from research and design to be brought together with users and technology in an open-ended design process in a real-world context [185]. Such frameworks are especially well-suited to the support of long-term cooperation, co-design and collaborative exploration among researchers, users and other stakeholders. The advantages of the Living Lab approach lie in its flexibility, how it provides creative spaces for the discussion of new concepts and how it supports long-term observational studies and, where necessary, lab-based

interventions that are designed to assess the *long-term* appropriation of new IT-artefacts [376].

8.3.1. Setting up the Living Lab

This research was embedded in the context of a larger living lab research project. We ran our living lab with 12 households (29 participants) over a period of 26 months. We started recruiting interested households via local press and radio stations in early 2015. Applicants signed up via a website, which allowed us to gain some basic information regarding their living conditions, technological equipment, and expertise.

In a thorough selection process involving over 100 interested households, participants were chosen so as to constitute a diverse sample stratified in terms of age, gender, household size, rented or owned homes, houses or apartments, rural or urban residential areas and tech-savviness, as well as educational level. Additionally, households had to have an internet connection with a minimum speed of 2MBit/s and a smartphone.

The final sample of 12 households (Table 2Table 5) with 29 participants consisted of two single-person households, five multi-person households without children and five multi-person households with children. Three households lived in rental apartments, while nine owned their homes. The participants' age was between 27 and 61 years. For participation, we offered no compensation, except being able to use the provided hardware and software. Motivation varied, ranging across dissatisfaction with existing Smart Home systems and technological interest, to curiosity about being part of a research study. Almost all (i.e., 10) of the households did not currently have a Smart Home system installed. In order to include more experienced users, however, two households were recruited that already had a Smart Home system in operation and three others reported having experience with networked energy monitoring devices. These systems were either DIY Zigbee- or ZWave-based multi-component systems, similar to our system, but incompatible.

Table 5: Overview of participant sample in the Living Lab

	Household size	Type of housing	Location	Tech. Knowledge
H1	2-pers. household	Apartment	City	Yes
H2	3-pers. household	House	Rural area	Yes
H3	3-pers. household	House	Rural area	Yes
H4	3-pers. household	House	Rural area	Yes
H5	4-pers. household	House	Rural area	Yes
H6	2-pers. household	House	Rural area	Yes
H7	2-pers. household	Apartment	City	No
H8	1-pers. household	House	Rural area	No
H9	3-pers. household	House	Rural area	No
H10	2-pers. household	Apartment	City	No
H11	1-pers. household	House	City	No
H12	3-pers. household	House	Rural area	No

Two 2-hour workshops were conducted at our university, subsequent interviews (45-90 minutes) were recorded during on-site home visits. Although we always invited all members of each household to participate, on most occasions the original applicant was our primary contact.

The overall project for which the participants were recruited aimed to study Smart Home user experience. In this paper, we focus specifically on how the participants managed their cyber-physical Smart Home system in terms of maintaining it, handling errors, and tracking and correcting any perceived system faults over time, as they were getting used to the system and slowly incorporating it into their everyday lives.

8.3.2. The System Provided to Households

The system[4] used in our study was a commercially available off-the-shelf system, which incorporated a range of features common in DIY Smart Home products. The system was based on Zwave and relied on a coordinating hardware gateway that managed the connection for remote access and data upload. Measurements

[4] We provide a description of the Smart Home system we used but refrain from naming the product or providing screenshots because of a respective agreement with the vendor.

and rule sets were both uploaded into the vendor's cloud, which allowed for complete remote control of the system. At the same time, the local gateway also stored the program logic in order to achieve independence from internet connectivity. The internet connection was only necessary when users wanted to change the systems' configuration. The system's ecosystem offered a variety of sensors and actuators from which households could choose freely (this was covered by the project budget). Overall, the households selected 14 room thermostats, 31 radiator thermostats, 14 motion and brightness detectors, 29 door-/window contacts sensing open or closed states, 45 smart plugs for measuring electricity consumption and switching appliances, 6 remote controls, 11 freely-positionable

switches supporting two or four different positions, and 10 smoke detectors. The chosen devices varied slightly according to the perceived use cases, with some households focusing on security (movement detection and door-/windows sensors), and others favoring comfort or energy monitoring with thermostats, brightness sensors and smart plugs. Due to the systems' flexible plug-and-play adaptability and extendibility, the households were also able to include further sensors, e.g., for implementing new use cases that emerged over the course of the study. This typically happened when participants realized new possibilities or learned about other households' setups. Within budget limitations, some of the additional devices were provided by the researchers. However, others were also bought by the households themselves, such as cheaper third-party sensors with the same capability as those originally offered, smart LED lamps, and networked weather stations. In terms of software control, the system supported the setup of automated rules in an if-this-then-that style. Additionally, "scenes" enabled the definition of certain states for multiple actors. For example, a "Watching a movie" scene could be instantiated such that several lights would be dimmed or set to a predefined desired state and a smart plug could switch on all the necessary entertainment devices. In a third component, groups of multiple devices could be defined, for example all of the sensors in a room could be grouped together.

For visualization, the system used a dashboard approach for both native applications (iOS and Android) and a web-based interface. As well as being able to check and control all system devices with independent widgets, the dashboard also included a local weather widget and a text-based home-log widget. The latter listed all changes in a sensor's state and triggers (motion detection, on/off for smart plugs, windows/doors opened/closed, etc.) and general information on the system state (re-/boot of the system, dis-/connection to the internet, updates, etc.) over the previous 48 hours.

As these interfaces were part of the vendor's product, we were not allowed or able to modify them. Therefore, all data collected by the gateway was exported to a local Raspberry Pi and sent to a custom open source visualization framework based on open.HOME (see Figure 2). This framework enabled us to use web technologies (Javascript, HTML, CSS) to freely design alternative interfaces using the data provided by the Smart Home systems' middleware. In addition, when we began collecting data from the gateway, we found that it was collecting

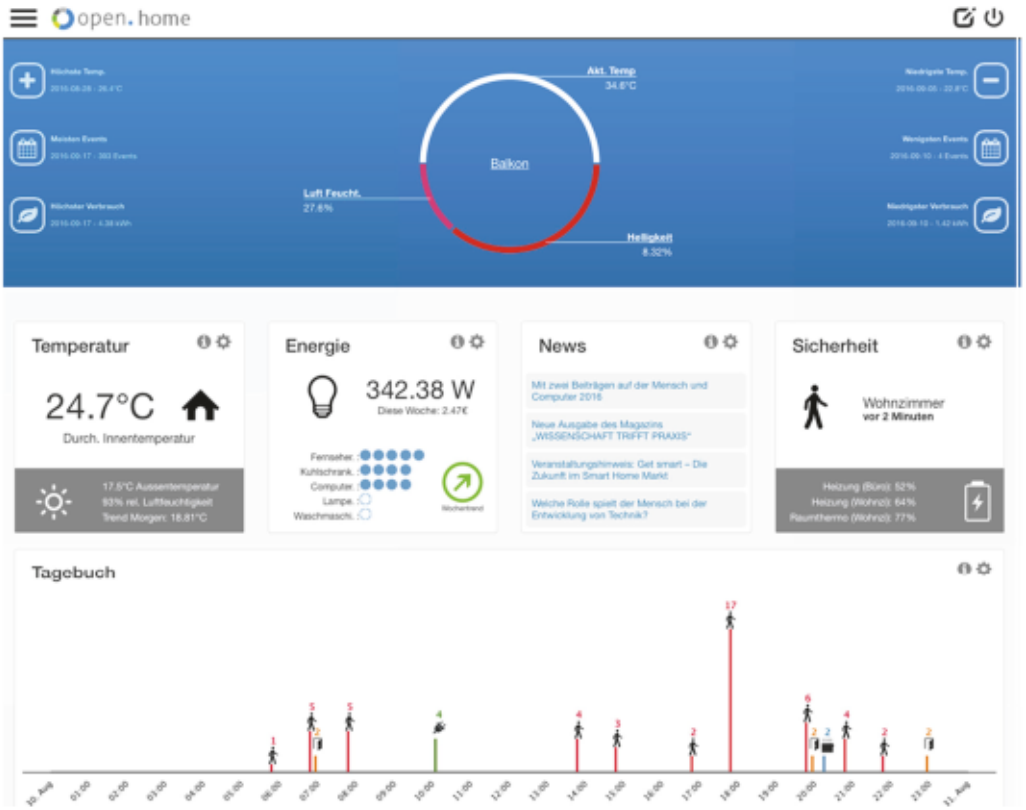


Figure 2: The home screen of the open.HOME interface with the first version of the system-awareness log at the bottom.

much more data than the commercial frontend was using. This, then, provided us with even more flexibility in reacting to user demands. The open.HOME framework was itself developed on the basis of user demands we had identified at the beginning of the study. It was therefore made available to the households after about 13 months. While both interfaces remained active, once it was available, open.HOME was used more frequently by the participants.

8.3.3. Research Activities on Smart Home Awareness

As described above, the work described here formed part of a three-year project that generally sought to identify and tackle user experiences of DIY Smart Home platform systems. For the early stages of the research, Smart Home system awareness was not a particular focus. However, over time it became clear (and more specifically during the course of two rounds of interviews) that users often struggled with understanding the system's behavior as well as what its potential might be. The main part of this paper focuses on presenting findings from a set of research activities that we explicitly developed to uncover instances of people trying to understand and keep on top of what their Smart Home system was doing, together with our design of the supporting visualizations (see Figure 2). Following the design case study approach described by Wulf [528], we first sought to gain an understanding of the phenomenon of coping with the Smart Home in general. Participants' challenges were then successively identified from our empirical work, leading to the iterative development and testing of prototype interfaces for Smart Home interaction in the living lab's real-world environment, with the goal of supporting users in their everyday life within their Smart Home. With each analysis of the empirical data iteratively informing the design of the following phase, we were able to ground the research and take into account the participants' evolving practices (see Figure 3). We thus progressively focused on: (a) exploring

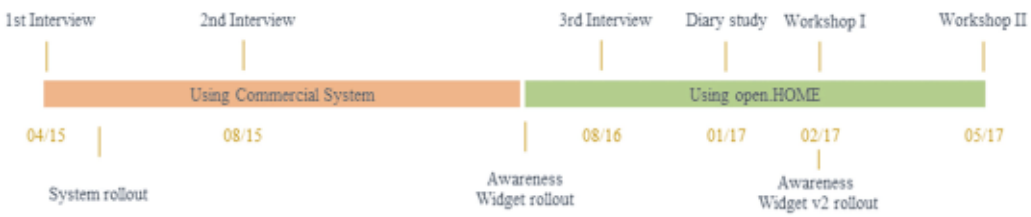


Figure 3: Timeline of research interventions and visualization rollout in the Living Lab.

the information demands of novice users; and (b) understanding the patterns of use exhibited once participants became more experienced.

Exploring the Information Demands of Novice Smart Home Users

To gain a contextual understanding of what households planned to use or actually used the system for, during the first phase of the study, we conducted two rounds of semi-structured interviews with all of the households and observed the process of system installation.

The first interview was conducted before the Smart Home system was rolled out, with the intention of exploring participants' initial wishes and their anticipated use of the system. The participating households were invited to talk generally about their interest in Smart Homes and envisioned use cases for the Smart Home technology. They then chose the sensors and actuators they wanted to use in their Smart Home setup.

Shortly afterwards, we observed the participants installing the system in their homes either directly (n=6) or through video self-documentation (n=6). To support this process, and as a means of maintaining a close connection with the households and being able to collect feedback in-situ, a mobile feedback app was provided to each household and a mobile instant messaging group for interaction between the households and for exchanges with the researchers was instantiated.

After four months of living with the Smart Home system, a second round of interviews focused on having the participants reflect on the system's performance so far and on how the system had been embedded into their daily lives. This initial round of empirical work motivated the design of an awareness widget for the Smart Home, which was subsequently rolled out and evaluated.

Prototype Evaluation and Understanding the System Awareness of Experienced Users

For the second part of the study, we used the open.HOME visualization framework to prototype system status visualizations with the participants. This

was mainly aimed at flexibly supporting the use cases participants envisioned. We conducted three main interventions in the households, which are described next.

Having analyzed the empirical data from the first two rounds of interviews, the feedback tool and informal discussions in the messaging groups and from informal meetups with households, we started to focus on the system's intelligibility for the users and the role this played in users' efforts to maintain their system, thus narrowing our broad initial research questions about 'user awareness.' In conjunction, we rolled out a visualization tool to support users in understanding system (mis-)behavior.

Six months after rollout of the initial awareness widget, we conducted a four-week diary study in order to get a better picture of evolving practices. Informed by cultural probe approaches [193], we asked participants to write a digital diary about when they interacted with the system for maintenance or troubleshooting. Again, we focused on information demands and instances in which households sought information about what was going on with their Smart Home system. To provide some basic guidance, we formulated questions that might be answered in this diary, targeting both satisfied and dissatisfied information demands. For example, we asked, what households wanted to know about their Smart Home, how they tried to obtain the information demanded and whether they were successful.

After the diary study, we conducted two co-design workshops in which we asked participants to reflect on their most significant information demands, as suggested by the collected data, and on their strategies for interacting with the Smart Home system to satisfy those demands.

The first workshop was divided into three phases: First, we asked households to share and discuss their views regarding the system's potential for clearly conveying its behavior via feedback widgets. We asked for their views upon both the original commercial solution and our self-developed widget in this regard. Second, we encouraged the participants to envisage a solution that would best

address their need for monitoring and control without considering any technological restrictions, i.e., we wanted them to start with a "blank slate". Finally, in the third phase, critique and dreams were brought together to find realizable solutions. This approach enabled us to follow a two-fold strategy: (1) Collecting input for improving the existing system awareness widget, and (2) providing scope for the potential evolution of the participants' demands for system awareness, as they became more sophisticated users of the technology i.e. further appropriated it.

The second workshop followed a similar structure in order to further explore new ways for providing system awareness brought up in the previous workshop. We presented a second version of the awareness widget we had developed, based on user input and asked the group to discuss its advantages and disadvantages. In a second part of the workshop, we more specifically focused on feedback regarding new channels for providing system awareness, both within and outside the open.HOME system. The options here included a PC, a tablet, a smartphone, or any kind of ambient display. We provided printed templates for smartphones and for a PC browser view of open.HOME with blank pages. The participants were given markers and asked to scribble onto them their preferred enhancements to the existing system.

Data Analysis

All interviews, workshops and on-site interviews were audio-recorded and transcribed for later analysis. The analysis drew upon the transcripts and upon written feedback from the diary study. These documents were processed individually by two members of the research team using thematic analysis with an inductive coding process [66].

In our analysis, we were particularly looking for instances of system information-seeking, the reasons for this, how the system feedback was used and any relationship between these aspects. We found that barriers relating to debugging the system and the need for adaptive feedback to meet individual requirements

were the most common issues raised. All empirical data was translated from German into English by the authors after analysis.

8.4. Findings: What, Why, and How is my System Doing (What)?

We have organized our findings around practices of obtaining and maintaining system awareness according to whether it was (1) novice users using the default visualization provided by the vendor, or (2) more experienced Smart Home users in the later phases of appropriation using the open.HOME dashboard. The first part is fueled by the thematic analysis of the two interview studies, while the latter is based on the diary study and both design workshops.

8.4.1. The Need for System Awareness among Novice Smart Home Users

The findings described in this section are based on our analysis of the interview data and articulate the main themes we uncovered regarding the use of the system awareness tools provided.

The Need for System Awareness and Lack of Feedback Mechanisms

In our field studies, we quickly identified a difference between system awareness and home awareness among participants. On the one hand, the home log (see Figure 4) was used to support awareness of the home as a place, as it was the only interface that showed all events the system sensed or triggered. The need for this was mentioned in the very first interviews, even before the system had been rolled out. For example, a participant stated:

> *"I would love to maybe be able to take a look into my house remotely, to see if everything is in order."*

Such check-ups on the home were unspecific with regards to purpose, but spanned across multiple use cases and were common to Smart Home products in general. So, participants looked at the energy consumption of devices or of the overall home, monitored the home's security and checked the temperature in certain rooms to ensure comfort throughout the Smart Home.

However, after the installation and initial configuration activities, many users still felt uneasy about the system and whether they could trust its performance. Fearing unintended system behavior or that they might have somehow configured it incorrectly, they wanted to understand what the system was doing and assess whether it was behaving as intended. One participant checked whether the smart thermostat's heating behavior was accurate. The household had defined timespans in which they were not at home or sleeping, during which time the living room thermostat could be turned down:

> *"I checked the system to see if something had failed, like my heating control at the beginning?"*

This example is fairly typical. When it was difficult to follow the system's activities from observing sensor and actuation behavior, participants turned to the home log to check whether triggers and rules had been executed successfully. The absence of overt feedback channels led to an awareness gap amongst the users. Uncertainty and a general lack of confidence in their own configuration skills and the reliability of system performance went so far that one household decided to double check the effects of their remote commands via an installed IP camera:

> *"[When we were on vacation] we sometimes [remotely] switched on the light in the hallway. [...] Then I simply used my smartphone and switched it on and in doubt, I double checked with the camera whether it actually was turned on."*

We also found other less common strategies for acquiring system feedback, highlighting that households sometimes sought to establish their own feedback channels in the absence of suitable pre-defined mechanisms. One household, for example, set up a rule so that an email would be sent whenever a door contact was triggered. This was not for security reasons, but rather to check whether the system was accurately sensing events. An important contributor to the uncertainty here was that the remote control functionality lacked feedback mechanisms, so households were not always sure a desired action had actually been performed by the system.

Limitations of the Default Home Log: Clutter, Unprocessed Raw Data and Limited History

During the initial phase of installing and configuring the Smart Home, households used the home log (Figure 4) provided by the commercial vendor as a feedback channel for testing their configurations. For instance, they experimented with the sensitivity of brightness sensors in order to understand how to set thresholds for switching on lights. This pattern of trial-and-error configuration was evident across all households and resulted in rather unsatisfying and lengthy setup sessions for some participants. In particular, the home log's long and unfilterable list of events hampered their ability to gain an overview. This is in line with Lim et al.'s findings regarding system transparency [324].

The lack of overview provided by the default home log widget also severely limited the possibility of finding patterns in observed system failures. Participants struggled to identify rule correlations because only single sensor events were shown. A combination of insufficient means for understanding system behavior and perceived poor system performance in terms of rules not being triggered or commands not getting through even resulted in some users ceasing to use certain use cases:

> *"We still haven't figured this out, [why the rules for controlling the light sometimes go mad]. It sometimes remained on, sometimes it switched off just to switch on again, so that we found the lights on in the morning."*

In all likelihood, the Smart Home was performing actions based on triggers defined by the users. However, the lack of transparency regarding system behavior made it difficult to identify what exactly triggered the lights to turn on or off. Participants expressed a strong sense of the system behaving like a 'black box.'

When users wanted to regularly monitor the system's status and behavior, the embedded limitation of only showing 72 hours of recorded events seriously limited participants' ability to make sense of events. As a result, navigating to specific points in time in the log was burdensome or impossible. This is reflected

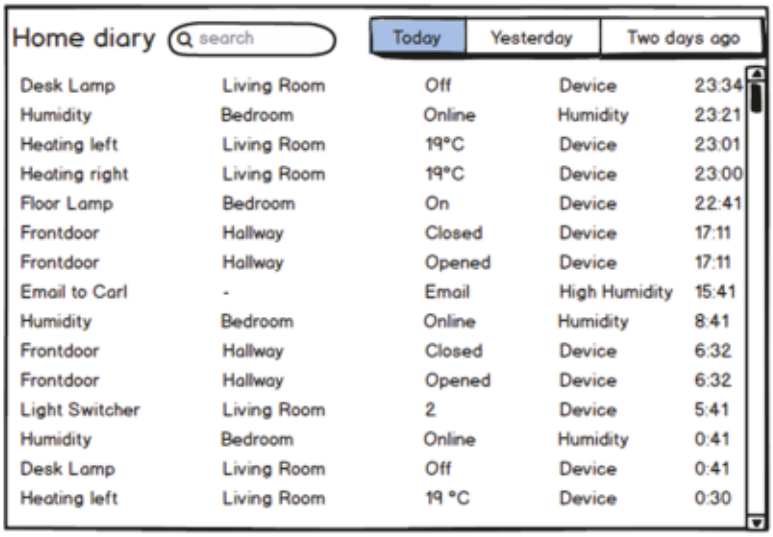


Figure 4: Mock-up of the vendor's official home-log interface as part of the web-based dashboard.

in how one participant described what happened when he tried to check on the system while the family was on vacation:

> *"You can basically forget the Smart Home diary log. Because with a history limited to the day before yesterday, this is totally uninteresting."*

Overall, then, as we have intimated, a limited history hindered participants in making sense of patterns of events as patterns were removed after 72 hours.

Privacy Considerations

Despite its shortcomings, the way in which the home log visualization brought together information from all installed sensors facilitated an awareness of possible privacy implications. The following household reported checking the home log and noticing that by interpreting the motion record and door-opening sensors, third parties would be able to infer presence and patterns of entering and leaving the home:

> *"After looking at the home log, I realized what information the Smart Home collected. Especially, in terms of motion profiles, because these are safety-critical information."*

Overall, however, data being transferred to the vendor's cloud backend was not considered to be a critical issue by the majority of participants. We had not explicitly brought up the topic of privacy but it is notable that households typically did not volunteer many concerns about privacy implications. There were, however, a few exceptions. For example, one participant talked about his perceived privacy implications after having used the Smart Home for four months:

> *"For now, I don't see any way of misusing my data that could turn out to be my downfall. [...] It would be nice, however, to see what data is transferred or stored. If I can control this, it's on me to decide what may be transferred or used."*

While he did not worry about the data in general, he admitted to not having any means for actually checking what data was being collected and transferred and felt it would be better if he could control the flow of data.

Initial Guidelines

Overall, the relatively simple log system was found to be an important factor in households being able to maintain control of the Smart Home system and it loomed large in establishing and maintaining a sense of system reliability, as well as their own ability to handle and configure it.

Based on our exploration phase, we defined the following design considerations for an improved log widget, which are reflected in our co-designed awareness widget (see Figure 5). While some of these guidelines merely reflect general design considerations, others highlight the importance of relating the operation of the widget to existing practices in order to demonstrate how the Smart Home was either integrating or interfering with the household ecosystem:

- **Consider levels of detail required:** Trust in the system was a major concern for users and getting used to the remote control of devices in the home was not always easy. To support transparency, we found that households wanted more detail regarding automatically triggered rules, user-triggered commands and system events. Right from the start, our first prototype enabled users to see the

complete history of their logs. In addition, participants were not looking for a reduced information load. Instead, when they wanted to understand the system's behavior they wanted full details about past statuses and the performance of their Smart Home. In the re-designed widget, next to an overview, a tooltip was provided for each sensor event, showing the exact time and value set for the component.

- **Use time as a structure:** As a counterpart to detail, time was a structuring metaphor in our improved design. In the exploration phase, we observed that many rules were triggered by time, brightness and movement (with about 40% of all events occurring regularly [127]). We therefore used one day as the default timespan for viewing all system data at once. A zoom-function also allowed for detailed views.

- **Present home activities instead of raw data:** To cope with existing and increasing amounts of data, we provided levels of abstraction and contextual cues that were meaningful to households. Next to providing the triggering ("if this") sensor state and the executed action ("then that"), or the initiated singular actions when triggering a defined scene, we directly included the rules and scenes into the awareness widget. The goal was to prevent reported situations in which sensor events (e.g., movement sensors) jammed the home log with a plethora of events. To reduce clutter, movement detected in frequent intervals was interpreted as an ongoing movement activity detected by the sensor, which we represented with one starting point and an end point.

- **Longer-term data availability:** Households wanted to check past system status at a glance, e.g., for debugging purposes. However, the existing text-based feedback solution did not allow them to check easily whether rules were executed, e.g., whether a window had been open or closed at a certain point in time, as only the change event itself was included in the log. What the participants really wanted was to be able to watch the system status and its change. As further support in this regard, we moved to having statuses such as windows being open or switches being on displayed as a continual line graph, with no graph if they were closed

/off. Similarly, varying thermostat values were represented through vertical variation in a line graph (the higher the temperature, the higher the respective line graph).

8.4.2. Evolving Demands for System Awareness

Based on our findings in the first phase, we designed an initial, more flexible and visual home-log which was introduced as part of the rollout of the open.HOME framework (see Figure 6). Once introduced, participants could add and remove the widget from the dashboards' home screen, as well as adjust its size and position. After the participants had used the new interface for four weeks, we conducted a third round of interviews, followed by the diary study and the two workshops. The results showed that the system needed to provide different kinds of feedback views, depending on the kind of information request they had. We also found that participants' information practices had shifted significantly. Once they had reached a stable configuration for their Smart Home, users were more interested in ambient feedback than in detailed logs and minimal information on system status. The first effects of installing and needing to configure the system started to wear off after between a couple of weeks and three months, depending on the technological experience of the households. Whenever the system was changed in terms of either software or hardware, however, there were renewed demands for greater levels of system feedback in subsequent weeks while people kept monitoring whether the new configuration was working as desired.

After three months there were 1,394 page visits to the interface (70% from desktops, 24% from smartphones, 6% from tablet PCs). The wearing off of need was demonstrated in particular by the fact that during the initial two weeks, the average visit duration was significantly longer than it was later on. Overall, 60% of all visits lasted less than ten seconds, while 28% were longer than three minutes.

Tailoring System Feedback to the Demands at Hand.

Further evaluating the open.HOME widget, we found that, along with a decreased use of the dashboard, detailed information regarding system conditions and behavior was less important to the users. Instead, they wanted more detailed

interfaces to be available on demand, matching observations originally made by Shneiderman [455].

> *"I think I would want to look at this more closely [when there is an error ...]. If something was really wrong, I would just zoom in and look at it [...]."*

Over time, households got used to the system and were able to understand and explain things, i.e., develop an account for its behavior for themselves. This evolution in their information demands was not only influenced by their increasing expertise in handling the system and the stability of configuration, it also related to the number of components being used. At the beginning of the study users started out with about ten components. Participants added more components if and when they had an interest or saw the need. Some households ended up with more than 30 installed components. In cases where households had a large number of sensors, participants tended to feel overwhelmed by the amount of information available on the dashboard and feared losing an overall sense of what was going on.

> *"However, the more [components] I add, the bigger is the danger of an overload on my end, and the important information just [slips by]."*

In order to help participants retain an overview yet still be able to focus on specific informational needs as they arose, we added a simple filtering mechanism, so that

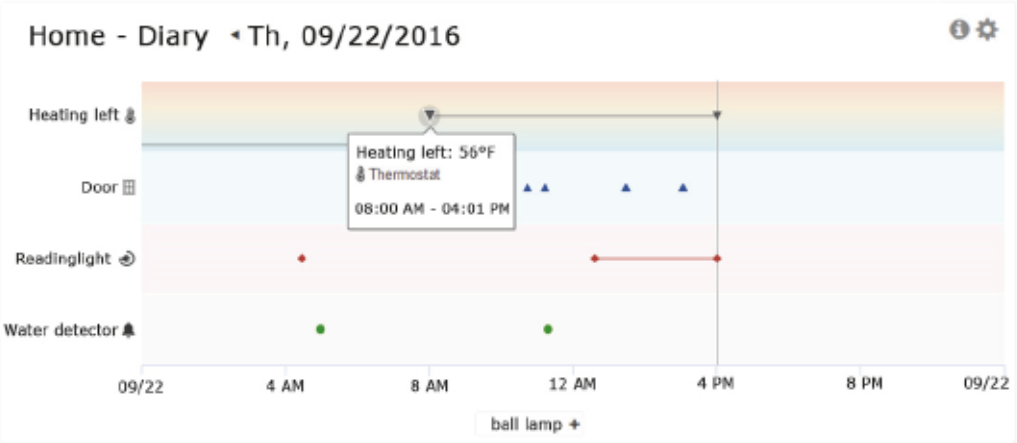


Figure 5: The co-designed system awareness widget for the web-dashboard, with a tooltip and the possibility of deactivating sensors (here the sensor "ball lamp" is currently removed from the graph).

on demand the visualization would only show specific sensors and events of interest (see Figure 5 where the "ball lamp" device has been excluded from the graph).

Management by Exception.

While in the earlier part of the study participants were looking for very detailed and varied information regarding the system's status, in the period leading up to the diary study this had changed and diminished. The two workshops towards the end were designed to allow participants to express and explore new ways of acquiring system awareness apart from the widget. Here, we found that, once users had mastered the system, they wanted the interface's content to change in significant ways:

> *"I know in the beginning I was a great advocate of information. [...] But only information from my household? Well that's just [not relevant anymore]."*

In this later stage of the study, participants were only interested in receiving Smart Home system information if something was not working, needed their attention, or required active maintenance. Examples include changing batteries or re-connecting components that had lost contact with the central gateway. Households now expressed interest in a distinct, aggregated view relating to their routine behavior. They wanted the system to be able to learn about the household's routines and thus detect when something was not working as expected. Put simply, incongruities with household rhythms defined awareness needs to a significant extent and sometimes that meant there was no desire for additional information at all. :

> *"I don't want to know things in depth. Except for when something is wrong. [...] If I am coming home and the system is fine, just the way I want it, there is nothing I need to know."*

Some households reported that instead of using the open.HOME interface their awareness of system status was now provided for implicitly by observing whether the system acted as desired. To help participants avoid unexpected malfunctions

and breakdowns of the system, we aimed to provide households with new means of acquiring system awareness. During the workshops, we let participants draw what they would consider their 'perfect' awareness widget and found that they focused exclusively on warnings and notifications. In its purest form, one participant drew a very high-level, binary status icon into the top bar of their smartphone so that they could always see whether there was an issue with the Smart Home system requiring their attention (see Figure 6). They only wanted to use the full-scale widget if they needed to dig deeper.

While the open.HOME awareness widget was considered helpful, at this stage they considered it too complex for ordinary regular monitoring. Feedback on the system condition was only required if something was clearly wrong, e.g., system breakdowns or deviation from the home's "normal" state.

> *"Well, a green dot would be enough for me, and if something was weird, it would just turn red."*

Figure 6: Detail of a design scribble for enabling management by exception on a smartphone.

Participants expected the Smart Home system to 'know' what counted as normal and thus be able to report deviations. For example, room temperature was deemed irrelevant as long as it did not differ from the desired, i.e., defined or usual, temperature. Similarly, the state of electronic devices was typically found uninteresting, except for when a programmed rule failed to execute. This stands in sharp contrast to the initial behavior, when constant double-checking of the execution of commands was typical (e.g., via an IP camera). Equally, motion sensor activity was only considered important if it was outside of usual or expected periods of activity. The only cases in which households wanted information unconditionally, was when batteries were running low or rules had not been triggered automatically.

Embedding Feedback in Everyday Life.

With households getting used to their Smart Home and having more stable configurations, interaction with the rule editor and the dashboard decreased and it was found to be mostly unnecessary. In the workshops, the households expressed the view that they would not use the home widget regularly because it was not the kind of interface they needed for daily use. While they did still feel that the existing feedback widget would be useful on occasion, providing an actual desktop or mobile interface seemed to be beyond what was required for everyday access. Instead, the households wanted system feedback to be more embedded into their everyday lives. During a workshop imagination phase, one participant expressed this view quite clearly:

> *"In principle, I never want to have to use the tablet, the laptop or my Android. Really, only if totally necessary, and I would like to have [Amazon] Alexa tell me that something is wrong in my Smart Home."*

While not all of the participants were comfortable using voice assistants, the embedding of the technology in the fabric of everyday life with no overt presence was considered crucial by all of them. Suggested solutions largely focused on technologies that were already being used in daily activities, such as smartphone push notifications or a widget on the phone's home screen, or having a dedicated ambient display in the kitchen or the hallway that could just display system conditions, thus enabling the noticing of errors in passing (Figure 7).

> *"Last time, I said I only wanted to be warned of important stuff, but I kind of moved away from that idea again. [...] I'm currently thinking to install a display in my entrance [for the home-log]."*

There was still an interest in supervising the system state, but at this stage of appropriation participants wanted this information to be unobtrusively embedded into the flow of their everyday life. Even push notifications were seen as a potentially problematic form of system feedback in terms of possible information overload:

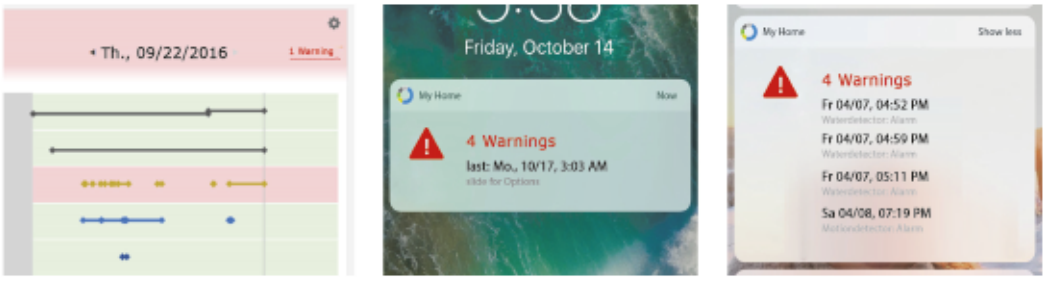


Figure 7: Low level prototypes of households' suggestions to provide system awareness in later phases of use. All scribbles focused exclusively on providing warnings on dedicated displays or smartphones.

> *"Well you have to see that you receive push notifications not only from your [Smart Home] system, you maybe have other things doing that, too. And then there is the topic of information overload – you might end up overlooking a notification or misjudge it."*

As a result, participants quickly imagined a classification of urgent messages that should be pushed and others that should not interrupt or distract users from what they were doing. Ambient displays and voice assistants were also criticized because of their privacy implications. System feedback information needed some security they argued. At the very least safety- or privacy-critical information should not be just available to people passing by or visitors:

> *"Security-relevant stuff of course should not be visible there. Alternatively, they should somehow be secured."*

Overall, in the workshop, users expressed a preference for staggered interaction. One should be made aware of a possible issue via a push notification on a smartphone. There would then be a status light or ambient display that indicated the status more concretely. After this, it would be possible to dig deeper into things using the home awareness widget on the same device.

8.5. Discussion

With Smart Home systems entering households, we have another case where systems and, in this case, cyber-physical systems, are in the hands of users who might not know a lot about, or even be interested in handling technology. In particular, Smart Homes that are not installed professionally make the user the

system's administrator. In this regard, our study provides insights into how to design for DIY Smart Home awareness beyond building rule systems and understanding their hierarchies [68, 128, 523]. We argue that more attention needs to be paid to exactly what it is that users want and need to be aware of, when, and why (see [389]) and in which stage of appropriation. This will entail presenting Smart Home hardware components and logic in an intelligible fashion, such that users can understand "the story a system tells about itself" [139]. [116]).

We find that, besides supporting installation and configuration, as well as information visualization that enables people to pursue the use cases made possible by Smart Home technology, the system's ability to make its own actions and status available and accessible was an important factor in people's acceptance of this technology within their home. Over time, and especially in situations of breakdown and (re-)configuration, we found that participants required their system to provide information about itself [141] in order to increase its accountability [43] and credibility [184].

In this section, we discuss our main findings by relating them to existing work and describing the limitations of our study.

8.5.1. Limitations

It could be argued, that some of the challenges that confronted our households were specifically related to the products and the Smart Home system we chose to use. Having described the system in 8.3.1, however, we feel it is fairly in line with the dominant form taken by DIY Smart Homes, from both a technological and interface perspective. Moreover, our study does not merely provide insights regarding the challenges that participants faced, but rather focuses upon their information requirements with respect to the status of their home's system. Dashboards and if-this-then-that rule definition mechanisms are, of course, already common features and we assert no originality in relation to our visualization techniques. Additionally, the rollout of the awareness widget did not consider seasonal differences or summer vacations and – due to the nature of our study – could not be tested during the setup phase. Although our workshops

revealed that voice feedback and routine patterns for aggregating system views were promising, technological restrictions meant that we were unable to implement them in our study.

Additionally, the study did not take into account possibly conflicting voices or information needs among household members. Other studies, less geared to the building of new interfaces, have certainly shown that such needs, and their management, vary considerably from family member to family member [397, 398, 496]. Our study was not so much concerned with these issues, but we recognize that our method might not have been suited to getting an understanding of the implications 'gatekeeping' functions may bring to family life. Participants were not paid for participation and it is conceivable that participants were biased in so far as they may have been generally positive towards technology or the specific product. We think this unlikely. A relatively small sample of households cannot be representative of all possible household variations but we initially sought to only include households interested in having a Smart Home system for the reason that they would be more likely to continue to participate throughout. We then took care to recruit a mix of tech-enthusiasts and regular users.

During our research, we built several working prototypes for a web-based visualization framework presented in the paper (shown in Figure 2 as part of the dashboard, and Figure 5 in detail). This helped us, testing out the need for certain kinds of awareness tools and how they evolved over time. However, we did not build a working prototype implementing the final set of features we identified mainly for technical reasons: As described, we were not able to deduce routines from existing log files, and thus were unable to include activities in the visualization. Moreover, with the Smart Home product in place, our prototype was unable to access rules as defined via the system to appropriately reflect them. We believe, however, that Figure 5 gives a good notion of our implementation of the design guidelines already. Finally, since our research was qualitative in nature, this study should only be taken as a starting point for further evaluation of our suggested design implications.

8.5.2. Drivers of Acceptance and System Usability

Making the System Intelligible by Relating it to Routines.

During the initial months of living with the Smart Home system, in which participants wanted to configure it and set up specific use cases, all of the households sought on specific occasions ways of acquiring system feedback regarding its current or past state to check its performance and activity. The commercial system we rolled out made it difficult to accomplish this.

The natural rhythms of the household affected what it was that people wanted to monitor. Whether or not system states were of interest depended on the time of day, the quality of available light and on the kinds of movement in the household at that time [16]. Data became usable in and through households' understanding of the relationship between the system state and their household and environmental rhythms. In turn, this implied that, one day as a standard view on data was the quasi-natural interval for households.

We also found that participants sometimes wanted to be able to see all of the data the Smart Home was collecting; either for debugging or privacy reasons [287]. Again, existing systems typically have limited self-explication capabilities, which are often restricted to triggered rules or sensed events of limited intelligibility.

In our study, households sometimes came up with several aggregations of single events that they perceived to provide meaningful guidance in a log. For instance, they discovered that rules can be an aggregate of triggers and events, as can be the logging of triggered scenes. However, as noted above, another important way of aggregating data in a meaningful manner was predicated on people's own routines and rhythms. The Smart Home, we argue, should detect existing daily patterns and activities on its own and inform users about relevant deviations from typical patterns and routine behavior. Some of the participating households had more than 40 sensors, so inferring what is 'routine' in such a complex ecosystem might be a non-trivial problem. However, there are reasons to think it might be feasible [275].

In addition, users need effective, intelligible ways of assessing the system's state and its performance. Often our participants wanted to move beyond specific system events. Instead, they wanted to have a more holistic overview of the status of sensors and/or actuators, now or at any time in the past. Textual logs render this kind of information more or less invisible, because only state-changing events are recorded in the log. The system's holistic state at any specific point in time was therefore very difficult to grasp. Yet at the same time, sensors with high measurement fidelity, such as motion detectors, could jam the home log with largely redundant detail, drowning out events from other sensors or devices. Our solution was to batch proximate events and assign the assembled body a status with a start and end point so that a coherent overview of the system could be maintained, which reduced clutter and helped users identify the information relevant for the demand at hand. Nonetheless, we see that clustering and reducing data points for the sake of usability and user experience will have to be used with care so as to not remove information critical to the user.

Practical Guidelines for Conveying the State of the Smart Home

Some of our findings are well-aligned with well-known information visualization principles, such as providing an overview first and detail on demand [455]. However, our study underlines the need for designing such an overview from a user's perspective. What are the important aggregations, and what is this 'detail' to be provided by the system in drill-down cases? Instead of simply providing all raw-data on demand, we identified fine distinctions according to different use cases, where specific granularities of data were required such that too much detail could actually be counter-productive. It is one thing to identify some general principles of visualization in relation to overview versus detail, it is quite another to show what kind of information is needed both generally and according to some specific moment of use. We found in our study that certain kinds of aggregation are more important than others and at different times. In the following we provide some practical guidance regarding how to manage the trade-off between detailed views and aggregations and how to provide data structure in ways that will support system intelligibility:

- **Times, days and repetitive patterns provide structure**: Generally speaking, time is a meaningful cue for supporting people in reasoning about and making use of data [349]. One day as a standard view on data, on the evidence of our participants' stated preferences, was a quasi-natural interval for households seeking to investigate the household log. Furthermore, we observed that many automated actions that participants programmed were also triggered by the time of day, for instance brightness and movement is typically attached to regular diurnal patterns. This has already been discussed to some extent within the literature [127].
- **Routines and activities are guiding anchors:** Even with a general grouping of system logs into days, 24 hours may still hold a substantial amount of very detailed information. A way of aggregating this data in order to support users in sense-making is according to their existing routines. Smart Homes should automatically detect existing daily patterns and activities and inform users about any deviations. Routine activities have familiar organizational properties that people orient to easily and are often referred to in assessments of system behavior already, so this is a structure that can be readily exploited.
- **Groupings and aggregations should replace single events:** As a countermeasure for coping with complexity and the sheer amount of data created in Smart Homes, our households came up with several aggregations of single events that they saw as providing more meaningful guidance in a log. The rules that households created in their systems could be seen to be an aggregate of triggers and events; assuming that a rule worked, and single events subsumed within it could be hidden.
- **Continually provide information about the state of the system:** In a textual log, sensor states are invisible and can only be inferred from switching events generated as a log entry. Contextual information about sensor states, however, was important to households in order to be able to quickly grasp the overall system status, especially for events more than a few hours old. In that case, the system, we suggest, should also provide sensor state for any time in the past.

Appropriation and the Control of One's Life, not Technology

After very active use of the provided interfaces at the start, our households began to get used to the Smart Home system. As time went by, we found that their information demands shifted significantly. The Smart Home system became more of background feature in their homes; it became embedded in their environment. While the rate at which this evolution in needs occurred varied among households, the trend could be identified after a few months of use. As Smart Home use became more routinized, information needs changed. This change can be explained in part by how the technology had been appropriated into the home's infrastructure. The system had moved from being a shiny new gadget to being part

of the home's infrastructure. It was no longer being oriented to as a primarily technical object but as a social object that had become part of the social organization of the home and thus had to be accountable for its actions [62].

Phenomenological research has previously examined how practices have been transformed and established after the introduction of new technology [474]. This line of research originates in the domain of computer supported collaborative work, where Pipek [395] found that detailed information demands are typically only needed in the case of a breakdown in existing practices. In addition to this, Draxler and Stevens [141] have shown that the discovery and pursuit of new possibilities for using a technology also often creates a need for new information. Once the technology *and its use* has been integrated into the daily routine, however, it tends to move to the background, configurations become relatively stable, and information demands tend to decrease [72]. This does not mean they disappear. We found that participants' feedback demands evolved in two ways: 1) The required information was scaled down to the minimum of only wanting to know when something went wrong; and 2) the information participants sought tended to be embedded in daily routines. Here, the use of other devices for providing information such as ambient displays, has already been suggested for Smart Homes [89, 349]. While participants still valued gaining feedback in general, they wanted to be informed without having to explicitly access the system, but also did not want to be inundated with notifications. In this regard, we agree with Davidoff et al. [126] that users ultimately do not seek control over their technology but rather control of their lives. As a consequence, more straightforward factual or rapid feedback was demanded. These are known features of ambient pervasive systems where the point is to demand low cognitive load [222]. While not seeking to persuade as such, inspiration might be drawn from the design of such ambient systems. Having seen the diversity of feedback demands, we argue that what and how much information is provided to the user should be negotiated with or decided by the users themselves. Whatever the precise mechanism chosen, for certain aspects, such as necessary maintenance,

the system should provide a visual alarm on a device, with opportunities for users to dig deeper into the system status on demand.

8.5.3. Designing System Awareness with End-User Development

Given the highly contextual nature of feedback demands, and their evolving nature over relatively long periods of time, we argue that just how much and what information should be made visible should be up to the user. We suggest it is useful to look at EUD mechanisms for keeping users in charge and control of smart and connected systems, while still providing automation. With the complexity of everyday life hindering pattern recognition and machine learning algorithms that might foster automation, the most viable route for research would seem to involve engaging people in the control of devices. While we saw that the system was accepted as part of the home after a few months of use, breakdowns called for manual control and the means to make adaptions on the fly. From our study, we identified two main open research questions for Smart Home and IoT devices in general:

1. We found an abiding concern with the recognition of system error or inadequate functioning. Whereas pattern recognition is understood to be able to identify recurring sensor and trigger sequences [254, 480], ascribing meaning to such events and mapping them to activities is a complex process, which might require incorporating socially contextual information provided by inhabitants, especially in multi-occupant environments [45]. Here, EUD can provide tools to make individual collections of triggers or to assign them to meaningful activities in the home. Alarms on dedicated ambient displays or smartphones would provide a trigger for further interrogation of the system status. In this regard, EUD should also take into account the possibility of extending and tailoring visualizations on different devices, such as mobile and ambient displays [306] to convey errors and system intelligibility.
2. Where networked (not only Smart Home) systems touch upon safety-critical aspects, such as electrical systems, ovens or door-locks, not only practical but also legal questions of responsibility may arise in the case of malfunction. In terms of designing and tailoring system feedback, we therefore also see points of intersection with the law and the design of usable security mechanisms that relevant for EUD [434]. Future work should investigate the relationship between the tailorability of system feedback provided by EUD features and the responsibility of smart device vendors for highlighting malfunctions. With users possibly not caring about or not understanding much of what is said about information security

[79, 468], the design of risk assessment tools for individuals should also be explored, similar to existing programs of research in organizational contexts [429].

8.5.4. Privacy in Multi-User IoT Environments

We found that participants wanted, in principal, to be able to see all of the data collected in the Smart Home; not least for privacy reasons [287]. Therefore, Smart Home systems should not be restricted in their self-information capability, but should be designed in such a way that the information provided will reflect specific demands. As we have seen, data being transferred to a vendor's cloud backend was not considered to be a critical issue by the majority of our participants and none reported a reluctance to use features for security or privacy reasons. As Crabtree et al. [117] have argued before regarding the contextuality of privacy concerns, without bringing up the topic of privacy ourselves, households typically did not talk about privacy implications very much.

Looking down the road for designing privacy in multi-user environments, and especially the home, which is *the* private place in modern western societies, we identified two major themes to address:

First, there may well be a significant difference between privacy concerns as expressed by 'experts', including official agencies, and those expressed by our participants. It would be wrong to simply assume that this gap can be explained by user ignorance. We did see participants conducting some kind of boundary regulation towards the networked data [24, 382], Finding that they struggled to do so, our study points towards the fact that users care about processed information rather than raw data, because they want to make sense of and apply their assessment of the relevance of data to home privacy in a contextual manner. Providing data type (image, text, different kinds of sensors, e.g. movement detection), intervals of disclosure (real time vs. any kind of higher interval) is typically obligatory by law and our households needed this basic information, too. In addition, however, when trying to make sense of data, they were trying to relate data to activities in and around the home, especially taking the perspective of "What can others get to know about me from the data to be disclosed?"

Reasoning about privacy implications, our households commonly tried to manage their "attack surface" [117] by using abstractions from raw data to identify potential conflicts with privacy demands. To put it another way, we need a better understanding of exactly what kinds of privacy demands are being made, in what circumstances, by whom, and why.

While privacy guidelines and law (such as the European General Data Protection Regulation [164]) frequently call for designing data disclosure "transparently" such that data practices are highlighted to users, how to actually design for such transparency in IoT environments is especially challenging for several reasons. IoT environments, such as Smart Home products, are invariably equipped with sensors, which constantly produce data. Moreover, the space of potential use for this data is rather abstract and the implications for privacy are not clear from the disclosure of one data item, but rather from the constant stream of data and its triangulation with other data sources and/or analysis by big data algorithms. Users, as we have argued, are keen to be able to make sense of the potential threat. They are not concerned with privacy as such, but are concerned with their lack of knowledge about the specific ways in which data use by others could feasibly constitute a problem for them. We see that a stronger emphasis on the possible implications of data disclosure could be a promising path to follow and that introducing usable privacy and security management for embedded and networked sensors or IoT devices would constitute a way forward. There is a particular need to rethink privacy in an IoT context because data disclosure often relies on a consumer's informed consent [e.g. 72].

Second, smart sensors in the home do not only provide tools for surveillance for external parties, but also for family members. Although the family is often understood as a circle of trust and private in relation to the outside, within families there are (perhaps especially) certain privacy demands relating to individuals, too. While it could be argued that any family member could have access to the Smart Home backend, during appropriation we found that one household member often acted forcefully as a gatekeeper. Similarly, others [437, 500] have found primary, secondary and tertiary users. This resulted not only in that person being

responsible for setting up and maintaining the system and its rules, which carries implications for familial power distribution, as Ur et al. reported in their study on networked door lock cameras [500], but also in them having the opportunity to "spy" on their families remotely using sensor logs, or switching off and on lights, to play jokes on them. With regard to analysis, while our users did not anticipate potential privacy conflicts or raise them later on, they did want full access to system logs 'just in case'. These findings point to another challenge of Smart Home technology when it is being used by multiple users: What should users be able to see about each other's activities in the home and how can privacy demands be respected by designing adequate mechanisms, such as access control [475, 501].

8.6. Conclusion

As Hurlburt et al. [247] have pointed out, with regard to the Internet of Things at large, "The amount of data will continue to grow exponentially, furthering the belief that we're increasingly swamped with raw data. The underlying question then becomes one of harnessing all of this data into something intelligible" (p57). Our point is that, while it may be operating on a smaller scale, there are obvious lessons in this for the monitoring of data in the home and its immediate environment as well. So, in the home, too, there is an ever-more pressing and significant need to make data intelligible. As our work has shown, the intelligibility of data, in turn, depends on the various and 'occasioned' uses for it over time. Our living lab-based design case study has identified different ways in which people demonstrate their need to be aware and to take heed of system information and, just as importantly, when they do not. Having systems that are capable of some form of self-declaration is clearly an important aspect of making DIY Smart Home systems work. We have shed light on the long-term evolution of information demands for maintaining system awareness and have derived, demonstrated and evaluated some initial design guidelines. When people take heed of system information it is because they have particular needs and these needs change according to circumstance. Supporting this requires rather more than the sum of rules, scenes and events, but does need effective visualizations, not

only of current state, but also of past system states, to enable users to learn about system behavior over time. Moreover, meaningful aggregations for handling the amount of log data need to consider home routines and activities. This will help users understand and orient to aggregations as a feature of their everyday lives and will assist in the reconstruction of contextually useful information. We have also demonstrated how Smart Home system awareness evolves as users gain expertise and reach stable configurations of routine use over time. In particular, we identified a management by exception approach and outlined means to support it, emphasizing the need for embedding feedback in places where it can be encountered as an ordinary part of the daily routine. To sum up, then, our contribution lies in:

1. Recognizing that ever more complex arrays of sensors and other components will create new difficulties and hence new responses from users and that ways of handling this will evolve over time as new technologies are appropriated and embedded into everyday life. In order to understand this evolving use better, long-term approaches to the study of user behavior are necessary. We argue that the Living Lab approach facilitates this.
2. The long-term focus further allows for the recognition that users develop new skills and construct new relevancies in their use of Smart Home data and this has implications for the development of flexible and evolving forms of support.
3. These factors together, in turn, require a sophisticated approach to 'tailoring', one which we argue is best served by a focus on end user development. Such tailoring needs to reflect the different ways in which users, at different stages, will both monitor systems and actively engage in their reconfiguration.

For future work, we seek to take a closer look at the potential of voice assistants to provide ambient system awareness. In this vein, with Smart Home systems increasingly allowing inclusion of third party hard- and software, we will also investigate the role of privacy in Smart Home system awareness. While privacy awareness already featured as a part of the study, the shift towards inclusion of third party elements will make managing privacy in the Smart Home an even more pressing issue in the near future.

9. Providing Smartphone Data Visualizations to Support Privacy Literacy

The privacy settings of smartphones are rarely in compliance with the privacy needs and goals of their users. The gap originates in awareness of privacy as well as in missing privacy literacy. To overcome this gap, research to date has either focused on adjusting device settings implicitly (no user interaction) or on including notifications in the context of specific activities. It has not yet been considered that user data have become more abstract and hence interpretation and decision-making have become more challenging. For example, single GPS data may not reveal habits, but long-term observations might. Here we present a case study by which we show how abstract smartphone data can be prepared and presented to enable users' awareness and privacy literacy to better suit their privacy needs and goals.

9.1. Introduction

Given the popularity of mobile devices, their abilities in combination with online usage data are available anytime and anywhere. This development let to a multitude of new mobile services and applications (apps) for all kinds of use cases. These apps usually offer some benefit for users, but they also ask for wide-ranging or permanent access to personal data in return. Many studies have shown that users generally lack the understanding of the implications of such authorizations. Their mental model of threats to privacy does not match actual threats. The realization of the discrepancy between expected and actual data transmission usually leads to users' resentment [149, 173]. Existing research has focused on mechanisms to show data flow, and have not taken into account the knowledge that is needed to interpret abstract data. It is important to support users and their specific privacy needs and goals while they use apps on their mobile devices. Users need to understand the information, which can be extracted from their data flow. Oftentimes, users have irrational apprehensions while real threats to their privacy remain unnoticed. A shift away from irrational apprehensions towards the

understanding of real threats to privacy and their effective management can lead to more trust and higher acceptance of technology in general [65].

In our case study, we show how smartphone data can be prepared and presented in a way that enables users to improve their understanding of privacy literacy and to better align their privacy needs and goals with the abilities and settings of their devices. In addition, we derive design guidelines for mobile devices, which allow privacy management with improved usability.

Our contribution is to provide a didactic method, which enables users to become aware of real threats to privacy according to their individual privacy goals and to use their privacy literacy to translate these privacy needs into suitable decision-making and concrete preventive measures.

9.2. Designing for Privacy on Smartphones

The control over personal data in times of interconnectivity of data and *ubiquitous computing* [514] has become a challenge. Technical advances allow increasingly implicit collection and usage of data. Additionally, users are not aware of the way the data is used and the implications of granting access to their data [11]. Oftentimes, users are not aware of the options available to protect their data. Users tend to use default settings, as shown with Facebook [12]. Below, with privacy by design and usable privacy, we present two popular approaches to establish privacy in information and communication systems. Furthermore, we introduce the perspective of *privacy literacy*, which is based on the *privacy awareness* discourse.

9.2.1. Privacy by Design

The concept of privacy by design [93] is based on the idea of including considerations of requirements about privacy and security early in the development of new technologies and taking them into account throughout the entire development cycle [499]. Adjustments of a system at a late stage in the development cycle are usually more difficult and time consuming. Hence, problems with privacy should be identified and handled at the beginning of the

development process or as early as possible. One example of such a procedure is shown by Enck et al. [152]: They try to identify information transferred to critical servers and notify users about it [152]. Privacy by design has become a policy for the specification of public IT systems in Germany. It was used in health care projects such as electronic healthcare ids [435] and in Smart Metering [92]. Privacy by default is an approach in which privacy measures are default settings and not opt-out functions.

9.2.2. Usable Privacy for Smartphones

Privacy by design does not necessarily include considerations of usability. Though, it can be expected that privacy increases when usability measures are considered in the process of development, because privacy and security features are perceived to be disruptive and incomprehensible [180]. This perception can result in unfavorable privacy settings and the general attempt to disregard privacy settings with faulty operation or workarounds [180]. One aspect of usability is to incorporate users' knowledge and ability when developing new technical solutions. Nevertheless, the differences in technical knowledge and understanding that users have of complex, yet frequently used, apps, is not always considered for privacy measures and results in reduced protection of user data from the users' perspective [272].

In order to do research on usable privacy the users' requirements have to be elicited according to the context of the users' goals first [416]. Smartphone apps offer many useful features and services. Though, during installation, most apps ask for a variety of access authorizations before usage is even possible. Access to contacts, camera, location and SMS are only a few of authorization requirements during the installation process of an android app which are perceived as disruptive and incomprehensible by users [173]. There are some approaches to solve problems such as these. For example, Brodie et al. [69] developed a privacy management tool based on user-centered interviews and surveys. Lin et al. [326] try to make decision making for privacy settings more comprehensible. Patil et al. [387] describe the effect of feedback and control over disclosure of data with location sharing decisions. Margulis [335] indicates that the desire to protect

against social influences and control has to be ensured by understandable and usable privacy guidelines.

9.3. Privacy-Literacy

Margulis' [335] strategy can be complemented with the facilitation of didactical methods and tools which allow users a better understanding of the consequences of data collection on smartphone apps. Such education enables users to identify hazards and can prevent Misconceptions. Shneiderman and Hochheiser [456] mention these knowledge gaps as the main challenges for designing good usability in privacy measures.

A long-time discussion is the endeavor to enhance awareness about users' own data distribution habits as one possible solution [400]. For example, Balebako et al. [33] have evaluated how direct visual and haptic feedback effects data transmission on mobile apps. In analogy to the understanding of the term energy-literacy [446] in the context of energy data, we do not focus on the transmission of data, but we investigate possible methods and tools to promote privacy-literacy to users in this study.

9.4. Method

In the following section, we describe our research method including the overall procedure, data elicitation methods, and the two workshops which are essential parts of the case study. In a kick-off workshop, we explored the background of participants. This included their technical understanding - in particular about smartphones - as well as their knowledge and awareness about privacy and mobile authorization processes. We asked participants to name sensor types and to explain which ones could be interesting and critical to privacy. Afterwards, we used these criteria to configure a monitoring app which was installed on a smartphone to collect data and monitor data transmission. The participants picked several sensors which were then used to collect specific data on the participant's device. These data were also transmitted to a cloud server at the university.

In the next step the data were analyzed and prepared by the researchers to reveal personal information such as daily habits. Then the prepared data were given to the same participants in a second workshop. In this workshop, the participants analyzed the results and implications of the prepared data and reflected the consequences this should have on authorization and privacy settings on android apps.

9.4.1. Acquisition of Participants

The University of Siegen maintains a platform on which citizens can register to participate in user-centered research with several hundreds of subscribers [375]. These candidates were filtered by search-criteria such as android smartphone, location, interest in field study. The resulting sub-group was invited to participate via email with a description of the project. In addition, all candidates were contacted over the phone within two weeks. The participants explained their interest in the study with their lack of control over the data on their smartphone and their inadequate level of information. The five chosen participants were between 20 and 76 years old and had different levels of technical understanding.

9.4.2. Exploring Smartphone Privacy Demands in Workshop I

The focus of the first workshop was to establish the level of knowledge and understanding participants had regarding privacy. Participants were asked to name fields and services in which private data such as banking, social media, smartphones are relevant. They also had to rate the sensitivity of such data. Finally, this information was used to explore actual privacy settings of the participants.

Based on the pre-interviews via phone, we already had a first impression of how well trained participants were using the smartphone. For a better understanding, during the workshop, we asked all participants individually, to write down all known sensors and resources of data which applications could get access to on their smartphone. In a second step, we collected the sensor types mentioned, made them visible to the group, and completed the list with sensor types not mentioned,

but listed in the google developer pages as permission groups.[5] Participants then were asked to rate sensors individually in terms of perceived relevance for participants' privacy (Table 6). For this, participants were provided with five pro and con markers. Pro markers should reflect that a sensor was understood to

Table 6: Mentionings and Ratings of mobile Phone Sensors and Data Resources by Participants; Sensors Highlighted were later Monitored and fed back to Participants

Name of Resource	Mentioned	Positive	Negative
Wi-Fi Module	3	2	0
GPS Sensor	3	2	2
Installed Apps	2	3	1
Call history	2	1	3
Contacts	2	0	2
Camera/Photos	1	0	3
SMS	1	0	1
Posting in my name	1	1	1
Battery	1	4	0
Date/Time	1	1	0
Usage time (Screen on)	1	3	0
Activity sensing	1	0	3
Duration of Internet Use	1	2	0
OS Version	1	3	0
Calendar	1	0	1
Purchases	1	0	2
Microphone	0	1	3
Identity	0	0	3
Access to wearable data	0	0	2
Bluetooth Connection	0	0	1
Device ID & phone number	0	0	2
Mobile data connection	0	0	1

[5] At that time, Android 6.0 was only just released. See permissions here: https://support.google.com/googleplay/answer/6014972

provide value to the participant. Con markers should be used in case a sensor or resource was perceived to be potentially invading privacy.

9.4.3. Data Collection, Selection and Pre-processing

At the end of the first workshop, we installed a mobile sensing framework described in Ludwig, Dax, Pipek, & Randall [328] on the smartphone of one participant just after the workshop. This collection and monitoring tool allowed us to pick each sensor individually for upload to a university cloud environment.

The decision to install the tool only on one of the participant's mobile phone and not on all devices was based on a variety of considerations. One reason was to foster communication between participants and create a common base of knowledge about the data. If every participant had their own set of data, it would have been counterproductive, because it would have added additional abstraction and reintroduced overwhelming complexity to the procedure. More time and effort would have been necessary to illustrate the different findings in each collected set. Additionally, comparing the different views of the data subject and analyzing participants, we were creating a playful atmosphere where assumptions could be discussed directly. Moreover, the effect of visibility of personal information in a social setting in the subsequent evaluation workshop would most likely have been less revealing to participants. Another reason was to avoid distraction by thoughts about personal details such as to try to remember why a certain location was visited when it was only interesting to see that it was possible to reveal this location in the context of a personal pattern.

Based on the rating and usability of the data in the workshop, we finally agreed on a set of seven resources - no static sensors and not to personal data such as SMS, pictures, and microphone - to be monitored on one participants' smartphone for the next three months. During this time, we collected 126,294 GPS positions resulting in an average of about one position per minute, 33,621 WiFi SSIDs, (one SSID every 15 minute), 55 calls, 24 battery status logs, 24 installed applications, 388 screen-on events, 219,143 activity logs (bicycling, walking, driving, not moving, tilting and unknown; about 1.6 entries every minute).

During the three months of data collection there were no interventions with participants. They could go back to their daily routines. The monitoring tool was used to follow the development of data. In preparation of the second workshop we selected a set of sensors and analyzed data, looking for patterns manually. Doing so, we identified an untypical and typical days in terms of GPS-data (as can be seen in Figure 8), calls, WiFi SSIDs and screen-on events. We selected one of each, to reduce the complexity of data shown to participants to make data manageable.

Finally, we set up a presentation which showed installed applications, call history, screen-on events, battery status, WiFi SSIDs, activity sensing and GPS positions. For the analysis of a single day we used GPS, activity-logs, call-logs und WiFi-data. By transforming the data into Pivot-tables it was possible to filter for most important entries. The call-log shows caller's name, number, length, date, and type (outgoing, incoming, missed). The WiFi-table shows the SSID of the WiFi network and the number of scans, sorted by count. The activity-table shows the the values of the activity (bike, on foot, vehicle, resting, tilting, and unknown) per hour and visually in an additional graph.

In the data analysis and preparation step for typical daily activities of the participant, data of the entire sampling interval were used, complemented by a list of used sensors, with an overview over all installed apps, as well as a diagram for screen-on and battery sensors. The table with WiFi-data was filtered to get an overview over most scanned SSIDs sorted by the number of days. SSIDs with a standard label and no personal name were removed from the list. The location-data were filtered for another three days on which locations were revisited. From these data, new maps were created.

9.4.4. Breaching Experiments in Workshop II

For the second workshop, we introduced the analysis of smartphone data as a game. We asked participants to try to deduce as much information as possible from the data we provided and explain their reasoning to the group. Only

afterwards, the analysis subject was supposed to respond and clarify on interpretations and conclusions made by participants.

Generally, the workshop was divided into two main sections. The first section was about a day in the life of the analysis subject, the researchers had identified as non-typical during the pre-procession. In a second phase, a day selected as rather typical in terms of data was shown for analysis. For both sections, we did not provide all data at once, but introduced sensor data charts after another and only provided the full picture in the end. We did so, to stimulate analysis of each sensor individually.

In the first part, we presented the phone call history and then the activity analysis. Subsequently, we showed the screen-on events of one day, WiFi SSIDs and finally the map-embedded GPS data was presented. As a last step, all data sheets were shown together, to foster combination of data sources.

In the second part of the workshop, we also included rather static information of installed applications. Additionally, the total call history, battery status, and screen-on events were aggregated to provide information about the whole past three months. For ease of use, we chose a typical day in terms of WiFi SSIDs and GPS data, to limit the amount of data to analyse within the two-hour workshop. The method was based on the breaching experiment which has the goal to invoke thinking and action in the face of new information and circumstances from the participants [111]. In this method participants get historical smartphone data which include private, sensitive information from another participant of the same workshop. These information is rated by the participants and supplemented with personal experiences. Participants are supposed to think about what consequences these data and the gained knowledge will have on their interaction with an app or their phone. Similarly to Kang et al. [272] we visualize collected smartphone data and use the Think-Aloud protocol [156] to explore the understanding of privacy settings of apps and privacy goals from users' perspective.

9.5. Findings

In the following, we provide an overview of our findings throughout the two workshops. First, we analyze the participants' general assessment of privacy and security risks on the Internet in general, on the smartphone and regarding its specific sensors or resources in particular. Second, we are reporting rich descriptions of how participants interpreted smartphone data of somebody they did not know.

9.5.1. Explorative Workshop

In this section, we describe the findings related to our explorative workshop.

Privacy and Security on the Internet

During the kickoff discussion, participants mentioned a number of services of everyday life, which were understood to process personal data and thus potentially interfere with their privacy. Topics mentioned included E-Mail, online banking, cloud services, personalized advertisements, search engines, social networks, insurance, Connected Cars and smartphones. Regarding strategies of tackling privacy invasion by such services, participants highlighted two different strategies.

First, participants mentioned the challenge of securing their data from unauthorized access. For example, phishing mails or usage of online banking were seen critically. In this regard, P4 states:

> *"Every now and then I am worried that something [data] could be simply taken. "(P4)*

In addition, the security of data processed by insurances or service providers was seen critically. Especially, however, the potential to protect one's own data by measures of IT security were understood to be ineffective, as P3 put it:

> *„If even the government can be hacked, how should I as a plain citizen be able to protect myself? "(P2)*

As a second challenge for managing privacy online, participants also reported on privacy practices. For example, during the workshop one participant logged onto his Google-account and found that data and search queries as old as three years were still stored and available. In this vein, two participants mentioned using a search engine that does not store such information.

Similarly, participants mentioned to avoid cloud services and to use email encryption. Here, however, some participants did not find this necessary.

> *„I usually have nothing so important that I need to encrypt it." (P1)*

Such privacy practices also included use of the smartphone. Especially, the smartphone was less trusted than a PC or laptop. Three participants reported to not use online banking on their smartphone due to perceived security and privacy issues. Such issues were also reflected in a lack of knowledge how a smartphone worked, or especially what some applications did – probably without knowledge of the user. Especially, when pre-installed, smartphone applications were perceived as privacy and security risks.

> *„Well, partially I don't know at all what they are doing. Because sometimes you ask yourself: Why would this app need this authorization? "(P1)*

A similar transparency problem existed in the context of rights management when installing applications. P3, for example, could not understand why a camera-application would need access to her phonebook. When connections from applications to sensors or resources were not well understood, this fostered mistrust. As a way of dealing with such a trust deficit, P2 reported to rely on the online reviews in the store and only installed the best-rated and/or most downloaded applications. Still, participants agreed that when they wanted an application they always granted all rights it called for, even though they were aware that by doing so, personal data was disclosed.

In general, the usability and measures for controlling and especially understanding data disclosure were criticized:

„I feel really badly informed. Now under Android 6 you can still manage single permissions [of an Application] without root access. But nowhere else is mention of what is collected at all. "(P2)

P1 also explicitly called for tools to get to know his data and its disclosure better:

"[...] Because I want to know the background. Because I want to know exactly, what data is taken when I disclose WiFi-information or my calendar or contacts." (P1)

Knowledge about and Sensitivity of Data Resources

Collecting sensors and resource, we found that the overall knowledge of sensing capability was limited among participants. Table 6 shows how many participants could name each sensor or resource. None of these items was mentioned by all participants, with WiFi and GPS being the most commonly known sensors (three out of five participants mentioned them). Only five more were mentioned twice. The resources which received no mentioning at all were added by the researchers, for enabling consideration of unknown sensors for subsequent evaluation, too. Marking sensors with positive and negative connotation regarding perceived potential benefits and threats to privacy, partly showed conflicting outcomes. For example, whereas GPS received two pro and con markers each, the WiFi module was uncritical. Participants were aware that a GPS-sensor would be able to locate users, which was understood ambivalent:

P1: "With some things you really have to think about them. On the one hand, positive, on the other hand negative. For example, GPS analysis. On the one hand, it is good that you can find your position down to few meters. On the other hand, of course, this is problematic." (P1)

"Well, here, monitoring the calendar is similar [to GPS]. From one app, I might even need it to do this, others however, should not ask for this permission at all." (P4)

The items valued most privacy sensitive, however, were barely mentioned, apart from the „contact" permission. Discussing items, it became clear that participants

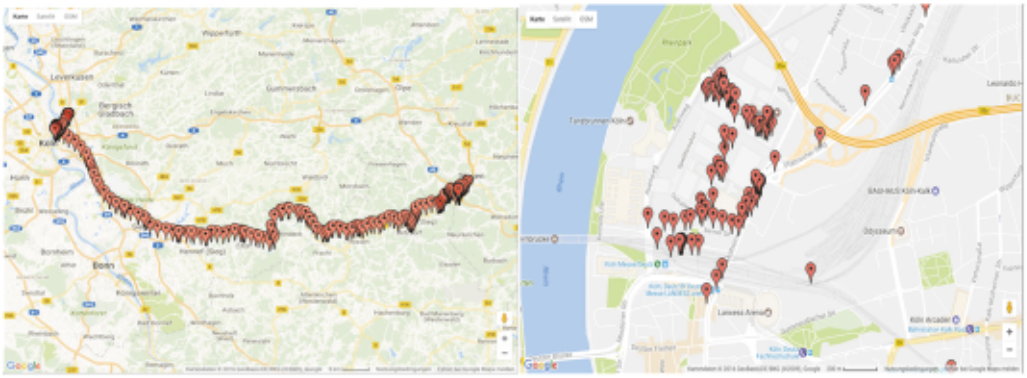


Figure 8: Left: Overview view of GPS data of the "non-typical" day. Right: Detailed city-view of GPS data of the "non-typical" day

thought to be able to relate to the items in question. It was rather clear what the permission to collect the contacts or access to the microphone would mean. In contrast, access to the "Identity" was perceived as potentially harmful, although no participant could outline, what this permission would disclose.

Similarly, although „activity sensing" was unknown to all but one participant, it was perceived to be very relevant to participants' privacy management on their smartphone. On the other hand, "battery" and "Usage time" rated as items an app should be allowed to have access to, largely to provide statistics and warning of low battery.

9.5.2. Evaluative Workshop

In our second workshop, we let participants analyze a set of data we had collected and pre-processed. We first introduced each of the seven sensors individually and finally provided an overview of all of them. In this chapter, we are describing how participants proceeded in analyzing provided smartphone data. Participants could find out both some basic and demographic data, peers, and routines.

Demographics and Peers

Regarding general usage, participants argued that the person in question would not use the smartphone very often, as there were only 338 screen-on events. Still, the GPS data showed that the user carried it with her pretty much all the time. As a relatively static information, the installed applications underlined these assumptions. Further analyzing the list participants were also able to guess the

smartphone manufacturer, as there were several proprietary and manufacturer-specific applications installed. Moreover, the participant in question used an application for comparing gas prices, making it likely for the data subject to have a driver license, and to probably own a car himself. The data subject admitted owning a car, for him, the list made him think which applications he could uninstall. He also criticized that pre-installed applications were useless to him and should be removable.

The call log was the first source, which disclosed information on the persons' place of residence, as a landline number in the log was titled "home". Moreover, next to allowing access to names of peers, several names featured relationship information, such as "brother" or "uncle". Participants here worried that one-selves' privacy to a certain extent was depending on somebody else's behavior:

> *„Once a number is stored in the phone book, this person is virtually a public person, whether she wants or not. This other person has no influence whatsoever on whether or not she becomes known. And I think that's a bit critical, because you cannot estimate who wants what." (P4)*

Most astonished were participants by the information which WiFi SSIDs revealed. For example, only by looking at accumulations of SSIDs, participants identified the likely neighborhood of the data subject by referring to a SSID named after a craftsmanship:

> *"Well, heating engineer [anonymized]. I would simply look up its location. And given the amount [of this SSID having been recorded], I would say this is a neighbor. Yes, and then I would roughly know where he lives." (P4)*

Activities, Interests and Routines

Analyzing also made participants guess activities, interests and routines. For example, the screen-on event graph showed that the smartphone was only used between 7.00 am and 10 pm (Figure 9) with most events distributed between 11 am and 6 pm. Participants also directly started reflecting their own behaviors:

"So, seeing this I guess I would have a lot higher bars everywhere. [laughing]" (P3)

In the eyes of participants, the battery status information conflicted with former assumptions about the participants' behavior. The graph suggested that the smartphone was likely to be loaded at night, as a high number of 100%-values could be found between 8 am and 11 am. The data subject, however, contradicted the assumptions and stated that there was no pattern of loading the smartphone at night. Quite the contrary: For security reasons, he did not do overnight-loading. Here, data quality or random accumulation misguided some interpretations.

WiFi information also allowed tracking daily activities. For example, several SSIDs pinpointed towards a local electronics market. More specifically even, participants suspected that the participant had spent time in the apple department of the market. Later, the GPS data provided reinforced this interpretation.

When examining the GPS data participants could recognize certain daily patterns. Due to a repeated footpath, they for example correctly assumed that the data subject might own a dog. The visit of an indoor swimming pool on a Monday, the visit of the metro market, and trips to the inner city were recurring events and offered reason for speculation regarding habits.

Although the general possibility of a GPS sensor to store a location of a smartphone was known to all participants, the information which comes from it was very surprising to participants. Participants were surprised by the detailed

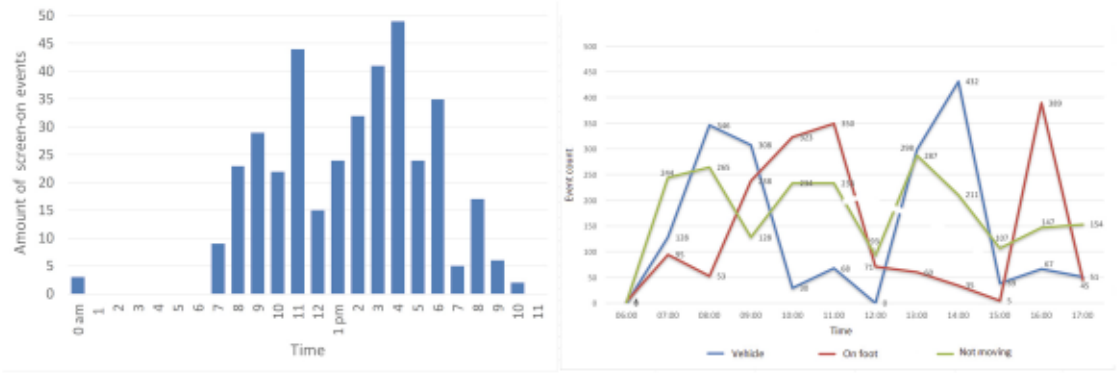


Figure 9: Left: Activities based on activity recognition sensing of a non-typical day. Right: Screen-on events over a typical day

presentation of the individual days. From being able to assess the GPS sensor, they had only expected to be able to use a snapshot of the current position in use, but not a permanent storage of the individual waypoints.

The data subject finally confirmed the participants' suspicions and added that he was troubled by the accuracy of both GPS and WiFi:

> *„They [WiFi and GPS] both are problematic to my eyes. They [the analyzing participants] were able to exactly determine, what I was doing [using GPS data]. In which department, I was. [...] I see the exact same thing here with the WiFi networks." (P1)*

Finally, not only did participants find out a lot about the data subjects' life, the subject himself also reported having gained from the workshop: Specifically, he planned to not leave WiFi and GPS turned on permanently, as he did before. Also, he planned to remove some applications he only got aware of because of the list we provided.

9.6. Discussion

In our first workshop, participants were frustrated with not understanding why certain applications needed specific rights on their smartphone. Additionally, they were only able to come up with a small subset of data resources which their smartphone may provide to apps. Moreover, several of these resources were valued as rather insensitive. Discussing the underlying reasons showed that participants simply were unable to understand the potential information within data. We therefore decided to provide visualizations of data collected by a subset of sensors and resources to check whether the graphical feedback of data from a longer timespan would foster reflections on privacy decision making. Doing so, we identified three benefits of feeding back data collected by smartphones to users for (collaborative) analysis.

9.6.1. Fostering Privacy Literacy with Anonymous Data

One could argue that user reflection was limited by providing data that did not stem from the users themselves. On the one hand, it is true that data from a largely

unknown person might have hindered reflection of personal privacy practices. While call-logs seemed to provide a direct connection the person's peer network, we observed how participants rather guessed and were unsure about interpretations when handling more abstract data such as WiFi SSIDs, Activity recognition or GPS.

Still, they could contextualize data to a certain extend and deduce both demographic, such as place of residence, or likely profession, and personal interests, hobbies, and routines. Additionally, by using quasi-anonymous data we could remove contextual and implicit knowledge from the equation. Arguably, such an 'outsiders' perspective' is closer to the perspective of third parties analyzing data. Moreover, analyzing somebody else's data fostered a playful, engaging, and interactive workshop experience. The collaborative setting helped participants to learn from one another. They discussed lively and collaborated in the task of deducing information from data provided. More than once, participants were motivated by each other by bringing in individual perspectives on data and triggered new reflection processes. Both analysts and the data subject later on reflected on having learned new aspects of smartphone privacy and stated that in the future they would like to change their rights management practices, reduce the time using WiFi and GPS and more carefully watch the list of installed applications.

9.6.2. It is not the Data, it is the Information Within

Already during the first workshop, it became obvious that permissions, sensors and resources were not well understood by participants. This is in line with findings from research on usable privacy notices [33, 437]. The perceived threat of disclosing the "Identity" is a good example of a mismatch between undesired implications of data disclosure (namely: being identifiable), and a lack of understanding regarding information inherent to sensors and data resources, as the Identity permission only includes the phone number and the IMEI.

Moreover, data disclosure was reflected in terms of perceived information, third parties could gain from data. A lack of understanding these implications resulted in an inaccurate classification of data in question.

Especially WiFi information was not understood to carry privacy implications when being shared with third parties. Visualizing data made it tangible and supported users in applying their privacy reasoning to formerly invisible and abstract data, that was unknown with regards to the information it could disclose to third parties.

9.6.3. The Quantity Makes the Information

Whereas smartphone rights management highlights the importance of designing privacy notices usable, we argue that support needs to start earlier. Our study showed that participants could either not even mention most of the sensors existing in a modern smartphone, or were unable to assess their impact on privacy. This is backed by a study of Felt et al. [173], stating that only 3% were able to explain app permissions correctly. Other studies also show that users lack transparency, which leads to uncertainty [33, 326].

The gap between seeking to preserve certain information from being disclosed and the perceived threats to privacy is most obvious in the WiFi module. By only harvesting SSID names, participants were able to gain a basic understanding of where the person in question lived, and where she went on a day of travel. Besides the simple naming information, research has more sophisticated methods of using WiFi fingerprinting for location analysis [88, 357, 533].

Similarly, the collection of GPS-Data at one point in time may be unobtrusive. However, when frequently or constantly allowing access to location services, not only demographic data, but also habits and routines may be deduced.

For enabling effective privacy management, not only usable privacy notices should be researched as in [33, 46, 437]. Additionally, users should be supported in gaining an understanding of the long-term impacts of data collection on their privacy.

9.6.4. Limitations

Our study faces several limitations, which we discuss in the following. First, our study had a small sample size of five participants. Due to conducting an explorative study, we wanted to gain a basic understanding whether our concept could work in terms of raising awareness and fostering an understanding of what data collection on smartphones could mean to users' privacy in the longer terms. We explicitly do not provide design implications on UI-level, but remain on a conceptual level, as more research is needed to clarify on how to visualize smartphone data best, to enable reflection that is more accurate.

Second, our workshop featured a mockup visualization which was not interactive and only provided a very limited possibility to navigate along days and dive deeper into data. However, for breaching into smartphone data analysis in a two-hour workshop, we believe that it was necessary to make data manageable for non-experts. Especially, we believe that any interactive software should also provide some pre-processing to clean up data i.e. remove default WiFi SSID names, which hold no location-related information.

9.6.5. Future Work: Permanently Feeding Back Smartphone Data

Providing visual feedback of smartphone data has motivated participants to debate lively. It led to a critical reflection of sensor data and supported comparison with daily routines and properties of ones' own life, such as the place of residence. For taking our research further, we see mainly two ways of proceeding from here:

First, an interactive and unlimited access to smartphone data in terms of time and sensors might greatly diversify and enrich our findings. We are already building a visualization framework for this purpose and plan to feed back smartphone data continuously to users in order to further develop the dashboard tool in a user-centered way. This way, the didactic concept of a group of outsiders analyzing a person's smartphone data traces could be further shaped and developed.

Second, while the concept has proven successful with the playful characteristic of using 'spies' and a data subject, our findings also show that such a dashboard

could also target awareness and improved understanding regarding personal smartphone data disclosure. Therefore, we are also planning to provide mentioned dashboard to smartphone users for self-reflection and are curious in how far demands might differ.

9.7. Conclusion

While usability of privacy management on smartphones has gained a lot of attention in the past years, in this paper we show how user lack awareness regarding the existence and meaning of permissions, sensors and resources. We further presented a didactic method for co-analyzing smartphone data without contextual knowledge about data. Doing so, we provided mockup interfaces for fostering the understanding of what data means to users' privacy. In this regard, we suggest enabling users to permanently analyze their own data produced by their smartphone to bring aims and actions in terms of privacy management better in line. Our study shows, how 'privacy literacy', meaning an accurate understanding of what disclosure means in terms of leaked information, plays a major role in this regard. We argue that researchers on smartphone privacy could benefit from our experiences by raising awareness on implications of disclosure of larger amounts and streams of data to put data into the context of big data analysis potentials.

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

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.

10.1. 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 [514]. Tapping into these potential benefits through ubiquitous sensors in domestic environments will, however, make 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 [371] 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 [70]:

- **Embeddedness**: Embedded sensors automatically collect (potentially) large amounts of personal data, in a manner largely hidden from users,
- **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
- **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 [4]. 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 [407, 412]. Moreover, data is becoming an economic asset which suppliers trade and consumers need to be able to control properly [192]. Therefore, designing privacy mechanisms for embedded applications has become an important research topic [29, 347, 356, 421].

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 [311]. 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 [509], European General Data Protection Regulation [164], 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 [536]. These developments question the fundamental idea of „doing privacy" as a voluntary, individual decision about (non-)disclosure [13]. 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 [319] 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 [280].

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:

4. exploring and analyzing how people make sense of Smart Metering data,
5. elaborating and enriching our understanding of how individuals perceive the possible benefits and risks of Smart Metering, and
6. 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 [117, 382]. We do so by stressing the importance of a *practice based* approach [410, 528] 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.

10.2. 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.

10.2.1. 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 [380]. 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 [536]. 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 [104].

Although Smart Metering data is considered private, the guidelines for Smart Meter deployment rarely discuss usable means for end user control [473]. 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 [121]. 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 [292, 384].

Overall, various interest groups have outlined a number of benefits as well as risks [211, 346] 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.

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 [369, 422]. In

particular, Smart Meters are considered a prerequisite for building a renewable electricity infrastructure [28]. 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 [102]. Consumers as well as companies may reap the benefits via lower prices and a more resilient electrical grid [197].

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 [448] and discover potential savings [188]. The power consumption profiles generated from Smart Metering data are being applied to develop tariff recommender systems as an additional potential benefit [179]. Further, Smart Metering data could be a source for enhancing the content and delivery of power consumption advice [178]. Yet, the extent to which such savings are realized in practice is being debated [303].

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 [211, 303, 346]. In particular, the Smart Grid constitutes a critical infrastructure that must be protected against cyberattacks by hackers, criminals, terrorists, or foreign states [168, 181]. As a result of digitization, cyberattacks are more common and damaging [345]. For the individual, the data collected by a Smart Meter poses the risk of others deducing life choices and domestic routines [76, 230]. Technology acceptance is also an important factor as consumers may not trust utility providers [219, 419].

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 [298, 529]. At the same time, studies show that consumers lack proper understanding of who can access their data [272, 419]. Krishnamurti et al. [303] 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 [493]. However, Krishnamurti et al. [303] 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.

10.2.2. 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 [491]. 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 [463]. For instance, when photography entered the mainstream, privacy was proclaimed as the „right to be left alone“ [510]; with advances in surveillance devices, privacy was described as the claim for self-determination of the communication of information about oneself [517] with the advent of information technology, privacy was characterized based on control over the flows of personal data [182, 358]; with the growth of the Internet and online interactions, privacy was framed in terms of ‘contextual integrity’ [370]. 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 [29, 347, 356, 512].

Traditionally, understandings of privacy can be thought of as entailing a normativity or being bound up in issues like trust (see [228] 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 [24], 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 [382] 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. [117] 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., [145, 183]), data mining (see e.g., [321]), and mobile services (see e.g., [231]).

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 [64]. From an economics viewpoint, privacy related choices can be characterized as a function of decisions made by a rational actor [10, 134]. 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 [64]. This individual balancing is also referred to as the mental privacy calculus [134] 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 [10, 64]. From this perspective, the mismatch between stated privacy attitudes and actual behavior presents a paradox [371] as people seem to make irrational decisions. The concept of 'bounded rationality' [202, 459] provides a partial explanation for the paradox, explaining it as a result of the opaqueness of privacy implications [30], context-dependency of decisions [227], and a lack of

sufficient awareness and knowledge regarding matters relevant to privacy decision-making [400]. 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 [309]. Therefore, *perceived* pros and cons are as important as the actual consequences of a decision [493].

In addition, scholars like Solove [463] and Reckwitz [410] have pointed out that human behavior in general, and privacy regulation in particular, must be understood from the background of historically contingent social practices, where privacy decisions are embedded in collective cognitive and symbolic structures that enable a socially shared way of ascribing meaning to the world.

As Reckwitz [410] 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 [463]. 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.

10.2.3. 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 U.S. Privacy Act of 1974 that introduced Fair Information Processing Practices (FIPPS) [504], the EU Directive 95/46/EC [165], and European General Data Protection Regulation (GDPR) [164]} regulate the handling of personal information. Additional regulation and standards, such as the Common Criteria [104], 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 [473]. 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 [162], 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) [123]. 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 [309] and even Smart Metering [92]. 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" [90]. Such an approach includes efforts to put users in possession and control of their data [221, 344].

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 [198, 473, 519]. 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 [428, 444]. 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 [92, 473].

10.2.4. 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 [311] 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 [316], e.g., taking into account mental models of the system operation [326] and providing mechanisms for managing access to personal data [248].

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 [400]. Additionally, there are several general guidelines mentioned in the literature, such as including understandable privacy

notices [437] or providing feedback and control regarding data disclosures [44]. 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 [311]. 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 [33, 290, 322, 400]. Other similar commonly used strategies for making implications visible include using heuristic threat models that aim to assess risks [243] or providing justifications for requesting personal data [293]. With data becoming more and more abstract, making data collection, processing, and usage understandable to the user remains a challenge [454, 495]. As Cranor [119] 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."

Given the importance of existing expertise and routines for handling privacy (e.g.,[407]), research based on the notion of practice [410] tends to follow exploratory approaches, making it an essential first priority to try to understand how individuals and households appropriate and make sense of systems and data for everyday life.

From a practice-theoretical perspective [410], 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. [213, 214], for instance, uncovered practical challenges in making home networks work. Focusing on support for power consumption advice, Fischer et al. [178] found that referring to household routines and practices made data more meaningful. Tolmie et al. [495] 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.

10.2.5. 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 [206]. 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 [433], data anonymization [325], random noise integration [507], and obfuscation via local buffers [271]. The second approach provides anonymity via aggregation [427] implemented in one of two ways [158]:

- **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
- **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 [148] 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) [206]. 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 [383]. 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. [137], 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:

- 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?
- 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?

10.3.Method

Our methods were informed by the design case study methodology [528], a multi-staged, action-research approach [232] that combines methods from ethnographically-oriented research on user behavior and the corresponding rationales underlying the behavior [405] 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 [111, 194]. 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 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. [405] 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 [331]. The point here is that an understanding of practice does not require a specific method but a commitment to the idea of members' rationales [227], especially if we are to take seriously the individual perspective we spoke of above (see Section 10.2.3). 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.

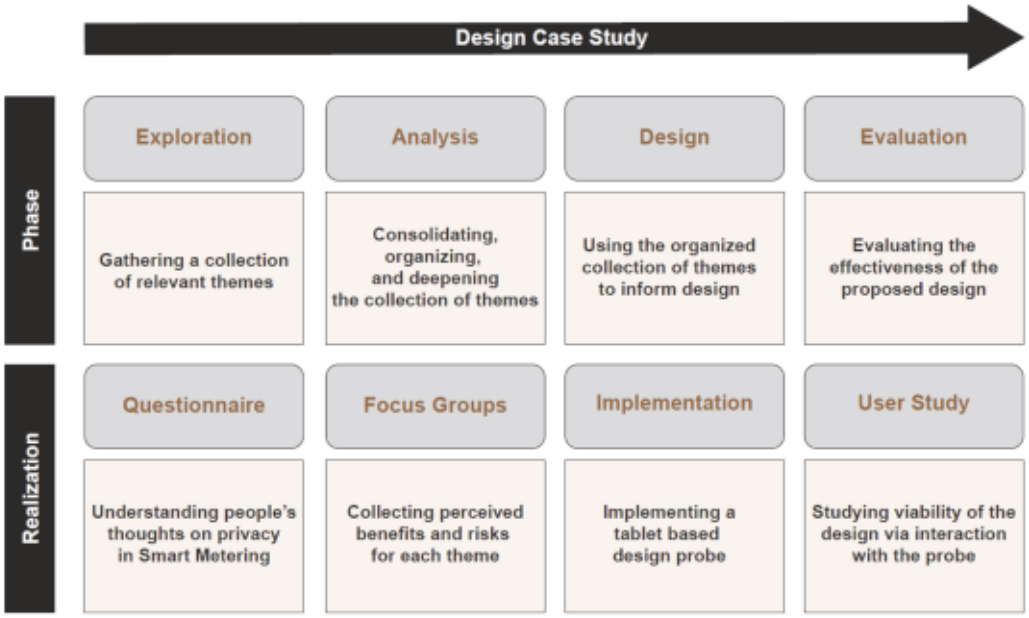


Figure 10: An overview of our multi-stage research approach

Figure 10 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 [98, 208]. 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 [58] 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.

10.3.1. 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 [159]. 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 [241, 270, 484]. 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.

10.3.2. 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 [440] 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 the Appendix 13.1) 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 [66] which emphasizes paying attention to how people express their expectations, concerns, and needs. Thematic coding is situated within the broad tradition of grounded theory [204] 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[6], 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.

10.3.3. 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

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

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 showed an introductory video on Smart Metering produced by an independent foundation (see Figure 11). 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.

Figure 11: Screenshot from the introductory video on Smart Metering and the Smart Grid (https://www.youtube.com/watch?v=iyvAwd4p6ds).

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 [66]. 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.

10.3.4. 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.

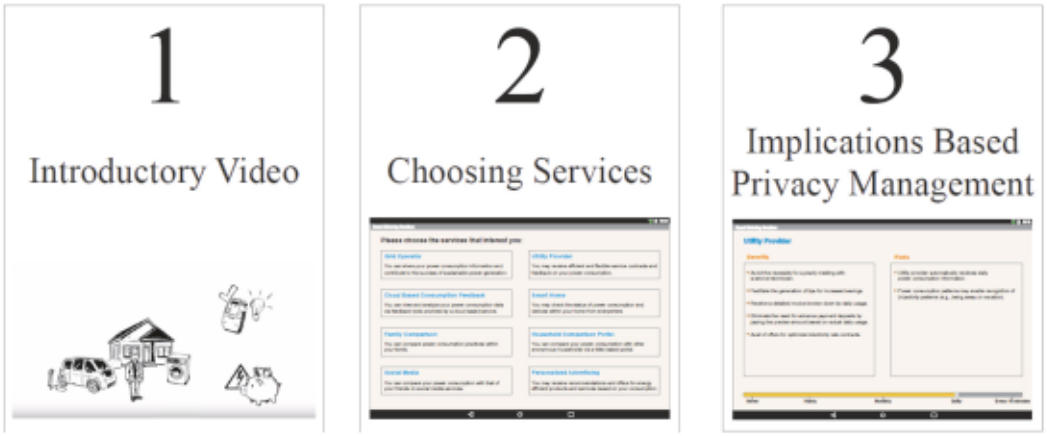
To design the app, we coupled our knowledge of user-centered privacy mechanisms with guidance from relevant literature. The app was designed to provide information on the benefits and risks of data disclosure [134] for possible Smart Metering services. As mentioned earlier, two techniques are commonly 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 [158, 427], representing an enhancement to the concepts proposed by Efthymiou and Kalogridis [148], 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 12):

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 12).



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

(b) Presenting value-added Smart Metering services.

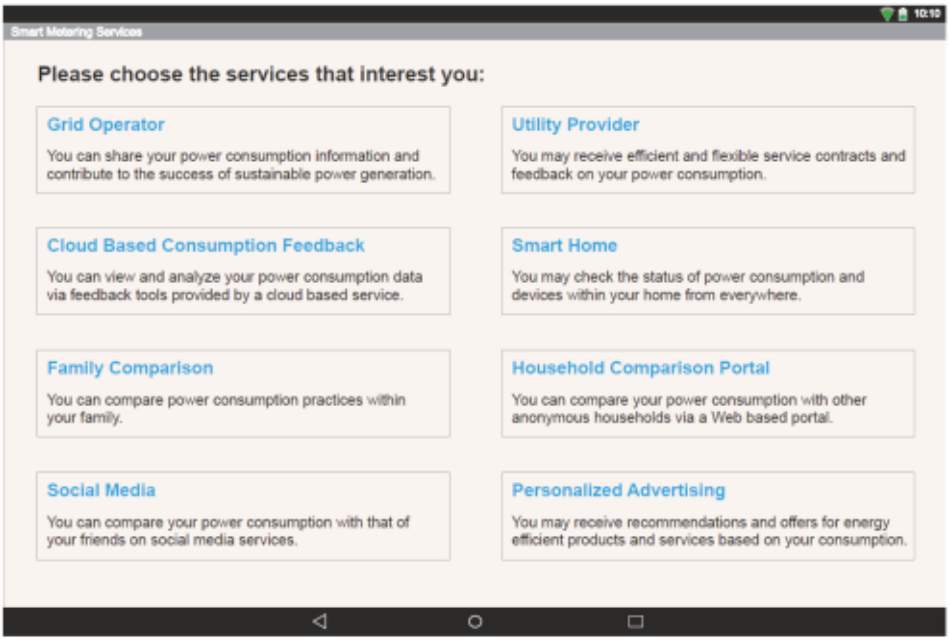
(c) Adjusting data disclosure based on the corresponding privacy implications.

Figure 12: Interaction flow of the design probe

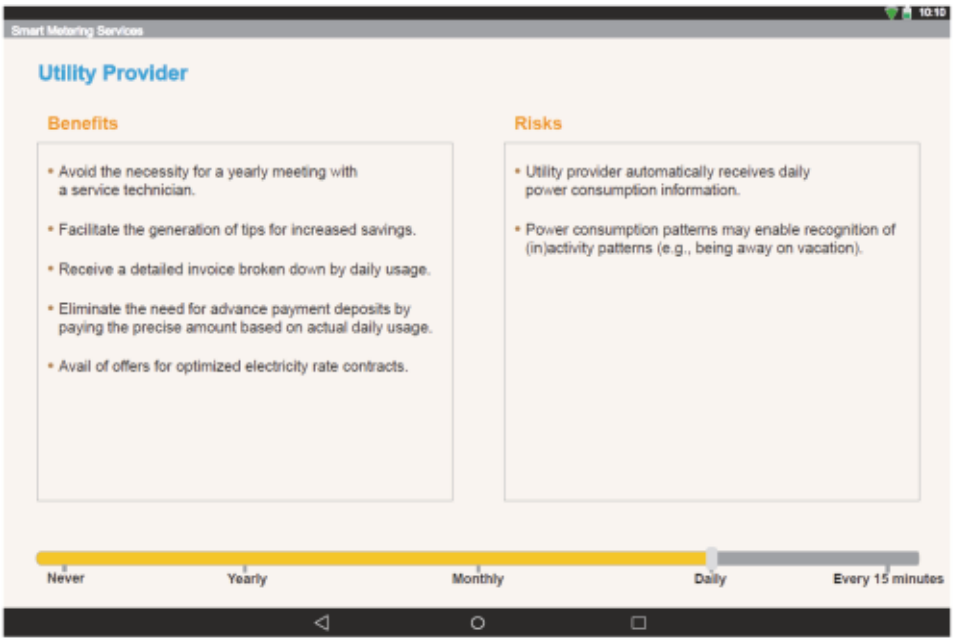
First, we provided a general introduction to the topic of Smart Metering and the Smart Grid. Second, the user was asked to choose desired Smart Metering services (see 12a). Third, the user was shown a list of benefits and risks corresponding to the respective services. The list was compiled from the questionnaire and focus group findings (see 12b). 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 revoke the initial data transfer choices. Changing the granularity of data disclosure updated the benefits and risks shown.

The screen allowed specifying the desired privacy setting for each of the previously selected services.



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



(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.

Figure 13: Screenshots of the tablet based app for Smart Metering privacy management.

10.3.5. 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 11) was shown (see Figure 12). 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 12). 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 12), 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.

10.3.6. 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.

10.4. 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.

10.4.1. 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.

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 / CO2 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)*

Safety and Security

The first section of the questionnaire focused gain an understanding of what is important to consumers in the context of the electricity supply. Primarily, respondents expected low costs. In this regard, participants further mentioned trustworthiness and correctness in billing. A few respondents mentioned that appropriate handling of private data was important.

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)*

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. Improving the provision of information regarding possible benefits and risks was often cited as a factor important for acceptability and utility of Smart Meters.

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)

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)*

Table 7: Implicit and explicit references to the implications of data transfer

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

„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 7: Implicit and explicit references to the implications of data transfer

). 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 [211], 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.

10.4.2. 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 8). We organized these scenarios under several higher level themes.

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.

Table 8: Perceived benefits and risks with number of corresponding mentions in the questionnaire and focus group responses, respectively

Perceived Benefits	Perceived Risks
Energy Literacy & Feedback • Consumption data could be available online anytime, anywhere (31/4) • Consumption data could be compared and shared with family and friends (10/4) • Consumption data could be collected anonymously for comparison with similar households / appliances (13/4) **Savings** • Tariffs could be made flexible (3/1) • Tariffs could be optimized for each individual household (2/2) **Flexibility** • Tariff changes could be simplified (1/1) • Meters could be read remotely (without an in-person appointment) (0/1) • When moving, account changes can be processed faster (0/1) **Sustainability** • People could be incentivized to engage in environmentally friendly habits (6/2) **Independence** • People could manage data access by others (2/3) **Advertisement/Information** • Advertisement could be optimized through personalization (e.g., showing ads for a more efficient fridge based on meter readings) (6/2) **Safety/Security** • People could receive a warning message in case an appliance (e.g., stove) is not turned off (12/2) • People (especially the elderly) could receive a call/text message when no consumption is measured or consumption differs from daily routines (5/1) • People could check on appliances from remote locations (4/1) **Technically infeasible** • People could switch on/off home appliances remotely, e.g. via mobile application (3/0) • People could separate the consumption in apartments that share a Smart Meter (1/0)	**Actions of utility companies** • The energy supplier could engage in privacy discrimination (1/3) • Utilities could get sensitive information (20/2) • Utilities could switch off energy (3/1) **Privacy and daily routines** • One may become a 'transparent citizen' and have privacy violated (31/4) • Home presence could be deduced from data (8/2) • Third parties could derive behavior patterns and create profiles (11/3) • Employers could engage in employee surveillance (e.g., coffee maker/computer usage) (1/0) • Others could know of one's purchases (1/0) **Advertising** • Advertisers could personalize ads (21/4) • Salespersons could know when someone is home (1/0) **Hacking** • Energy supply could be interrupted (7/2) • Consumption data could be modified (11/2) • Private information could be collected (4/0) **Technically infeasible** • Manufacturers could analyze the use of specific products (1/1) • TV license center could check for the existence of specific home appliances (1/0) • Movie industry could target pirates based on identifying watched movies (1/0) • Neighbors in apartment buildings could control each other's energy consumption (1/0) **More general concerns** • Smart Metering systems might be hard to handle (8/0) • People may waste energy when it is cheaper (0/1) • Consumption sharing may create moral exposure by the need to justify choices (7/1)

„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. In situations where electricity was cheap due to lower tariffs, it was mentioned that it could be wasted on unnecessary activities. Such an inversion was imagined to be consequential in terms of power consumption. Participants feared being discriminated against for not being as flexible as others in using tariffs or power at the right times.

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.

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 "Potential Exposure of Everyday Practices").

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."*

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."*

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."

However, participants were willing to take a high degree of responsibility, indicating that they implicitly assumed that they would be offered the ability to control data disclosure according to their preferences.

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.

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]."

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.

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.

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.

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 8). 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.

10.4.3. 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 10.3.4.

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 Table 8). 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 (seeFigure 14). 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.

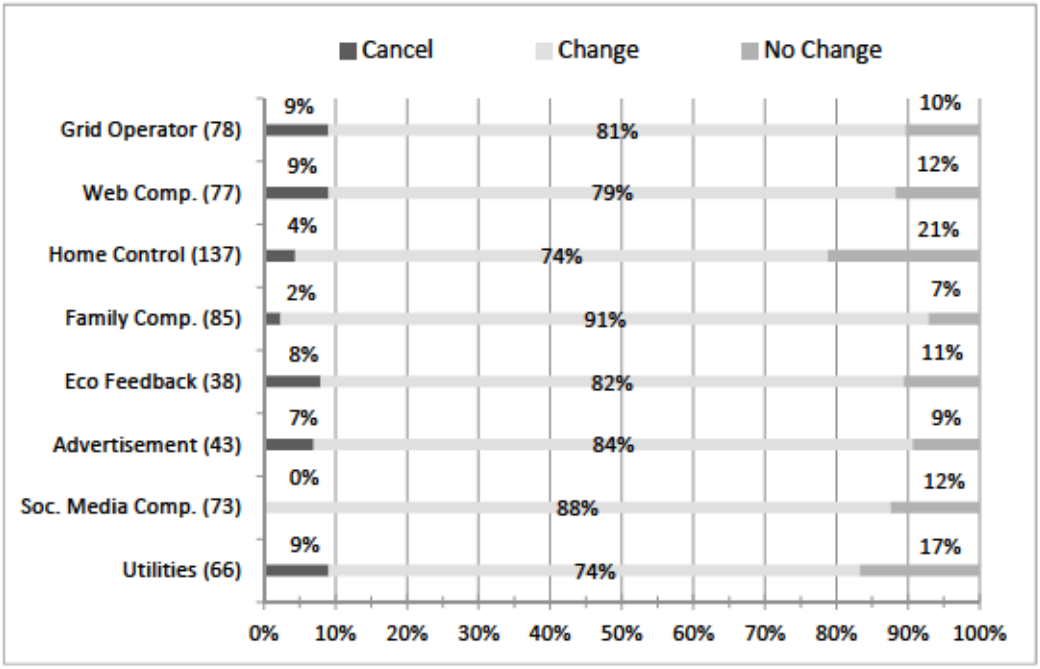


Figure 14: Service subscription decisions of the participants after encountering the corresponding privacy implications

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 10.3.4).

Figure 14 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 14 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)*

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.

10.5. 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. These practices of making privacy implications accountable suggest supplementing the typically data-centered perspectives on privacy with a perspective focused on users' perceptions of the information they share.
- Third, we provide a set of methods and a starting point for intertwining regulatory, technological, and individual perspectives on privacy.

10.5.1. Make Data Accountable via Connection to Practices

Legislation, such as the GDPR [164] and FIPPS [509], 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 [178]. 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 and 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 [37]. 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. [117] 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 [403].

10.5.2. 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 [215], organizational information systems [69], and e-commerce [9]. 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?" [407]. 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 [...]" [114].

Forms of impact assessment are known from technology research and computer ethics [240, 268]. With regard to privacy impact assessment [101], there are frameworks for companies or developers to assess the ethical impact of their technologies and products [525]. For highly sensitive data, such as data regarding health or religion, the GDPR prescribes such impact assessment [164]. 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 [269] 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.

10.5.3. 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 [201]. 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 [421] as reflected in the acceptance problems regarding electronic health records [83] or digitally enhanced ID cards [367, 484]. In this regard, user-centered design [7], and, more specifically, multilateral security [390], 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.

10.6. Conclusion

We presented an understanding of the privacy demands in Smart Metering from a consumer perspective. Based on a design case study approach [528], 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 [135], 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.

11.Discussion

This thesis contributes to HCI research by making two main arguments : First, taking a conceptual perspective, it discussed how end users can be supported in privacy decision-making. Here, the studies in the contexts of smartphones, smart homes and smart metering privacy provide lessons learned. Investigation of individual and collective sense-making of IoT data has led to a conceptualization of means for supporting privacy practices by adopting an end-user risk assessment approach. On a more general level, these findings may also contribute to a broader support of individual data literacy in IoT technologies.

Second, adopting a methodological perspective, the thesis demonstrates fundamental aspects to consider for better aligning usable privacy research and regulation processes. Particularly in the areas of smart metering (Chapters 4 and 10) and the connected car (Chapters 5 and 6), the research on usable privacy was strongly intertwined with regulative processes. In this regard, the thesis provides suggestions to better integrate both research on usable privacy and regulation processes.

11.1.End-User Risk Assessment

The studies presented in this thesis critically investigated how users related to their data while characterizing them in terms of privacy sensitivity using a practice lens [410], fostered by the "data work" [495] approach. Adopting a user perspective on privacy on the IoT and more specifically looking at practices of making data accountable, the studies show that data are of less importance to users when weighing privacy sensitivity. Instead, frequently, instances of what can be considered "folk risk assessment" was observed. The phenomenon unveiled features several connections to professional risk assessments, which originate in the organizational context. For example, in the ISO 2700x norm family [251], assets, risks and costs are key terms in ISMSs. The studies (Chapters 8, 9 and 10) show that these mechanisms are also important for end-user privacy. Still, as discussed in Section 11.1.1, when transferring the concept of risk assessment to the end-user context, some fundamental differences have to be considered. The

following section give room for a description of these differences and the challenges they pose when applying the method of end-user risk assessment and in the IoT context.

Furthermore, these mechanisms are not yet reflected in the practice of designing privacy management support. In this regard, the studies in this thesis have also identified possible ways by which to design in support of end-user risk assessment. Section 11.1.2, hence, discusses concepts for supporting risk analysis and data literacy more generally.

11.1.1. Perceived Risks, Assets and Costs

A great deal of research on risk assessment for users already exists in the area of usable privacy. For example, considerable amounts of research have targeted designing the presentation of privacy information from a user perspective based on metaphors such as nutrition tables [277, 278]. Such concepts typically highlight items such as data, recipient, data processor and purposes. However, taking a step back, given that privacy in an abstract concept, it remains unclear whether these items map on what users understand as privacy and whether they optimally support managing user privacy.

From a legal perspective, this uncertainty calls for defining the legally protected good that privacy is for users: "What should be protected by data/privacy protection measures?" Transferring this to the ISMS world, one would ask "What are the assets and their corresponding protection objects?" With regard to the challenge of understanding the phenomenon of "privacy" on the IoT and thus making the protection objective accountable, the studies on smart metering provide insights in different IoT contexts.

More generally, throughout this thesis, users also frequently expressed concern about "who gets what and how often." However, the findings especially Chapter 10 point to the fact that the "who" and "what" served as means to the end of evaluating the privacy *implications* of data disclosure. Users did not refer to what data should be directly protected but used data and third parties' resources as a

basis for their privacy risk assessment strategies. Such assessments were typically situated in considering what information could be deduced from the data to be disclosed and remind one of the management of "attack surfaces" discussed by Crabtree et al. [117]. However, while Crabtree et al. described the phenomenon qualitatively, they remained on a conceptual level.

The work on smart metering (Chapter 10) showed how the risk assessment model could be made usable for end-users: First, that indicated that users related to the possible consequences of disclosing data that they would like to keep confidential, were identified. Second, it was shown that presenting such undesired data use scenarios via a privacy management tool resulted in an improvement of the basis of decision-making and control of privacy perceived by users. A second important outcome of this research is the collection and presentation of concrete instances of what users wanted to keep private. The ways in which users assessed the perceived risks associated with what others might learn about oneself not only became clear when considering actual data in conducting "data work" [495] but also through the open-ended questionnaires about hopes and fears with regard to IoT technology (Chapter 10). Rather than referring to data, users spoke or wrote about which parts of their private lives they wished to keep private or felt uncomfortable disclosing. Perceived outcomes and implications for everyday life in terms of what others might learn about the data subject were mentioned frequently.

The mechanism of managing how one is seen by others is closely related to the concept of "face work" [207]. Many attitudes identified in the interviews hint at the existence of a similar mechanism concerning how the perception of one's own "face" is seen endangered as a result of potentially negative consequences, both socially and commercially.

Therefore, the previous studies suggest that support for managing privacy in IoT should incorporate and be grounded in the presentation of perceived risks. By unveiling the user language used to describe privacy-related issues and developing an initial catalogue of perceived risks, this thesis seeks to both foster the

compatibility of usable privacy and regulation (Chapter 4 and, to a lesser extent, Chapter 5) and to inform design of privacy management tools with new empirically grounded insights.

The risks associated with new technologies are often defined by experts. The results of the studies suggest that user vocabulary should be taken into account as a powerful resource for designing meaningful approaches to privacy management. In order to bring these perspectives together, risks must be rendered understandable and comprehensible from the user's point of view so that they can be defined together with stakeholders such as developers, designers and experts. In particular, an understanding of how these risks are constituted from the user's perspective must be developed. In this regard, user studies on perceived risks can contrast and/or extend experts' views in terms of the relevant issues to take into account, the vocabulary to be used, the degree of perceived severity and the risks to be assessed. In case of diverging risk perception, it cannot generally be said which side gets it "right".

Table 9: Matrix on the options when expert and user perception of risks are in dissent

	Expert-perceived risk	No expert-perceived risk
User-perceived risk	-/-	1. Take the user seriously: Discuss the assumptions that led to the judgment, review and understand user reasoning 2. Communicate to the user that there is no risk/provoke insight
No user-perceived risk	1. Own risk assessment based on asset assessment: How do users perceive assets and why? Normative: What are user assessments based on? 2. Communicate the risk in a user-centric manner. Perform protection task (one strategy: support data literacy [or privacy literacy, which data literacy is a part of])	-/-

When bringing together user and expert views on risks, there are basically four ideal-typical cases (see Table 9). (For the sake of simplicity, it is assumed that a perception of risk also includes its severity and type and ways of explicating and communicating it.) First, both sides could agree that there is no privacy risk. This might be the easiest case, as both sides will agree that no measures must be taken to protect privacy. Second, both experts and users could agree that there is a privacy risk associated with the use of a technology. In this case, the parties should collaborate on implementing measures for its mitigation and control.

The remaining two cases of dissent are more complex to solve. Third, if experts know about a risk that users do not perceive, the former's task is to empathize with users by understanding their perception of the value of the assets at stake. Based on this understanding, experts can go on to identify appropriate ways to communicate the risks and implement strategies to enable the effective protection of users. In this vein, there is a growing body of literature aiming at increasing privacy awareness [33, 400, 438]. Fourth, case users may perceive a risk that is not perceived by experts. In this case, experts should be sensitive to user concerns and engage in a discussion with them about the underlying assumptions that led to the evaluation, questioning not only the users' judgment but also their own. Should it be found that no risks exist in the case at hand, researchers should aim to foster transparency and provoke insights on the user side.

While the demonstration focused on a subset of IoT technology, using this awareness mechanism arguably can also inform design for other IoT contexts. Indeed, given the increasing complexity of IoT arrangements and their spread into more aspects of everyday life, making privacy implications transparent seems to be an urgent concern in terms of enabling people to maintain their privacy in the IoT era.

11.1.2. Supporting Tools and Strategies

Risk assessment for users is becoming increasingly difficult due to the emergence of abstract and invasive technologies, increasing value being placed on personal data and the decoupling of interdependencies (temporal, organizational and

contextual) and therefore needs support. In cases where the data provided are relatively familiar, such as an address or credit card information, attack vectors can be relatively clear. However, as IoT applications become commonplace, an increasing number of sensors are collecting abstract data, the information value of which users are not yet able to judge by themselves.

To support users in maintaining and regulating their privacy using end user risk assessment, the presented studies suggest two main approaches. First, means for cost-benefit analyses should be provided in privacy management tools. Second, taking a broader perspective that is decoupled from concrete use cases, methods intended to foster users' data literacy are suggested.

Providing Means for Cost-Benefit Analysis

The concept of an informed user assumes that he or she can derive all possible implications from the data presented to him or her. However, this is a somewhat idealistic picture that can be criticized from the perspective of both bounded rationality [202] and from the praxeological perspective [410].

The studies found that users use data, its recipients and the purposes of data collection as tools by which to assess data privacy sensitivity. This mechanism, however, leaves the burden of bridging the gap between the disclosure of data and potential effects on life to the user. through the use of advanced data analysis tools and means of analyzing big data, data can provide insights into private life that are not easy to anticipate, if at all. The emergence of data brokers and the resulting possibility of triangulating data streams will only increase the degree of abstraction. In this vein, it must be asked whether informed consent, in its current data-centered form, can live up to expectations and actually help consumers to appropriately manage their privacy in a digital world.

Introducing a user perspective, the studies' results suggest that design for privacy management should attempt to bridge the aforementioned gap by adopting an "information-centered" approach. The key implication for the design of an information-centered approach to privacy is making the implications of privacy

settings understandable to users by not only showing what benefits a service may provide but also demonstrating what new threats may arise from subscribing to a service. In this respect, Chapter 10 presented a holistic study on transferring the concept of *information-centered* privacy information into a design for privacy management in the field of smart metering. The results suggest that extending currently dominant data-centered privacy tools with information-centered decision-making support changes users' attitudes towards disclosing (or not disclosing) data (see Chapter 10). Qualitative assessment further suggests that presenting real-world scenarios help users to bring their service subscriptions more in line with their privacy demands, thus contributing to reducing the attitude-behavior gap [19, 133].

While tools for abstract risk-benefit analysis exist, grounding them in everyday stories seem promising to provide a bridge from technologically complex, abstract information to the data to be transferred. Ideally, these categories would be generated by the users themselves. There are two main reasons why this would be preferable: First, user-generated risks and benefits improve the comprehensibility of privacy implications when deciding about data disclosure by providing suitable and relevant background information.

Second, identifying concrete impacts increases accountability of privacy implications beyond information about the data disclosed and their receiver alone, as legislation typically demands. For example, making the risks and benefits that arise from a service visible to consumers also extends the principle of purpose limitation of data disclosure, as demanded by German law [201]. In abstracting from concrete data sets, this research came closer to understanding what people do when making choices concerning privacy in respect of smart metering and both identified and designed starting points for users' decision-making with regard to their privacy.

Data Literacy

There are many definitions of the term data literacy (see [295] for an overview of related definitions). For example, as part of statistical education [209, 470], data

literacy is often researched as a skill for teaching professions and librarians [294, 334, 490] or as part of school education [327, 336]. Often, these concepts are used to refer to the entire process of collecting, managing, evaluating and maintaining data. Featuring a stronger notion on the interpretative skills in investigating data, according to [401], data literacy enables individuals to access, handle, interpret, critically assess, manage (incorporating preservation and curation), and ethically use data. Similarly, Mandinach and Gummer [333] define data literacy as "the ability to understand and use data effectively to inform decisions." According to Koltay [295], this understanding of data literacy highlights the skills required to transform "data into information and ultimately into actionable knowledge."

Arguably, data literacy is not only of concern for teachers, sociologists or research. Instead, in today's data-driven economy and society, data literacy is a key skill for any person and an essential competency for regulating one's privacy. The studies presented also show that data literacy is not static but is rather context-dependent, evolves and may improve over the course of technology appropriation, especially if users are provided with feedback on data (Chapters 7, 8 and 9).

Privacy and data literacy can be seen as co-evolving concepts: On many occasions, such as during creativity workshops on information visualization or during interviews, participants had moments in which they reflected on privacy. Particularly when engaging in "data work" [495], participants would at times discover information about themselves or map data to their everyday doings and be surprised at being able to see their lives reflected in data [43, 262, 324].

Long-term Living Lab-based studies also revealed that data literacy mainly developed in late phases of appropriation of technology. Particularly during early workshops, participants often had few ideas concerning both the potential use and misuse of data. Although they already spoke in terms of undesired scenarios, such scenarios were often based on media stories instead of being driven by concerns regarding misuse perceived individually relevant. By seeing, exploring and using data, however, users improved their data literacy—a crucial skill for managing

one's personal digital footprint and generally navigating in an increasingly digital world.

Against the backdrop of these experiences, people arguably need to learn about data and their potential meaning, at least at a basic level. Instead of concealing complexity, it should be reduced, but still present by means of transformation to more accountable form, to allow people to interact with and establish a rough understanding of data [217].

The findings of the thesis suggest several potential approaches to fostering data literacy [217], which can be divided into two main categories (Table 10).

Table 10: Different methods for supporting data literacy

Learning	**As a side effect**		**In focus**	
Type	Data-based services	System intelligibility dashboards	Data work	Learning tools /methods
Chapters	6,7	8	7,8	9,10
Scalability	High	High	Low–mid	Mid–high
Availability	High	Mid	Low–mid	Low–mid
Location	Independent	Independent	Dedicated	Both possible
Term	Short	Long	Mid	Short
Expertise needed	High	Mid–high	Low	Low
Support provided	None	Low–mid	Strong	Mid

First, there are means to support data literacy as a side effect of using technology. To some extent, the use of **data-based services** themselves proved helpful in helping users to independently gain an understanding of what can be done with data. Such services are highly available commercially and are thus also scalable solutions in terms of supporting privacy literacy. To actually improve individuals' data literacy, however, the studies found that users need some technological understanding to be able to transfer the mechanisms that operate in one service to other possible services. Less tech-savvy participants seldom profited in the way that more experienced users did.

In this regard, the studies showed how **system intelligibility dashboards** can be designed to be sensitive to novice users' demands. The field of information visualization [97, 455] can provide important starting points with regard to how data can be visualized in a meaningful way. Additionally, the studies highlight how concepts from the field of end-user development [40, 89, 177, 323] may provide flexibility to both novice and expert users and thus help to address highly individual information demands. These systems could be provided as part of a product by default and thus will be able to scale very well. However, implementing said functionality would require additional effort on the part of companies, which makes them a seldom seen feature.

Second, prior research in the area of usable privacy has yielded methods specifically designed for the purpose of fostering data literacy, such as nutrition tables [277, 278]. Research in this thesis relied on applying or (further) developed several methods to support data literacy:

The method of **data work** [495] has been shown to be able to support data literacy in many ways in different fields of research, but mainly in the smart home. Adopting this approach reflection workshops and on-site interviews in which users were asked to explain the data on their own devices and discuss about visualization demands alongside, were conducted. Frequently, participants then referred to what was occurring in their homes to, for example, explain peaks in energy consumption, opened doors or the activation of movement detectors. In projects related to mobility, similar patterns were observed: For, for example, going shopping or (not) driving to work. Individual assessment of data using dashboards has therefore been shown to be able to promote data intelligibility and privacy awareness to a certain extent.

The application of **learning methods and tools** as part of studies in this thesis, attempted to find a middle way between the demands of scalability on the one hand and individualized support and experience also for users with different savviness on the other hand.

In this regard, various modes of collective data exploration (e.g., using gamification and playful exploration strategies [130]) were used in letting a group of users "investigate" the private life of a single participant (see Chapter 8). In these cases, the participants were highly motivated and learned about privacy implications in an enjoyable manner. As an alteration, also anonymized or synthetic data were used. Doing so reduced privacy invasiveness, especially when reflecting on data in groups. However, it allowed for better scaling of workshops without needing to collect participant data in advance.

In addition, some of my studies made attempts to overcome the traditional technological boundaries of isolated sensors or services and provide a 360° view on the digital self. Up to now, most design approaches to understanding and supporting privacy have focused on single technologies. With increased networking of devices and data streams, a core feature of the IoT, such an approach can only provide scattered parts of a puzzle. To gain a comprehensive view on the digital selves, users need means by which to assess the privacy implications of data-sharing practices *across* devices and applications. The studies represented the first steps in such a direction, for example by including smart metering in the smart homes of Living Lab households if available (Chapter 8). The increasing amount and complexity of data likewise call for flexible and individualized approaches to information visualization [89, 262] to provide meaningful information from data. Beyond technologies designed to visualize data for consumers, the right laid out in Articles 12 and 15 of the GDPR [164] to receive all data collected from a service provider may also play a vital role.

While the data literacy of the individual is of pivotal importance, one should not reduce the concept to the individual level. Instead, it should be recognized that data literacy will be a core capability in future societies. As early as 2014, a report to the Obama White House suggested that

> *"[White House Office of Science and Technology Policy] together with the appropriate educational institutions and professional societies, should encourage increased education and training opportunities concerning privacy*

protection, including career paths for professionals. Programs that provide education leading to privacy expertise (akin to what is being done for security expertise) are essential and need encouragement. One might envision careers for digital privacy experts both on the software development side and on the technical management side."[402]

While education on data and their potential use and misuse is needed, as it could increase data literacy, in this thesis instead considered how service providers and/or regulations could make efforts to support users in managing their privacy in order to reduce the extent of the attitude-behavior gap in online privacy [19, 120]. The findings led to the identification of strategies for service providers to adopt more usable strategies of informing customers. Likewise, these design patterns could also be included in regulative processes, for example, to extend the purpose-limitation mechanism in the GDPR [164] by supporting a risk-based approach to evaluating the privacy impact of data disclosure.

Experience has shown, however, that voluntary approaches such as promoting corporate social responsibility are usually not sufficient on their own but instead need to be accompanied by legal regulations. This observation raises the question of how usable privacy research can contribute to the regulation of emerging technologies.

11.2. Aligning Usable Privacy Research and Regulation

As outlined in Chapter 2, privacy is a dynamic concept in that it evolves with emerging regulations and technologies and social changes. Accordingly, usable privacy research should carefully consider these factors. The concept of privacy is constantly being re-negotiated alongside evolving contextual socio-technical developments. Several of the studies described in this thesis reflect this evolution, as they were conducted in periods in which regulations and technologies evolved.

For example, during the heuristic analysis of users' privacy demands (Chapters 4 and 5) with regard to smart metering, in 2013 [171] and 2014 [170, 366], the BSI[7] and the National Metrology Institute of Germany[8] released a series of documents regarding the design of smart metering systems and their security features. Some of these documents' attachments were last updated in January 2019.

Similarly, the German Federal Ministry of Transport and Digital Infrastructure set up an Ethics Committee on Automated and Networked Driving consisting of five working groups in September 2016. It issued its report in June 2017 [80], during the period of time when investigating the privacy concerns associated with connected cars (Chapters 5 and 6).

On a more global level, my studies roughly fall within the same period as the development of the new European GDPR [164]. Its first proposal was made public on January 25th 2012 [103]; it was finalized on April 27th 2016 and put into effect on May 25th 2018 [166].

These examples demonstrate that there is no sequential process of first researching a phenomenon and then regulating it; rather, both regulation and research on individual privacy demands are acting and co-evolving, unfortunately often in a rather unaligned manner. Hence, this thesis argues that both fields could benefit from better aligned usable privacy research and regulation processes.

However, promoting such alignment would not be a one-way road but would instead have implications for both sides: On the one hand, regulations would have to take usable privacy research more seriously; on the other hand, usable privacy research would correspondingly have to take regulation processes more seriously. In the following, the arguments concerning how research on usable privacy could adapt to regulations, and vice versa, are outlined in greater detail.

---

[7] Bundesamt für Sicherheit in der Informationstechnologie
[8] Physikalisch Technische Bundesanstalt

11.2.1. Regulations should take usable privacy research more seriously

Regulation efforts have become increasingly aware of user issues. The Ethics Commission [80] on automated and networked driving, for instance, is a positive example of legislation taking the user into account: In addition to experts on law and technology, experts on technology assessment and human sciences from the Federation of German Consumer Organizations were invited, as well as a bishop [80]. However, consulting experts does not provide an understanding of either security or privacy in practice. In this regard, user studies, preferably accounting for the complexity of the real world, are indispensable, as they can show how the threats and risks anticipated by experts can be handled in a practical fashion. Furthermore, user studies can identify the use cases and risks perceived by users that may not been anticipated but could potentially crucially impact the security and privacy of the overall system.

Moreover, from experience of being part of a smart metering project, both ethical and usable privacy considerations are often not taken into account when planning regulatory measures (Chapter 4). This is particularly true when planning legislation intended to protect critical infrastructure but can also be witnessed when the protection of individual privacy is being regulated. In such regulation processes, technological, legal and economic perspectives seem to dominate, whereas the consumer perspective is often underrepresented. The studies within this thesis, however, demonstrate the limitations of technologically oriented regulations that do not take into account the individual perspective: Transferring abstract legal concepts to specific technologies or contexts without understanding user demands and the appropriation of technology may actually undermine security and privacy practices and result in a decline in protection, as described in Chapter 4.

Therefore, demands and tools for usable privacy need to be researched and defined with respect to the technology in question and against the backdrop of an understanding of how that technology is being or will be used. Historical examples show how privacy demands and relevant regulations have been constantly (re-) negotiated and (re-)defined against the backdrop of technologies such as

photography, the telephone or computers [24, 463, 510]. The presented studies show how various IoT technologies pose new challenges to the concept of privacy and thus the question of how usable privacy controls should be designed.

In recent years, the HCI community has taken a turn to user practices [308], acknowledging the complexity of interacting with technology in the wild: "because [user practices] are contingent, mediated and cannot be understood without reference to the particular place, time and concrete historical context where they occur, they can only be studied 'close-up'" [308]. In a similar vein, it can be argued that the legal perspectives on the privacy issues associated with new technologies would benefit from taking into account the privacy practices of users.

The PbD principles [91, 311], which are reflected by the GDPR (e.g. in Art. 25 GDPR, as "Data protection by design and by default" [164]), serve as a prominent example in support of the above arguments. The Article states that data controllers shall "implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" [164]. The principles thus set highly abstract demands for data protection measures, calling for an individual interpretation and weighing of the "appropriateness" of such measures for each point of data collection. For each point, various stakeholders' interests need to be considered carefully—not least the demands of users. Users, however, may themselves have self-conflicting goals. There is an internal tension between desiring quality of service and privacy.

This thesis have demonstrated how considering a user perspective is required for appropriately understanding suitable solutions in light of said tension, for example in the field of smart metering (Chapter 4). The consumer interface for German smart meter gateways, for example, was designed as a common LAN plug (RJ-45), which was intended to allow the integration of these devices into home networks. However, this specification disregarded the fact that the gateways are not physically accessible for most inhabitants of rental apartments. As a result, the most common solution intended to allow users to obtain feedback on their energy

consumption quasi-automatically resulted in a serious decrease in privacy: Users had to send all of their data to the respective utilities via the Internet, where consumption would be presented on a personalized webpage. To make these conflicts of interest visible and to embed this perspective into privacy regulations for the IoT, it is important to understand what interests and goals users have in using a technology. These requirements cannot be deduced from mere practice; instead, when designing privacy restrictions for technology, practices associated with the use of technology and data need to be understood to design for usable privacy.

To not only passively react to legislative initiatives and instead be able to actively inform regulations with such a user's perspective, research on usable privacy should continue to strategically investigate key emerging technologies.

11.2.2. Usable privacy research should take regulation processes more seriously

There are many different methods for studying privacy issues empirically. In smart home studies (Chapters 7 and 8), a Living Lab approach with a long-term focus was implemented, for example. This allowed studying how privacy practices are shaped by the appropriation of technology and how users made data accountable when learning about the relevance thereof to their personal everyday lives. In particular, to gain an understanding of how to design for data literacy, the users needed to establish such literacy themselves. As outlined in Section 8, growing data literacy typically needs time, as the appropriation of the technology in question is a slow process. Short-time inventions thus fail to uncover such phenomena.

The early and constant involvement of users in the co-creation processes of IT artifacts is seen as an important characteristic of the Living Lab approach [436]. By allowing for long-term and sustainable collaboration, Living Labs enable the capture of both the ideas *and* the actual experiences of users in real usage contexts. Longitudinal field research holds, it is suggested, "a considerable if often

unrealized potential for the progressive refinement of design concepts and the evaluation of the artifacts that result" [375].

Long-term, user-centered approaches have their merits, but they come at a price: To participate in the legislative process and be able to provide a well-grounded user perspective, user research needs to fit the timelines of such legislative processes. Once the process is complete, the user perspective can only be addressed by making repairs to a predefined framework of specifications. In this regard, long-term research faces two major challenges:

1. Long-term studies such as those adopting Living Labs approaches often take longer than 12 months when including planning, the process of conducting and analyzing technological appropriation. While regulative processes are not necessarily swift, they may have demanding schedules, meaning that it will be difficult to incorporate the findings of HCI research. From this perspective, HCI needs to identify suitable ways of collecting rich feedback concerning privacy practices while also cooperating with the requirements of regulative processes.
2. More importantly, besides the organizational challenges, there are conceptual challenges that HCI researchers must confront. In terms of the setup, Living Lab approaches underemphasize the relevance of users' first contact with an innovation. The setup phase is of crucial importance for privacy management which may not be changed for a long time of use and long into the appropriation phases. More importantly, in this phase the user must be considered a novice who has no experience using the technology: When new devices are introduced into household ecosystems, privacy settings will have to be determined without a deeper understanding of the consequences thereof due to a lack of personal experience on the part of users. This creates a kind of dilemma, as, when managing privacy on the IoT, the relevant settings have to be identified prior to the use of a device. When studying usable privacy, demands of novice users and experts should be investigated using different methods, as has been suggested by findings in other fields in HCI [323, 474].

Hence, the method toolboxes of usable privacy researchers should be supplemented by focusing on key technologies in advance, as well as by the use of more lightweight, short-term and heuristic methods. In this sense, the thesis does not only a call for legislation to open the process for a human perspective in a one-way manner, rather, similarly, the HCI community itself must evolve with regard to three specific and interconnected aspects:

1. Research on HCI should not be limited to investigating the appropriation of existing technologies and reacting ex post or identifying ideas concerning the next generation of a product.

Instead, it must also methodologically be able to look into the future to provide empirically based technology assessments and subsequently derive recommendations for design intended to inform regulations.

From a market-liberal point of view, users in the private sector can, in principle, reject a product due to its possibly disadvantageous data protection guidelines. Even in this context, however, experience shows that such market functions do not work for consumer IT. For example, there are no specific privacy regulations regarding smartphones. Driven by market mechanisms, the current product landscape basically features only two viable ecosystems, namely those of iOS and Android—both of which are highly invasive of privacy.

In the public infrastructure sector, the situation is even more problematic, as people may be obliged to install devices such as smart meters. Today, government agencies frequently specify privacy regulations without performing a detailed assessment of the user's perspective. To this end, however, regulatory bodies cannot and should not wait for technology to be adopted by the general public and unfold its effects on privacy before they step in but must instead make long-term decisions in the early stages of a product or technology's diffusion.

In both the private and the public sectors, regulations therefore must provide some technology-specific minimum requirements (in terms of IT security and data protection) for all market participants. To avoid such lack of specific privacy regulation in the emergence of future technologies, regulating bodies should be able to draw on empirically reliable technology impact assessments to translate experiences into design requirements that are reflected in legislative guidelines.

2. Research on HCI should identify and investigate emerging key technologies in advance, before they are ready for regulation.

Following the first point, if the HCI research community has the ambition to help shape future social developments (not only with respect to privacy), then it must occupy important fields at an early stage. In this way, research results regarding

experience of technology appropriation can directly fuel legislative commissions such that users' voices will not only be present but well-grounded in scientific rigor. One framework that is particularly suited for probing into possible futures and designing potentially viable solutions in multi-stakeholder scenarios is that of Living Labs. In a similar vein to participatory design [112, 281], Living Lab research seeks to align the interests of different stakeholders [122, 191], for example by identifying means of multi-lateral security and privacy [390, 406, 475]. In societies that are changing at an increasingly rapid rate, however, manageable alternatives that flexibly provide valid answers to current requirements and questions must be identified.

3. Research on HCI needs to balance research depth with the practical necessities of regulation to be able to make contributes that are in-line with existing formats and process boundaries.

Informing regulation with insights on technology appropriation with Living Lab research is a long-term commitment and, like practice-based research, poses a "labor-intense, risky, and long-term research approach […]" [528]. However, my research (Chapter 4) shows that many framework conditions may still be in flux during the development of regulatory processes. Technological development is also steadily increasing in speed. Against this background, new issues can arise at short notice, such as new stakeholder interests, which will need to be addressed swiftly. In this regard, HCI needs to acknowledge practical needs of regulative processes. In order to have an impact, in addition to long-term research, HCI should provide methods by which information can be provided in response to user demands in a given situation on a short-term basis.

The studies presented show how some methods could fit into a regulatory process and contribute to a discourse. Table 11 describes these methods with regard to when they should be applied, what insights they may provide for the regulatory process and the amount of time they require to produce results.

Scenario-based analyses can inform regulative processes that may already be in late phases and lack a user perspective. Research presented in Chapter 4, engaged with the regulative process only in a late phase. Until that point, many

considerations were purely driven by an IT security perspective. To provide a user perspective within a fairly brief period of time, a scenario-based analysis was conducted. Such an approach can highlight some major concerns by applying heuristics for user demands, especially since it was conducted against the backdrop of extensive pre-studies in the field of energy monitoring [256, 259, 264, 446, 449]. Similarly, when some well-grounded hypotheses have already been formulated, surveys can be used to test research findings and/or the assumptions embedded in regulations quantitatively, before they are codified (Chapter 10). These approaches, however, should be used in combination with more in-depth research methods. Should regulations still be in an early phase, research on user demands should more actively engage with users.

Living Lab studies are arguably the most time-consuming alternative, but they can provide a platform for strategically investigating the appropriation of privacy demands in a new technology. By prototyping possible futures, research conducted in Living Labs can inform regulations with well-grounded insights on how an emerging technology is likely to be used and which protection mechanisms users may seek in the long-term. They therefore allow for the integration of a variety of methods (including co-design workshops, data work and prototyping), many of which applied in Chapters 7 and 8.

For example, co-design workshops were a method used within the Living Lab settings (Chapters 7 and 8) to identify user demands with regard to service design and visualization mechanisms. These can also be conducted with users that are not part of Living Labs and can provide results with which to inform potential protection concepts fairly rapidly. Integration in Living Labs will provide participants with a stronger background and greater experience regarding a technology and may thus lead to more well-grounded findings.

The best reason for embedding co-design workshops in Living Lab settings, however, is arguably the possibility of continuing the prototyping process in real-world environments. Prototypes were developed both within (Chapters 7 and 8) and outside of Living Lab settings (Chapter 10). The prototypes allowed for

breaching into possible futures of user interaction with technologies (and their privacy management tools).

Similarly, also the data work method was applied both within (Chapters 7 and 8) and without (Chapter 9) Living Lab settings. Running a Living Lab setting enabled collecting and providing a data corpus for applying data work sessions based on actual and contextualized personal data. While it increased the amount of effort that needed to be invested in, the long-term personalization of data for such data work sessions allowed for the investigation of how users of smart home technologies related to a continuous stream of data and the possibility of visualizing and analyzing them over longer periods of time. An alternative would involve the use of synthetic data to accelerate the process of analysis at the cost of personalization and depth of insights. Also, Chapter 9 demonstrates use of the method of collective data work, in which data from smartphones was collected over the course of several weeks. Visualizing the data of only a single person, other participants were assigned to attempt to investigate the person behind the data in a game-like fashion (Chapter 9). These data work sessions were aimed at both fostering participants' data literacy and researchers understanding of participants' privacy demands in terms of perceived sensitivity.

Table 11: Methods for incorporating user-centered privacy in regulations for emerging technologies

	Timing	Extent	Period	Insights	Use cases
Scenario-based analysis	Up to late in the process	Expert analysis (low)	Short-term	Heuristics for user demands	In urgent need of input from a user perspective
Co-design workshops	Before or during regulation	User co-creation	Short-/ mid-term	User-centered protection mechanisms	Exploration of possible protection concepts
Living Lab studies	Before regulation	In-depth qualitative studies (large)	Long-term	Users' privacy demands using technology in practice	Strategic exploration of privacy demands in specific contexts over the course of appropriation
Collective data work	After regulation or as part of Living Labs	Visualizing and reflecting on data	Short-/ mid-term	Reflections on data to explore privacy demands	Privacy risk analysis of data

Prototype studies	Any time	Qualitative testing (medium)	Short-term	Privacy demands on first tech contact	Assessing user privacy demands in sign-up phases
Surveys	Up to late in the process	Testing hypotheses (low)	Short-term	Evaluation of potential protection mechanisms	Testing hypotheses about assets and privacy risk understanding

In a nutshell, HCI can exploit its strengths to represent a user's perspective with regard to the human factors of security and data protection to shape regulations and enforce design guidelines by law. To play an active role and make a valuable contribution, HCI research must balance its choice of methods and cooperate with the requirements of regulators. This would be an important step in allowing HCI research to become involved in the further development of society and establish itself outside of research as a field that is relevant to IT security regulations.

11.3. Limitations

This thesis highlights ways in which privacy management tools can be rendered more usable. However, there are some limitations due to the manner in which this research was conducted and technological advances; these limitations are discussed below.

First, from a methodological perspective, the results of this study cannot and should not be generalized in any statistical sense, as they have not been evaluated using a large-scale qualitative approach. Given their sample sizes and focus on Germany, the studies do not feature a representative sample of users. Despite this limitation, however, in the sense of theoretical sampling [110], our findings draw on a rather broad spectrum of participants. Germany is considered a leader among Western societies in its treatment of privacy and data protection issues. With the advent of the GDPR [164], these aspects have also become more pressing in the other EU countries. In a similar vein, our focus groups were imbalanced in terms of gender and could have benefitted from more female participation. Treating generalizing from the hypothetical to the "real" with a degree of caution is important. Still, having found similar schemes throughout a wide array of studies across use cases, the findings are strongly grounded in user-centered research.

Another methodological limitation concerns the general level of uncertainty in studies focused on future technologies: Methods for researching the future are inherently speculative to a certain extent. However, through scientifically cautious high-quality work, it is possible to estimate futures.

On another note, the majority of our participants had neither a smart meter nor a connected car. However, when the IoT enters households, users will inevitably have to make privacy decisions without prior experience with these systems. In line with previous research on technology appropriation [473], this thesis specifically wanted to gain an understanding of perceived privacy issues from the start, when users are necessarily more-or-less non-experts (in the sense that, besides the smartphone case [see Chapter 9], they have only a vague familiarity with the technologies at hand). Moreover, with users having to agree to certain levels of privacy protection and data disclosure upon service subscription, usable privacy in IoT by its nature has to cope with lay users to be effective from the very beginning (see also Chapter 10).

Researching novice users' privacy demands is not to be seen as a substitute but rather as a supplement to and extension of the user debate: this thesis investigated inexperienced users to see what they needed. In addition, it still seems reasonable to carry out appropriation studies on privacy similar to the studies conducted in the smart home (Chapters 8 and 10), as needs change over the course of technology appropriation.

Overall, during this research, it was necessary to treat the topic of privacy carefully in order to avoid promoting any responses on the part of participants:

Making privacy an explicit topic in interviews or workshop is prone to prompting participants to say participants say what is desired but does not necessarily reflect their behavior in daily life; this is known as the social desirability bias (e.g. [212, 368, 418]). While this thesis indicates that privacy was a major issue for participants (Chapters 7, 8, 9 and 10), at the same time, workshops still needed to encourage the participants to think creatively about the potential uses of data.

12. Conclusion and Outlook

This thesis shows that for users to be able to play an active role in managing privacy in a connected world, highlighting potential real-life consequences may support and empower them to ascribe meaning to abstract data collection and analysis as a means for supporting existing privacy practices, which often revolve around assessments of what "others" could discover by analyzing data.

Without further support, the potential of analyzing, for example, driving behavior, was often unclear to users. In this context, even if users knew what they wanted third parties not to be able to gain information about (e.g., driving behavior), they were uncertain as to how this goal could be mapped onto disclosing or not disclosing (combinations of) sensor data. They were unclear as to how sensor data could be used to obtain the information in question.

As a result, this thesis argues that public policy has to go beyond attempting to ensure privacy via privacy by design approaches and actively take user demands into account. Privacy by design could be adapted to user requirements: Informed by user studies, more privacy-friendly infrastructures, such as trust concepts or a local proxy cloud infrastructures, could be applied. However, further investigations should also be carried out into the uses and appropriation of technology: In addition to a technical component intended to protect privacy, information should also be provided about the data collection and processing taking place, as users need or expect to apply their privacy practices to such processes.

In this regard, this thesis revealed three major challenges:

First, existing concepts with regard to privacy awareness do not sufficiently address the factor of embedding privacy into everyday practices. Information provision requiring low (not only cognitive) levels of attention (e.g., ambient awareness techniques) are underresearched. Systems often lack dedicated visualizations that are designed to promote privacy from a user's perspective. Instead, standby and on/off buttons are used to control a device, but it is often

difficult or impossible to determine whether sensors are currently collecting data or not (for example, by eCall in the connected car). In the sense of the self-disclosure and intelligibility of devices, however, privacy features or settings should be made clearly visible. For example, webcams often communicate their general off/on-status via an LED. With regard to other hardware, often times, it is unclear whether a television or smart speaker is listening. In any case, the data collection and sharing practices often remain highly unclear. Researching suitable low-threshold ambient awareness support for privacy and/or data collection is an area of investigation with significant potential for improvement.

Second, research in the field of information visualization must be further advanced in order to promote data literacy, especially privacy literacy. Visualization concepts for privacy invasiveness or impacts need to be better understood; dashboard concepts have emerged in recent years for this purpose. These must be context-specific and tailored to the specific application case in order to optimally address user needs. It remains important to acknowledge that one size does not fit all and that tools intended to promote data literacy need to be flexible. Similarly, studies could identify individual data protection requirements across different use cases. Regarding the risk assessment support, this thesis identified a key metaphor that users of connected services applied in their privacy practices. Still, further research is needed for a deeper understanding.

As a next step, the concept of folk risk assessment concept should be evaluated using real data in various application areas. In addition, potentials should be tested as to how the concept of risk-based assessments can be reflected and embedded in the GDPR. A first point of reference here could be risk assessments, as they are now necessary in organizational contexts.

Third, it is necessary to further investigate how jurisprudence and design for human factors can be further integrated into practice so that a regulatory process can take human factors into account. However, from the HCI perspective, further methods need to be tested in order to fit in well in this context. The work presented in this thesis has already provided some starting points to regulate networked

systems in a technically and practically secure and data protection-friendly manner. HCI could bring insights about balancing value-proposition and usable privacy from a user perspective to the regulators tables to minimize the risk of regulatory stillbirths.

13. Appendix

13.1. Questionnaire about Smart Meters

Note: We will hold a raffle that includes all carefully completed questionnaires. The raffle will be for four vouchers with a value of €20 each for Amazon, the local mall or the DM drugstore. (More information about the raffle can be found at the end of the questionnaire.)

Personal data

Personal data will only be used 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.

To understand your opinion and analyze your responses, please provide us with 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 costs in your household? ☐ Yes ☐ No

What is your monthly gross income? (Optional) ☐ None ☐ €1–€450 ☐ €450–€2,000 ☐ €2,000–€4,000 ☐> €4,000

Informative text for questionnaire

Rising electricity prices have become a trending topic in recent years. For many people, electricity has become an increasingly important factor in their household budgets. But where and how can you save? In the near future, a smart meter, which

would simply replace your old electricity meter, could provide you with the information about and assistance on 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 patterns and leaks that might have gone unnoticed. In addition, a smart meter can provide information on how much electricity was and is currently being consumed (e.g., via an app on a smartphone, tablet, laptop or computer). Thus, the consumer can gain control, and, ultimately, power consumption can be lowered.

The utilities themselves gain various advantages from smart metering. A smart meter can transmit power consumption in near real-time to the respective utility, allowing more detailed calculation of the power required and thus limiting excessive overproduction. Such a mode of operation also protects the environment because the capacity buffer required to keep the grid stable can be reduced. Smart meters thus provide important benefits to both consumers and providers.

The German federal government has initiated a process through which smart meters will be installed voluntarily in a consumer's household on request. In this questionnaire, we want to learn about your personal attitude toward smart metering.

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

Introductory questions on the topic

What comes to mind when you think about the topic of electricity as connected with safety?

What comes to 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 the customer information provided to the utility company?

Settings and user profiles for smart meters

Imagine you could assess the information on the power consumption of any person or group of people participating in smart metering if, in return, you had to share your information as well.

With whom would you want to share your data (e.g., neighbors, friends, family, other people, the utilities, the federal government or the Federal Office of Energy and Environment, anonymous comparison websites or other companies involved in the supply of electricity)?

Why would anonymous power consumption data from other households be interesting for you?

What do you think about the fact that others can view, for example, your energy consumption for the current day, the previous day or the previous month? How would you characterize the differences of sensitivity of your data based on what can be viewed and when?

Who do you see as responsible for ensuring that your energy consumption data are accessible only to those people and organizations you would want to have access to the data?

Privacy of smart meters and energy profiles

People might share data on current energy consumption because they believe in the value of comparing with each other in terms of energy consumption. Which safeguards would you wish to have in place in order to protect your data? Which concerns do you have with regard to distributing the data? What data do you consider particularly worthy of protection?

How do you rate the difference between others knowing your current total electricity consumption in watts and others knowing your current consumption based on individual electronic 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 privacy and security concerns related to smart meters? What is your view on the following tension: More privacy provides fewer savings, while less privacy results in 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 utilities and possibly other parties, such as the Consumer Association? Imagine that, in this scenario, you yourself would be able to access all consumption data, including the consumption of individual appliances Note that this would mean that you would not receive any hints or tips concerning saving energy.

Manipulation, crime and security

You can save money with smart metering, but criminals could interrupt or access the data transmission to utilities, for example to manipulate consumption information. How would you assess this risk?

Imagine that a smart meter comes with a seal of approval or certificate from a federal office (for example, the Federal Office for Security in Information Technology). To what extent would this alleviate your concerns, if at all?

Acceptance of smart meters

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 to receive from a smart meter? What else should a smart meter be able to do for you?

How would you rate additional functions, such as activating an alarm when a stove is left on or receiving relevant personalized advertisements when a smart meter notices patterns such as a refrigerator consuming too much power?

Dissemination of technology

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 responsibility of the household given the potential electricity savings?

What do you think is critical for the successful adoption of smart meters?

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

If you want 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 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!

14. References

[1] Abascal, J. and Nicolle, C. 2005. Moving towards inclusive design guidelines for socially and ethically aware HCI. *Interacting with Computers*. 17, 5 (2005), 484–505.

[2] Abdulrazak, B. and Helal, A. 2006. Enabling a Plug-and-play integration of smart environments. *2006 2nd International Conference on Information & Communication Technologies* (2006), 820–825.

[3] Abowd, G.D., Bobick, A.F., Essa, I.A., Mynatt, E.D. and Rogers, W.A. 2002. The Aware Home: A living laboratory for technologies for successful aging. *AAAI Technical Report*. 02, 02 (2002).

[4] Abowd, G.D. and Mynatt, E.D. 2000. Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction (TOCHI)*. 7, 1 (2000), 29–58.

[5] Abrahamse, W., Steg, L., Vlek, C. and Rothengatter, T. 2005. A review of intervention studies aimed at household energy conservation. *Journal of Environmental Psychology*. 25, 3 (Sep. 2005), 273–291. DOI:https://doi.org/10.1016/j.jenvp.2005.08.002.

[6] Abrahamse, W., Steg, L., Vlek, C. and Rothengatter, T. 2007. The effect of tailored information, goal setting, and tailored feedback on household energy use, energy-related behaviors, and behavioral antecedents. *Journal of Environmental Psychology*. 27, 4 (Dec. 2007), 265–276. DOI:https://doi.org/10.1016/j.jenvp.2007.08.002.

[7] Abras, C., Maloney-Krichmar, D. and Preece, J. 2004. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*. 37, 4 (2004), 445–456.

[8] Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A. and Smith, M. 2017. Obstacles to the adoption of secure communication tools. *Security and Privacy (SP), 2017 IEEE Symposium on* (2017), 137–153.

[9] Ackerman, M.S., Cranor, L.F. and Reagle, J. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. *Proceedings of the 1st ACM conference on Electronic commerce* (1999), 1–8.

[10] Acquisti, A. 2010. The economics of personal data and the economics of privacy. (2010).

[11] Acquisti, A., Brandimarte, L. and Loewenstein, G. 2015. Privacy and human behavior in the age of information. *Science*. 347, 6221 (Jan. 2015), 509–514. DOI:https://doi.org/10.1126/science.aaa1465.

[12] Acquisti, A. and Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Privacy Enhancing Technologies*. G. Danezis and P. Golle, eds. Springer Berlin Heidelberg. 36–58.

[13] Acquisti, A. and Grossklags, J. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy*. 2, (2005), 24–30.

[14] Acquisti, A., John, L.K. and Loewenstein, G. 2012. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*. 49, 2 (2012), 160–174.

[15] Adam Schlosser 2018. *You may have heard data is the new oil. It's not*. World Economic Forum.

[16] Adams, A. and Sasse, M.A. 1999. Users are not the enemy. *Communications of the ACM*. 42, 12 (1999), 40–46.
[17] Aichele, C., Doleski, O.D., Arzberger, M., Dieper, S., Dirnberger, J., Dornseifer, H., Fey, B. and Frank, R. 2013. *Smart Meter Rollout: Praxisleitfaden zur Ausbringung intelligenter Zähler*. Springer DE.
[18] Aigner, W., Miksch, S., Schumann, H. and Tominski, C. 2011. *Visualization of time-oriented data*. Springer Science & Business Media.
[19] Ajzen, I. and Fishbein, M. 1977. Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*. 84, 5 (1977), 888–918. DOI:https://doi.org/10.1037//0033-2909.84.5.888.
[20] Akerlof, G.A. 1970. The market for" lemons": Quality uncertainty and the market mechanism. *The quarterly journal of economics*. (1970), 488–500.
[21] Aldrich, F.K. 2003. Smart Homes: Past, Present and Future. *Inside the Smart Home*. R. Harper, ed. Springer London. 17–39.
[22] Alt, F., Kern, D., Schulte, F., Pfleging, B., Shirazi, A.S. and Schmidt, A. 2010. Enabling Micro-entertainment in Vehicles Based on Context Information. *Proceedings of the 2Nd International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (New York, NY, USA, 2010), 117–124.
[23] Al-Taee, M.A., Khader, O.B. and Al-Saber, N.A. 2007. Remote Monitoring of Vehicle Diagnostics and Location Using a Smart Box with Global Positioning System and General Packet Radio Service. *2007 IEEE/ACS International Conference on Computer Systems and Applications* (May 2007), 385–388.
[24] Altman, I. 1977. Privacy regulation: culturally universal or culturally specific? *Journal of Social Issues*. 33, 3 (1977), 66–84.
[25] Amiribesheli, M., Benmansour, A. and Bouchachia, A. 2015. A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*. 6, 4 (2015), 495–517.
[26] Anderson, R. 2001. Why information security is hard-an economic perspective. *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual* (2001), 358–365.
[27] Anzahl der Autos in Deutschland - PKW-Bestand bis 2018: *https://de.statista.com/statistik/daten/studie/12131/umfrage/pkw-bestand-in-deutschland/*. Accessed: 2018-12-03.
[28] Arzberger, M., Dieper, S., Dirnberger, J., Dornseifer, H., Fey, B., Frank, R., Hoppe, C., Janner, T., Kaiser, T. and Lauterborn, A. 2012. *Smart Meter Rollout: Praxisleitfaden zur Ausbringung intelligenter Zähler*. Springer-Verlag.
[29] Atzori, L., Iera, A. and Morabito, G. 2010. The internet of things: A survey. *Computer networks*. 54, 15 (2010), 2787–2805.
[30] Awad, N.F. and Krishnan, M.S. 2006. The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*. (2006), 13–28.
[31] Bader, G. and Rossi, C. 1998. Focus groups: A step-by-step guide. (1998).
[32] Bagüés, S.A., Zeidler, A., Valdivielso, C.F. and Matias, I.R. 2007. Sentry@ Home-Leveraging the smart home for privacy in pervasive computing. *International Journal of Smart Home*. 1, 2 (2007), 129–145.

[33] Balebako, R., Jung, J., Lu, W., Cranor, L.F. and Nguyen, C. 2013. Little brothers watching you: Raising awareness of data leaks on smartphones. *Proceedings of the Ninth Symposium on Usable Privacy and Security* (2013), 12.

[34] Balebako, R., Schaub, F., Adjerid, I., Acquisti, A. and Cranor, L. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. (2015), 63–74.

[35] Barcelos, V.P., Amarante, T.C., Drury, C.D. and Correia, L.H.A. 2014. Vehicle monitoring system using IEEE 802.11p device and Android application. *2014 IEEE Symposium on Computers and Communications (ISCC)* (Jun. 2014), 1–7.

[36] Bardram, E. 2005. The trouble with login: on usability and computer security in ubiquitous computing. *Personal and Ubiquitous Computing*. 9, 6 (2005), 357–367.

[37] Barkhuus, L. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2012), 367–376.

[38] Barkhuus, L. and Dey, A. 2003. Is Context-Aware Computing Taking Control away from the User? Three Levels of Interactivity Examined. *UbiComp 2003: Ubiquitous Computing* (Oct. 2003), 149–156.

[39] Barkhuus, L. and Dey, A.K. 2003. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. *Interact* (2003), 702–712.

[40] Barricelli, B.R. and Valtolina, S. 2015. Designing for End-User Development in the Internet of Things. *End-User Development*. Springer. 9–24.

[41] Beautement, A., Sasse, M.A. and Wonham, M. 2009. The compliance budget: managing security behaviour in organisations. *Proceedings of the 2008 New Security Paradigms Workshop* (2009), 47–58.

[42] Bellotti, V., Back, M., Edwards, W.K., Grinter, R.E., Henderson, A. and Lopes, C. 2002. Making sense of sensing systems: five questions for designers and researchers. *Proceedings of the SIGCHI conference on Human factors in computing systems* (2002), 415–422.

[43] Bellotti, V. and Edwards, K. 2001. Intelligibility and accountability: human considerations in context-aware systems. *Human–Computer Interaction*. 16, 2–4 (2001), 193–212.

[44] Bellotti, V. and Sellen, A. 1993. Design for privacy in ubiquitous computing environments. *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93* (1993), 77–92.

[45] Benmansour, A., Bouchachia, A. and Feham, M. 2016. Multioccupant activity recognition in pervasive smart home environments. *ACM Computing Surveys (CSUR)*. 48, 3 (2016), 34.

[46] Beresford, A.R., Rice, A., Skehin, N. and Sohan, R. 2011. MockDroid: trading privacy for application functionality on smartphones. *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications* (2011), 49–54.

[47] Berger Peter, L. and Luckmann, T. 1966. The social construction of reality: A treatise in the sociology of knowledge. *Garden City, NY: First Anchor*. (1966).

[48] Bergvall-Kåreborn, B. and Larsson, S. 2008. A case study of real-world testing. *Proceedings of the 7th International Conference on Mobile and Ubiquitous*

Multimedia - MUM '08. (2008), 113–116. DOI:https://doi.org/10.1145/1543137.1543161.

[49] Bernhaupt, R., Obrist, M., Weiss, A., Beck, E. and Tscheligi, M. 2008. Trends in the living room and beyond: results from ethnographic studies using creative and playful probing. *Computers in Entertainment (CIE)*. 6, 1 (2008), 5.

[50] Bernstein, D., Vidovic, N. and Modi, S. 2010. A Cloud PAAS for High Scale, Function, and Velocity Mobile Applications - With Reference Application as the Fully Connected Car. *2010 Fifth International Conference on Systems and Networks Communications* (Aug. 2010), 117–123.

[51] BGG - Gesetz zur Gleichstellung von Menschen mit Behinderungen: *http://www.gesetze-im-internet.de/bgg/BJNR146800002.html*. Accessed: 2018-12-20.

[52] Bizer, J. 2006. *Bundesdatenschutzgesetz*. Nomos.

[53] Bjerknes, G. and Bratteteig, T. 1995. User participation and democracy: A discussion of Scandinavian research on system development. *Scandinavian Journal of information systems*. 7, 1 (1995), 1.

[54] Blevis, E. 2007. Sustainable interaction design: invention & disposal, renewal & reuse. *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '07*. (2007), 503–512. DOI:https://doi.org/10.1145/1240624.1240705.

[55] Blumer, H. 1954. What is wrong with social theory? *American sociological review*. 19, 1 (1954), 3–10.

[56] BMW: Autobauer liefert Gericht Kundendaten für Bewegungsprofil: *http://www.manager-magazin.de/unternehmen/autoindustrie/bmw-autobauer-liefert-gericht-kundendaten-fuer-bewegungsprofil-a-1104050.html*. Accessed: 2018-12-05.

[57] Bødker, K., Kensing, F. and Simonsen, J. 2004. *Participatory IT Design: Designing for Business and Workplace Realities*. MIT Press.

[58] Boehner, K., Vertesi, J., Sengers, P. and Dourish, P. 2007. How HCI interprets the probes. *Proceedings of the SIGCHI conference on Human factors in computing systems* (2007), 1077–1086.

[59] Borodulkin, L., Ruser, H. and Trankler, H.R. 2002. 3D virtual "smart home" user interface. *2002 IEEE International Symposium on Virtual and Intelligent Measurement Systems, 2002. VIMS '02* (2002), 111–115.

[60] Bose, R., King, J., El-Zabadani, H., Pickles, S. and Helal, A. 2006. Building plug-and-play smart homes using the atlas platform. *Proceedings of the 4th International Conference on Smart Homes and Health Telematic (ICOST), Belfast, the Northern Islands* (2006).

[61] Boxer, B. et al. 2013. *What Information Do Data Brokers Have On Consumers, And How Do They Use It Before*. Senate Committee on Commerce, Science, and Transportation 113th Congress First Session.

[62] Brand, S. 1995. *How buildings learn: What happens after they're built*. Penguin.

[63] Brandeis, L. and Warren, S. 2013. *The Right to Privacy*. The Vancouver Day Press.

[64] Brandimarte, L. and Acquisti, A. 2012. The economics of privacy. *The Oxford handbook of the digital economy*. (2012), 547–571.

[65] Brandimarte, L., Acquisti, A. and Loewenstein, G. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*. 4, 3 (May 2013), 340–347. DOI:https://doi.org/10.1177/1948550612455931.

[66] Braun, V. and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative research in psychology*. 3, 2 (2006), 77–101.

[67] Breen, R.L. 2006. A practical guide to focus-group research. *Journal of Geography in Higher Education*. 30, 3 (2006), 463–475.

[68] Brich, J., Walch, M., Rietzler, M., Weber, M. and Schaub, F. 2017. Exploring End User Programming Needs in Home Automation. *ACM Trans. Comput.-Hum. Interact.* 24, 2 (Apr. 2017), 11:1–11:35. DOI:https://doi.org/10.1145/3057858.

[69] Brodie, C., Karat, C.-M., Karat, J. and Feng, J. 2005. Usable Security and Privacy: A Case Study of Developing Privacy Management Tools. *Proceedings of the 2005 Symposium on Usable Privacy and Security* (New York, NY, USA, 2005), 35–43.

[70] Brokers, D. 2014. A call for transparency and accountability. *US Federal Trade Commission*. (2014).

[71] Brush, A.J., Krumm, J. and Scott, J. 2010. Exploring end user preferences for location obfuscation, location-based services, and the value of location. *Proceedings of the 12th ACM international conference on Ubiquitous computing* (2010), 95–104.

[72] Brush, A.J., Lee, B., Mahajan, R., Agarwal, S., Saroiu, S. and Dixon, C. 2011. Home automation in the wild: challenges and opportunities. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2011), 2115–2124.

[73] BSI 2013. *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*. Bundesamt für Sicherheit in der Informationstechnik.

[74] BSI 2013. *Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* Bundesamt für Sicherheit in der Informationstechnik.

[75] BSI 2013. *Technische Richtlinie BSI TR-03109-2 Smart Meter Gateway Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls*. Bundesamt für Sicherheit in der Informationstechnik.

[76] Buchmann, E., Böhm, K., Burghardt, T. and Kessler, S. 2013. Re-identification of Smart Meter data. *Personal and ubiquitous computing*. 17, 4 (2013), 653–662.

[77] Buchner, B. 2015. Datenschutz im vernetzten Automobil. *Datenschutz und Datensicherheit-DuD*. 39, 6 (2015), 372–377.

[78] Budweg, S., Lewkowicz, M., Müller, C. and Schering, S. 2012. Fostering Social Interaction in AAL: Methodological reflections on the coupling of real household Living Lab and SmartHome approaches. *i-com Zeitschrift für interaktive und kooperative Medien*. 11, 3 (2012), 30–35.

[79] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*. 34, 3 (2010), 523–548.

[80] Bundesministerium für Verkehr und digitale Infrastruktur 2017. *Ethik-Kommission — Automatisiertes und vernetztes Fahren*. Bundesministerium für Verkehr und digitale Infrastruktur.

[81] Burkart, P. and Andersson Schwarz, J. 2014. Post-privacy and ideology. (2014).
[82] Cadwalladr, C. and Graham-Harrison, E. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*.
[83] Caine, K. and Hanania, R. 2012. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*. 20, 1 (2012), 7–15.
[84] Carroll, J., Howard, S., Vetere, F., Peck, J. and Murphy, J. 2001. Identity, power and fragmentation in cyberspace: technology appropriation by young people. *ACIS 2001 Proceedings*. (2001), 6.
[85] Carroll, J., Howard, S., Vetere, F., Peck, J. and Murphy, J. 2002. Just what do the youth of today want? Technology appropriation by young people. *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on* (2002), 1777–1785.
[86] Carsharing Drive-Now: Zeichnet BMW Bewegungsprofile auf? 2016. *https://www.faz.net/1.4351697*. Accessed: 2018-12-05.
[87] Car-Sharing-Unfall: Aufregung um angebliche Datenprofile in BMWs: *https://www.heise.de/newsticker/meldung/Car-Sharing-Unfall-Aufregung-um-angebliche-Datenprofile-in-BMWs-3277057.html*. Accessed: 2018-12-05.
[88] Castelli, N. 2013. Kontext-basiertes Heimenergiema-nagement mit Hilfe von WiFi In-. (2013).
[89] Castelli, N., Ogonowski, C., Jakobi, T., Stein, M., Stevens, G. and Wulf, V. 2017. What Happened in my Home?: An End-User Development Approach for Smart Home Data Visualization. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (2017), 853–866.
[90] Cavoukian, A. 2012. Operationalizing privacy by design: A guide to implementing strong privacy practices. *Information and Privacy Commissioner, Ontario, Canada*. (2012).
[91] Cavoukian, A. 2009. Privacy by design. *Take the Challenge. Information and Privacy Commissioner of Ontario, Canada*. (2009).
[92] Cavoukian, A. and Dix, A. 2012. *Smart Meters in Europe: Privacy by Design at its Best*. Information and Privacy Commissioner of Ontario, Canada.
[93] Cavoukian, A. and Jonas, J. 2012. *Privacy by design in the age of big data*. Information and Privacy Commissioner of Ontario, Canada.
[94] Cavoukian, A. and others 2009. Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*. (2009).
[95] Cavoukian, A., Polonetsky, J. and Wolf, C. SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*. DOI:https://doi.org/10.1007/s12394-010-0046-y.
[96] Chellappa, R.K. and Sin, R.G. 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*. 6, 2–3 (2005), 181–202.
[97] Chen, C. 2005. Top 10 unsolved information visualization problems. *IEEE Computer Graphics and Applications*. 25, 4 (Jul. 2005), 12–16. DOI:https://doi.org/10.1109/MCG.2005.91.

[98] Chen, S.Y., Fan, J.-P. and Macredie, R.D. 2006. Navigation in hypermedia learning systems: experts vs. novices. *Computers in Human Behavior*. 22, 2 (2006), 251–266.
[99] Chiasson, S., van Oorschot, P.C. and Biddle, R. 2007. Even experts deserve usable security: Design guidelines for security management systems. *SOUPS Workshop on Usable IT Security Management (USM)* (2007), 1–4.
[100] Chung, H., Iorga, M., Voas, J. and Lee, S. 2017. Alexa, Can I Trust You? *Computer*. 50, 9 (2017), 100.
[101] Clarke, R. 2009. Privacy impact assessment: Its origins and development. *Computer law & security review*. 25, 2 (2009), 123–135.
[102] Clastres, C. 2011. Smart grids: Another step towards competition, energy security and climate change objectives. *Energy Policy*. 39, 9 (2011), 5399–5408.
[103] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses: 2012. *http://europa.eu/rapid/press-release_IP-12-46_en.htm*. Accessed: 2019-03-10.
[104] Common Criteria Implementation Board 2012. Common Criteria for Information Technology Security Evaluation, v3.1 Revision 4.
[105] Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P. 2005. Location disclosure to social relations: why, when, & what people want to share. *Proceedings of the SIGCHI conference on Human factors in computing systems* (2005), 81–90.
[106] Cook, D.J., Youngblood, G.M., Heierman III, E.O., Gopalratnam, K., Rao, S., Litvin, A. and Khawaja, F. 2003. MavHome: An Agent-Based Smart Home. *PerCom* (2003), 521–524.
[107] Coronado, P.D.U., Sundaresan, V.B. and Ahuett-Garza, H. 2013. Design of an android based input device for electric vehicles. *2013 International Conference on Connected Vehicles and Expo (ICCVE)* (Dec. 2013), 736–740.
[108] Costa, R., Carneiro, D., Novais, P., Lima, L., Machado, J., Marques, A. and Neves, J. 2009. Ambient assisted living. *3rd Symposium of Ubiquitous Computing and Ambient Intelligence 2008* (2009), 86–94.
[109] Courtney, K.L. 2008. Privacy and senior willingness to adopt smart home information technology in residential care facilities. (2008).
[110] Coyne, I.T. 1997. Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of advanced nursing*. 26, 3 (1997), 623–630.
[111] Crabtree, A. 2004. Design in the absence of practice: breaching experiments. *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*. (2004), 59–68.
[112] Crabtree, A. 1998. Ethnography in Participatory Design. *Proceedings of the 1998 Participatory design Conference*. (1998), 93–105.
[113] Crabtree, A., Hemmings, T., Rodden, T. and Mariani, J. 2003. Informing the development of calendar systems for domestic use. *ECSCW 2003* (2003), 119–138.
[114] Crabtree, A. and Mortier, R. 2015. Human Data Interaction: Historical Lessons from Social Studies and CSCW. *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway*. Springer, Cham. 3–21.

[115] Crabtree, A. and Rodden, T. 2004. Domestic routines and design for the home. *Computer Supported Cooperative Work (CSCW)*. 13, 2 (2004), 191–220.
[116] Crabtree, A., Rodden, T., Tolmie, P., Mortier, R., Lodge, T., Brundell, P. and Pantidi, N. 2015. House rules: the collaborative nature of policy in domestic networks. *Personal and Ubiquitous Computing*. 19, 1 (2015), 203–215.
[117] Crabtree, A., Tolmie, P. and Knight, W. 2017. Repacking 'Privacy' for a Networked World. *Computer Supported Cooperative Work (CSCW)*. 26, 4–6 (Dec. 2017), 453–488. DOI:https://doi.org/10.1007/s10606-017-9276-y.
[118] Craig Timberg and Elizabeth Dwoskin 2018. A voter profiling firm hired by Trump likely grabbed data for tens of millions of Facebook users. *Washington Post*.
[119] Cranor, L.F. 2005. *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc.
[120] Cranor, L.F., Reagle, J. and Ackerman, M.S. 1999. Beyond concern: Understanding net users' attitudes about online privacy. *arXiv preprint cs/9904010*. (1999).
[121] Cuijpers, C. and Koops, B.-J. 2013. Smart metering and privacy in Europe: lessons from the Dutch case. *European data protection: coming of age*. Springer. 269–293.
[122] Dachtera, J., Randall, D. and Wulf, V. 2014. Research on Research: Design Research at the Margins: Academia, Industry and End-users. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2014), 713–722.
[123] Danezis, G. and Gürses, S. 2010. A critical review of 10 years of privacy technology. *Proceedings of Surveillance Cultures: A Global Surveillance Society*. (2010).
[124] Darby, S. 2006. *The effectiveness of feedback on energy consumption. A Review for DEFRA of the Literature on Metering, Billing and Direct Displays*. Environmental Change Institute, University of Oxford.
[125] Data is not the new oil: 2018. *http://social.techcrunch.com/2018/03/27/data-is-not-the-new-oil/*. Accessed: 2018-12-05.
[126] Davidoff, S., Lee, M.K., Yiu, C., Zimmerman, J. and Dey, A.K. 2006. Principles of smart home control. *International Conference on Ubiquitous Computing* (2006), 19–34.
[127] Davidoff, S., Zimmerman, J. and Dey, A.K. 2010. How routine learners can support family coordination. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), 2461–2470.
[128] De Russis, L. and Corno, F. 2015. HomeRules: A Tangible End-User Programming Interface for Smart Homes. (2015), 2109–2114.
[129] Demiris, G., Rantz, M.J., Aud, M.A., Marek, K.D., Tyrer, H.W., Skubic, M. and Hussam, A.A. 2004. Older adults' attitudes towards and perceptions of 'smart home'technologies: a pilot study. *Medical informatics and the Internet in medicine*. 29, 2 (2004), 87–94.
[130] Deterding, S. 2011. Gamification : Toward a Definition. (2011), 12–15.
[131] Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE 2010. *Die deutsche Normungsroadmap E-Energy - Smart Grid*.

[132] Dey, A.K., Sohn, T., Streng, S. and Kodama, J. 2006. iCAP: Interactive Prototyping of Context-Aware Applications. *Pervasive Computing*. K.P. Fishkin, B. Schiele, P. Nixon, and A. Quigley, eds. Springer Berlin Heidelberg. 254–271.

[133] Dienlin, T. and Trepte, S. 2014. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*. (2014).

[134] Dinev, T. and Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*. 17, 1 (2006), 61–80.

[135] Dix, A. 2007. Designing for appropriation. *Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI... but not as we know it-Volume 2* (2007), 27–30.

[136] Dixon, C., Mahajan, R., Agarwal, S., Brush, A.J., Lee, B., Saroiu, S. and Bahl, V. 2010. The home needs an operating system (and an app store). *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks* (2010), 18.

[137] Döbelt, S., Jung, M., Busch, M. and Tscheligi, M. 2015. Consumers' privacy concerns and implications for a privacy preserving Smart Grid architecture—Results of an Austrian study. *Energy Research & Social Science*. 9, (2015), 137–145.

[138] Dorner, M. 2014. Big Data und „Dateneigentum". *Computer Und Recht*. 30, 9 (2014), 617–628.

[139] Dourish, P. 1997. Accounting for system behaviour: Representation, reflection and resourceful action. *Computers and Design in Context, MIT Press, Cambridge, MA, USA*. (1997), 145–170.

[140] Dourish, P. 2003. The appropriation of interactive technologies: Some lessons from placeless documents. *Computer Supported Cooperative Work (CSCW)*. 12, 4 (2003), 465–490.

[141] Draxler, S. and Stevens, G. 2011. Supporting the collaborative appropriation of an open software ecosystem. *Computer Supported Cooperative Work (CSCW)*. 20, 4–5 (2011), 403–448.

[142] Draxler, S., Stevens, G. and Boden, A. 2014. Keeping the Development Environment Up to Date—A Study of the Situated Practices of Appropriating the Eclipse IDE. *IEEE Transactions on Software Engineering*. 40, 11 (2014), 1061–1074.

[143] Dubois, E. and Ford, H. 2015. Qualitative political communication| trace interviews: An actor-centered approach. *International Journal of Communication*. 9, (2015), 25.

[144] Duckham, M. and Kulik, L. 2005. A formal model of obfuscation and negotiation for location privacy. *International conference on pervasive computing* (2005), 152–170.

[145] Dwyer, C., Hiltz, S. and Passerini, K. 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*. (2007), 339.

[146] Eckert, C. and Krauß, C. 2011. Sicherheit im Smart Grid. *Datenschutz und Datensicherheit-DuD*. 35, 8 (2011), 535–541.

[147] Edwards, W.K. and Grinter, R.E. 2001. At home with ubiquitous computing: Seven challenges. *Ubicomp 2001: Ubiquitous Computing* (2001), 256–272.

[148] Efthymiou, C. and Kalogridis, G. 2010. Smart grid privacy via anonymization of smart metering data. *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* (2010), 238–243.
[149] Egelman, S., Felt, A.P. and Wagner, D. 2013. Choice architecture and smartphone privacy: There'sa price for that. *The Economics of Information Security and Privacy*. Springer. 211–236.
[150] Eggen, B., Hollemans, G. and van de Sluis, R. 2003. Exploring and enhancing the home experience. *Cognition, Technology & Work*. 5, 1 (2003), 44–54.
[151] Eloff, M.M. and von Solms, S.H. 2000. Information security management: a hierarchical framework for various approaches. *Computers & Security*. 19, 3 (2000), 243–256.
[152] Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L.P., Jung, J., McDaniel, P. and Sheth, A.N. 2014. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*. 32, 2 (2014), 5.
[153] Epstein, D., Cordeiro, F., Bales, E., Fogarty, J. and Munson, S. 2014. Taming data complexity in lifelogs: exploring visual cuts of personal informatics data. *Proceedings of the 2014 conference on Designing interactive systems* (2014), 667–676.
[154] Epstein, D.A., Ping, A., Fogarty, J. and Munson, S.A. 2015. A lived informatics model of personal informatics. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2015), 731–742.
[155] Erickson, T., Podlaseck, M. and Sahu, S. 2012. The dubuque water portal: evaluation of the uptake, use and impact of residential water consumption feedback. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. (2012), 675–684.
[156] Ericsson, K.A. and Simon, H.A. 1980. Verbal reports as data. Psychological Review, Vol. 87, no. 3. (1980), 215–251.
[157] Eriksson, M., Niitamo, V.-P. and Kulkki, S. 2005. *State-of-the-art in utilizing Living Labs approach to user- centric ICT innovation - a European approach.* Lulea University of Technology, Sweden.
[158] Erkin, Z. and Tsudik, G. 2012. Private computation of spatial and temporal power consumption with smart meters. *Applied Cryptography and Network Security* (2012), 561–577.
[159] European Commission 2014. *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*. Technical Report #52014SC0188.
[160] European Commission 2009. *Living Labs for user-driven open innovation*. European Commission.
[161] European Data Protection Supervisor 2016. *Executive Summary of the Opinion of the European Data Protection Supervisor on 'Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability.'*
[162] European Parliament and of the Council 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.

[163] European Parliament and of the Council 2014. *On the deployment of the interoperable EU-wide eCall service*.

[164] European Parliament and the Council 2016. *REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

[165] European Parliament and Council of the European Union 1995. *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

[166] European Parliament of the Council 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Official Journal of the European Union L 119/2016*. Volume 59, L119 (May 2016).

[167] Fahrleistung auf Autobahnen | Deutschland: *https://de.statista.com/statistik/daten/studie/155732/umfrage/fahrleistung-auf-autobahnen-in-deutschland/*. Accessed: 2018-12-03.

[168] Fang, X., Misra, S., Xue, G. and Yang, D. 2012. Smart grid—The new and improved power grid: A survey. *Communications Surveys & Tutorials, IEEE*. 14, 4 (2012), 944–980.

[169] Farhangi, H. 2010. The path of the smart grid. *Power and Energy Magazine, IEEE*. 8, 1 (2010), 18–28.

[170] Federal Office for Information Security 2014. *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*. Technical Report #Version 1.3.

[171] Federal Office for Information Security 2013. *Technische Richtlinie BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*. Technical Report #Version1.0.

[172] Felt, A.P., Egelman, S., Finifter, M., Akhawe, D. and Wagner, D. 2012. How to Ask for Permission. *HotSec* (2012).

[173] Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D. 2012. Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (2012), 3.

[174] Few, S. 2006. *Information Dashboard Design: The Effective Visual Communication of Data*. O'Reilly Media.

[175] Feyerabend, P. 1975. Against method: Outline of an anarchistic theory of knowledge. Atlantic Highlands. *Ferroni, F.,(2012,) Occhi indiscreti sul neutrino, Il Sole*. 24, (1975).

[176] Fezer, K.-H. 2017. Dateneigentum. Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten. *MultiMedia und Recht*. 18, 1 (2017), 3–5.

[177] Fischer, G. and Giaccardi, E. 2006. Meta-design: A framework for the future of end-user development. *End user development*. Springer. 427–457.

[178] Fischer, J.E., Crabtree, A., Rodden, T., Colley, J.A., Costanza, E., Jewell, M.O. and Ramchurn, S.D. 2016. "Just whack it on until it gets hot": working with IoT data in the home. *CHI 2016* (2016).

[179] Fischer, J.E., Ramchurn, S.D., Osborne, M., Parson, O., Huynh, T.D., Alam, M., Pantidi, N., Moran, S., Bachour, K., Reece, S. and others 2013. Recommending energy tariffs and load shifting based on smart household usage profiling. *Proceedings of the 2013 international conference on Intelligent user interfaces* (2013), 383–394.

[180] Fischer-Hübner, S., Iacono, L.L. and Möller, S. 2010. Usable security und privacy. *Datenschutz und Datensicherheit-DuD*. 34, 11 (2010), 773–782.

[181] Flick, T. and Morehouse, J. 2010. *Securing the smart grid: next generation power grid security*. Elsevier.

[182] Floridi, L. 2005. The ontological interpretation of informational privacy. *Ethics and Information Technology*. 7, 4 (2005), 185–200.

[183] Fogel, J. and Nehmad, E. 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior*. 25, 1 (2009), 153–160.

[184] Fogg, B.J. and Tseng, H. 1999. The Elements of Computer Credibility. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 1999), 80–87.

[185] Følstad, A. 2008. Living labs for innovation and development of information and communication technology: a literature review. *The Electronic Journal for Virtual Organizations and Networks*. 10, 7 (2008), 99–131.

[186] Fox, D. 2010. Smart meter. *Datenschutz und Datensicherheit-DuD*. 34, 6 (2010), 408–408.

[187] Fox, D. and Müller, K.J. 2011. Viele Daten um Nichts. *Datenschutz und Datensicherheit - DuD*. 35, 8 (Aug. 2011), 515–516. DOI:https://doi.org/10.1007/s11623-011-0127-6.

[188] Froehlich, J., Findlater, L., Landay, J. and Science, C. 2010. The design of eco-feedback technology. *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10* (New York, New York, USA, 2010), 1999–2008.

[189] Garfinkel, H. 1967. *Studies in ethnomethodology*. Englewood Cliffs NJ.

[190] Garfinkel, S. 2005. *Design principles and patterns for computer systems that are simultaneously secure and usable*. Massachusetts Institute of Technology.

[191] Gärtner, J. and Wagner, I. 1996. Mapping Actors and Agendas: Political Frameworks of Systems Design and Participation. *Hum.-Comput. Interact.* 11, 3 (Sep. 1996), 187–214. DOI:https://doi.org/10.1207/s15327051hci1103_1.

[192] Gates, C. and Matthews, P. 2014. Data Is the New Currency. *Proceedings of the 2014 New Security Paradigms Workshop* (New York, NY, USA, 2014), 105–116.

[193] Gaver, B., Dunne, T. and Pacenti, E. 1999. Design: Cultural probes. *Interactions*. 6, (1999), 21–29. DOI:https://doi.org/10.1145/291224.291235.

[194] Gaver, W. 2012. What should we expect from research through design? *Proceedings of the SIGCHI conference on human factors in computing systems* (2012), 937–946.

[195] Gaver, W.W. 2006. The video window: my life with a ludic system. *Personal and Ubiquitous Computing*. 10, 2–3 (2006), 60–65.
[196] Gedik, B. and Liu, L. 2008. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*. 7, 1 (2008), 1–18.
[197] Gellings, C.W. 2009. *The Smart Grid: Enabling Energy Efficiency and Demand Response*. The Fairmont Press, Inc.
[198] Gerber, P., Volkamer, M. and Renaud, K. 2015. Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *ACM SIGCAS Computers and Society*. 45, 1 (2015), 16–21.
[199] Gerhager, S. 2012. Informationssicherheit im zukünftigen Smart Grid. *Datenschutz und Datensicherheit-DuD*. 36, 6 (2012), 445–451.
[200] Gerla, M., Lee, E.K., Pau, G. and Lee, U. 2014. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. *2014 IEEE World Forum on Internet of Things (WF-IoT)* (Mar. 2014), 241–246.
[201] German Federal Constitutional Court 1983. *BVerfGE 65, 1 - Census*.
[202] Gigerenzer, G. and Goldstein, D.G. 1996. Reasoning the fast and frugal way: models of bounded rationality. *Psychological review*. 103, 4 (1996), 650.
[203] Gkikas, N. 2012. *Automotive Ergonomics: Driver-Vehicle Interaction*. CRC Press.
[204] Glaser, B.G. 1998. *Doing grounded theory: Issues and discussions*. Sociology Press Mill Valley, CA.
[205] Glaser, B.G. and Strauss, A.L. 2009. *The discovery of grounded theory: Strategies for qualitative research*. Transaction Publishers.
[206] Goel, S., Hong, Y., Papakonstantinou, V. and Kloza, D. 2015. *Smart Grid Security*. Springer.
[207] Goffman, E. 1955. On face-work: An analysis of ritual elements in social interaction. *Psychiatry*. 18, 3 (1955), 213–231.
[208] Goodwin, N.C. 1987. Functionality and Usability. *Commun. ACM*. 30, 3 (Mar. 1987), 229–233. DOI:https://doi.org/10.1145/214748.214758.
[209] Gould, R. 2017. Data literacy is statistical literacy. *Statistics Education Research Journal*. 16, 1 (2017), 22–25.
[210] Green, P. 2004. *Driver distraction, telematics design, and workload managers: Safety issues and solutions*. Society of Automotive Engineers Warrendale, PA.
[211] Greveler, U. 2016. *Smart Grid: Chancen und Risiken für Verbraucher*. DEU.
[212] Grimm, P. 2010. Social desirability bias. *Wiley international encyclopedia of marketing*. (2010).
[213] Grinter, R.E., Edwards, W.K., Newman, M.W. and Ducheneaut, N. 2005. The work to make a home network work. *ECSCW 2005* (2005), 469–488.
[214] Grinter, R.E., Greenhalgh, C., Benford, S., Edwards, W.K., Chetty, M., Poole, E.S., Sung, J.-Y., Yang, J., Crabtree, A., Tolmie, P. and Rodden, T. 2009. The ins and outs of home networking. *ACM Transactions on Computer-Human Interaction*. 16, 2 (Jun. 2009), 1–28. DOI:https://doi.org/10.1145/1534903.1534905.
[215] Gross, R. and Acquisti, A. 2005. Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (2005), 71–80.

[216] Grützmacher, M. 2016. Dateneigentum-ein Flickenteppich. *Computer Und Recht*. 32, 8 (2016), 485.
[217] Gummer, E. and Mandinach, E. 2015. Building a Conceptual Framework for Data Literacy. *Teachers College Record*. 117, 4 (2015), n4.
[218] Gürses, S.F., Troncoso, C. and Diaz, C. 2011. Engineering Privacy by Design. *Computers, Privacy & Data Protection*. (2011), 25 pages.
[219] Guthridge, G.S. *Understanding consumer preferences in energy efficiency: Accenture end-consumer observatory on electricity management.* Technical Report #ACC10-0229. Accenture.
[220] Häberle, T., Charissis, L., Fehling, C., Nahm, J. and Leymann, F. 2015. The Connected Car in the Cloud: A Platform for Prototyping Telematics Services. *IEEE Software*. 32, 6 (Nov. 2015), 11–17. DOI:https://doi.org/10.1109/MS.2015.137.
[221] Haddadi, H., Howard, H., Chaudhry, A., Crowcroft, J., Madhavapeddy, A. and Mortier, R. 2015. Personal data: thinking inside the box. *arXiv preprint arXiv:1501.04737*. (2015).
[222] Ham, J. and Midden, C. 2010. Ambient persuasive technology needs little cognitive effort: the differential effects of cognitive load on lighting feedback versus factual feedback. *Persuasive Technology*. (2010), 132–142.
[223] Hann, I.-H., Hui, K.-L., Lee, T. and Png, I. 2002. Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 Proceedings*. (2002), 1.
[224] Hansen, M. 2015. Das Netz im Auto & das Auto im Netz. *Datenschutz und Datensicherheit-DuD*. 39, 6 (2015), 367–371.
[225] Harper, R. 2006. *Inside the smart home*. Springer Science & Business Media.
[226] Harper, R. ed. 2011. *The Connected Home: The Future of Domestic Life*. Springer London.
[227] Harper, R., Randall, D. and Sharrock, W. 2016. *Choice*. John Wiley & Sons.
[228] Harper, R.H. 2014. *Trust, computing, and society*. Cambridge University Press.
[229] Harrison, S. and Dourish, P. 1996. Re-place-ing space: the roles of place and space in collaborative systems. *Proceedings of the 1996 ACM conference on Computer supported cooperative work* (1996), 67–76.
[230] Hart, G.W. 1992. Nonintrusive appliance load monitoring. *Proceedings of the IEEE*. 80, 12 (1992), 1870–1891.
[231] Hashem, T. and Kulik, L. 2011. "Don't trust anyone": Privacy protection for location-based services. *Pervasive and Mobile Computing*. 7, 1 (2011), 44–59.
[232] Hayes, G.R. 2011. The relationship of action research to human-computer interaction. *ACM Transactions on Computer-Human Interaction*. 18, (2011), 1–20. DOI:https://doi.org/10.1145/1993060.1993065.
[233] Heller, C. 2011. *Post-privacy: prima leben ohne Privatsphäre*. CH Beck.
[234] Hemker, T. and Mischkovsky, O. 2017. Erforderliche Schutzma\s snahmen für das (vernetzte) Auto. *Datenschutz und Datensicherheit-DuD*. 41, 4 (2017), 233–238.
[235] Henkemans, O.B., Caine, K.E., Rogers, W.A., Fisk, A.D. and Neerincx, M.A. 2007. Medical monitoring for independent living: user-centered design of smart home technologies for older adults. *Proc. Med-e-Tel Conf. eHealth, Telemedicine and Health Information and Communication Technologies* (2007), 18–20.

[236] Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 workshop on New security paradigms workshop* (2009), 133–144.
[237] Hess, J., Ley, B., Ogonowski, C., Wan, L. and Wulf, V. 2011. Jumping Between Devices and Services: Towards an Integrated Concept for Social Tv. *Proceedings of the 9th European Conference on Interactive TV and Video* (New York, NY, USA, 2011), 11–20.
[238] Hess, J., Ley, B., Ogonowski, C., Wan, L. and Wulf, V. 2012. Understanding and supporting cross-platform usage in the living room. *Entertainment Computing*. (2012).
[239] Hildreth, G. 1930. The child in America: Behavior problems and programs. (1930).
[240] Himma, K.E. and Tavani, H.T. 2008. *The handbook of information and computer ethics*. John Wiley & Sons.
[241] Hoerbst, A., Kohl, C.D., Knaup, P. and Ammenwerth, E. 2010. Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens. *International Journal of Medical Informatics*. 79, 2 (Feb. 2010), 81–89. DOI:https://doi.org/10.1016/j.ijmedinf.2009.11.002.
[242] Holstein, J.A. and Gubrium, J.F. 1997. Active interviewing. *Qualitative research: Theory, method and practice*. (1997), 113–129.
[243] Hong, J.I., Ng, J.D., Lederer, S. and Landay, J.A. 2004. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques* (2004), 91–100.
[244] Hornung, D., Müller, C., Shklovski, I., Jakobi, T. and Wulf, V. 2017. Navigating relationships and boundaries: concerns around ICT-uptake for elderly people. (2017), 7057–7069.
[245] Hornung, G. and Fuchs, K. 2012. Nutzerdaten im Smart Grid—zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung. *Datenschutz und Datensicherheit-DuD*. 36, 1 (2012), 20–25.
[246] Houben, S., Golsteijn, C., Gallacher, S., Johnson, R., Bakker, S., Marquardt, N., Capra, L. and Rogers, Y. 2016. Physikit: Data engagement through physical ambient visualizations in the home. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), 1608–1619.
[247] Hurlburt, G.F., Voas, J. and Miller, K.W. 2012. The internet of things: A reality check. *IT Professional*. 14, 3 (2012), 56–59.
[248] Iachello, G., Hong, J. and others 2007. End-user privacy in human–computer interaction. *Foundations and Trends® in Human–Computer Interaction*. 1, 1 (2007), 1–137.
[249] Intille, S.S. 2002. Designing a home of the future. *IEEE pervasive computing*. 1, 2 (2002), 76–82.
[250] Intille, S.S., Larson, K., Beaudin, J.S., Nawyn, J., Tapia, E.M. and Kaushik, P. 2005. A living laboratory for the design and evaluation of ubiquitous computing technologies. *Extended abstracts of the SIGCHI Conference on Human Factors in Computing Systems - CHI '05* (New York, USA, Apr. 2005), 1941–1944.
[251] ISO/IEC JTC 1/SC 27 IT Security techniques 2018. International Standard ISO/IEC 27000 5th edition. ISO.

[252] Ivanecký, J., Mehlhase, S. and Mieskes, M. 2011. An intelligent house control using speech recognition with integrated localization. *Ambient Assisted Living*. (2011).

[253] Jaferian, P., Botta, D., Raja, F., Hawkey, K. and Beznosov, K. 2008. Guidelines for designing IT security management tools. *Proceedings of the 2nd ACM Symposium on Computer Human interaction For Management of information Technology* (2008), 7.

[254] Jakkula, V. and Cook, D.J. 2007. Learning temporal relations in smart home data. *Proceedings of the second International Conference on Technology and Aging* (2007).

[255] Jakobi, T. 2013. Always Beta : Cooperative Design in the Smart Home. (2013).

[256] Jakobi, T. 2012. Integrierte Heim Energie Monitoringsysteme (HEMS) für iTV: Eine LivingLab basierte Design-Fallstudie. (2012).

[257] Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G. and Wulf, V. 2016. Smart Home Experience Journey: Über den Einsatz und die Wahrnehmung von Smart Home-Technologien im Alltag. *WISSENSCHAFT TRIFFT PRAXIS*. (2016), 12.

[258] Jakobi, T., Ogonowski, C., Castelli, N., Stevens, G. and Wulf, V. 2017. The catch (es) with smart home: Experiences of a living lab field study. (2017), 1620–1633.

[259] Jakobi, T. and Schwartz, T. 2012. Putting the user in charge: end user development for eco-feedback technologies. (2012), 1–4.

[260] Jakobi, T. and Schwartz, T. 2012. Putting the user in charge: End user development for eco-feedback technologies. *Sustainable Internet and ICT for Sustainability (SustainIT), 2012* (2012), 1–4.

[261] Jakobi, T. and Stevens, G. 2015. Energy saving at work - and when not working! Insights from a comparative study. *EnviroInfo and ICT for Sustainability 2015*. (2015).

[262] Jakobi, T., Stevens, G., Castelli, N., Ogonowski, C., Schaub, F., Vindice, N., Randall, D., Tolmie, P. and Wulf, V. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2, 4 (Dec. 2018), 28. DOI:https://doi.org/10.1145/3287049.

[263] Jakobi, T., Stevens, G., Castelli, N., Ogonowski, C., Vindice, N., Randall, D., Tolmie, P. and Wulf, V. 2018. Evolving Needs in IoT Control and Accountability: A Longitudinal Study on Smart Home Intelligibility. *ACM J. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4 (Dec. 2018), 28. DOI:https://doi.org/10.1145/3287049.

[264] Jakobi, T., Stevens, G. and Schwartz, T. 2011. EUD@ Smart Homes-Smart Refurbishment of Rented Apartments to Improve Energy Efficiency. (2011).

[265] Jakobi, T., Stevens, G. and Schwartz, T. 2014. Verhaltensbasiertes Energiesparen am Arbeitsplatz: Ergebnisse einer vergleichenden Studie. (2014), 76–88.

[266] Jara, A.J., Zamora, M. a. and Skarmeta, A.F.G. 2011. An internet of things–based personal device for diabetes therapy management in ambient assisted living (AAL). *Personal and Ubiquitous Computing*. 15, 4 (Jan. 2011), 431–440. DOI:https://doi.org/10.1007/s00779-010-0353-1.

[267] Jeske, T. 2011. Datenschutzfreundliches smart metering. *Datenschutz und Datensicherheit-DuD*. 35, 8 (2011), 530–534.
[268] Johnson, D.G. 2009. *Computer Ethics*. Prentice Hall Press.
[269] Jones, H. and Soltren, J.H. 2005. Facebook: Threats to privacy. *Project MAC: MIT Project on Mathematics and Computing*. 1, (2005), 1–76.
[270] Joukes, E., Cornet, R., de Bruijne, M.C. and de Keizer, N.F. 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, (Mar. 2016), 111–117. DOI:https://doi.org/10.1016/j.ijmedinf.2015.12.014.
[271] Kalogridis, G., Efthymiou, C., Denic, S.Z., Lewis, T.A. and Cepeda, R. 2010. Privacy for smart meters: Towards undetectable appliance load signatures. *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* (2010), 232–237.
[272] Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (2015), 39–52.
[273] Kappel, K. and Grechenig, T. 2009. Show-me: water consumption at a glance to promote water conservation in the shower. *Proceedings of the 4th international conference on persuasive technology*. (2009).
[274] Karg, M. 2010. Datenschutzrechtliche Rahmenbedingungen beim Einsatz intelligenter Zähler. *Datenschutz und Datensicherheit-DuD*. 34, 6 (2010), 365–372.
[275] van Kasteren, T., Noulas, A., Englebienne, G. and Kröse, B. 2008. Accurate Activity Recognition in a Home Setting. (2008).
[276] Kawsar, F., Nakajima, T. and Fujinami, K. 2008. Deploy spontaneously: supporting end-users in building and enhancing a smart home. *Proceedings of the 10th international conference on Ubiquitous computing* (2008), 282–291.
[277] Kelley, P.G., Bresee, J., Cranor, L.F. and Reeder, R.W. 2009. A nutrition label for privacy. *Proceedings of the 5th Symposium on Usable Privacy and Security* (2009), 4.
[278] Kelley, P.G., Cesca, L., Bresee, J. and Cranor, L.F. 2010. Standardizing privacy notices: an online study of the nutrition label approach. *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* (2010), 1573–1582.
[279] Kelly, D., Raines, R., Baldwin, R., Grimaila, M. and Mullins, B. 2011. Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics. *Communications Surveys & Tutorials, IEEE*. 99 (2011), 1–28.
[280] Kempton, W. and Montgomery, L. 1982. Folk quantification of energy. *Energy*. 7, 10 (Oct. 1982), 817–827. DOI:https://doi.org/10.1016/0360-5442(82)90030-5.
[281] Kensing, F. and Blomberg, J. 1998. Participatory design: Issues and concerns. *Computer Supported Cooperative Work (CSCW)*. 1993 (1998), 167–185.
[282] Kerkmann, F. 2013. Web Accessibility. *Informatik-Spektrum*. 36, 5 (Oct. 2013), 455–460. DOI:https://doi.org/10.1007/s00287-013-0724-x.

[283] Kern, D. and Schmidt, A. 2009. Design Space for Driver-based Automotive User Interfaces. *Proceedings of the 1st International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (New York, NY, USA, 2009), 3–10.

[284] Kientz, J.A., Patel, S.N., Jones, B., Price, E.D., Mynatt, E.D. and Abowd, G.D. 2008. The georgia tech aware home. *CHI'08 extended abstracts on Human factors in computing systems* (2008), 3675–3680.

[285] Kim, J.E., Boulos, G., Yackovich, J., Barth, T., Beckel, C. and Mosse, D. 2012. Seamless integration of heterogeneous devices and access control in smart homes. *Intelligent Environments (IE), 2012 8th International Conference on* (2012), 206–213.

[286] Kiometzis, M. and Ullmann, M. 2017. Fahrdaten für alle? *Datenschutz und Datensicherheit-DuD*. 41, 4 (2017), 227–232.

[287] Kirmse, A. 2012. Privacy in Smart Homes. *ComSys Seminar: Advanced Internet Technology SS2012*. (2012).

[288] Kitzinger, J. 1994. The methodology of focus groups: the importance of interaction between research participants. *Sociology of health & illness*. 16, 1 (1994), 103–121.

[289] Kleemann, A. 2012. *Rahmenbedingungen für Smart Metering in Deutschland*. Bundesministerium für Wirtschaft und Technologie.

[290] Knijnenburg, B.P. 2013. Simplifying Privacy Decisions: Towards Interactive and Adaptive Solutions. *Decisions@ RecSys* (2013), 40–41.

[291] Knijnenburg, B.P. and Kobsa, A. 2013. Helping users with information disclosure decisions: potential for adaptation. *Proceedings of the 2013 international conference on Intelligent user interfaces* (2013), 407–416.

[292] Knyrim, R. and Trieb, G. 2011. Smart metering under EU data protection law. *International Data Privacy Law*. 1, 2 (2011), 121–128.

[293] Kobsa, A. and Teltzrow, M. 2004. Contextualized communication of privacy practices and personalization benefits: Impacts on users' data sharing and purchase behavior. *Privacy Enhancing Technologies* (2004), 329–343.

[294] Koltay, T. 2017. Data literacy for researchers and data librarians. *Journal of Librarianship and Information Science*. 49, 1 (2017), 3–14.

[295] Koltay, T. 2015. Data literacy: in search of a name and identity. *Journal of Documentation*. 71, 2 (2015), 401–415.

[296] Koskela, T. and Väänänen-Vainio-Mattila, K. 2004. Evolution towards smart home environments: empirical evaluation of three user interfaces. *Personal and Ubiquitous Computing*. 8, 3–4 (2004), 234–240.

[297] Kotulic, A.G. and Clark, J.G. 2004. Why there aren't more information security research studies. *Information & Management*. 41, 5 (2004), 597–607.

[298] Kranz, L.M., Gallenkamp, J. and Picot, A. 2010. Exploring the Role of Control – Smart Meter Acceptance of Residential Consumers. *AMCIS 2010 Proceedings*. (Aug. 2010).

[299] Kranz, M., Franz, A., Röckl, M., Andreas, L. and Strang, T. 2008. CODAR Viewer - A Situation-Aware Driver Assistance System. *Sixth International Conference on Pervasive Computing* (Sydney, Australia, Feb. 2008), 126–129.

[300] Kranz, M., Holleis, P. and Schmidt, A. 2010. Embedded Interaction: Interacting with the Internet of Things. *Internet Computing, IEEE*. 14, 2 (2010), 46–53.
[301] Kranz, M., Röckl, M., Franz, A. and Strang, T. 2008. CODAR Viewer - A V2V Communication Awareness Display. *Sixth International Conference on Pervasive Computing* (Sydney, Australia, Feb. 2008), 79–82.
[302] Krauß, C. and Waidner, M. 2015. IT-Sicherheit und Datenschutz im vernetzten Fahrzeug. *Datenschutz und Datensicherheit-DuD*. 39, 6 (2015), 383–387.
[303] Krishnamurti, T., Schwartz, D., Davis, A., Fischhoff, B., de Bruin, W.B., Lave, L. and Wang, J. 2012. Preparing for smart grid technologies: A behavioral decision research approach to understanding consumer expectations about smart meters. *Energy Policy*. 41, (2012), 790–797.
[304] Kroll-Peters, O. 2010. *Evaluationsmethoden für benutzerzentrierte IT-Sicherheit*. Berlin Institute of Technology.
[305] Krumm, J. 2009. A survey of computational location privacy. *Personal and Ubiquitous Computing*. 13, 6 (2009), 391–399.
[306] Kubitza, T., Voit, A., Weber, D. and Schmidt, A. 2016. An IoT Infrastructure for Ubiquitous Notifications in Intelligent Living Environments. *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (New York, NY, USA, 2016), 1536–1541.
[307] Kuutti, K. 1996. Activity theory as a potential framework for human-computer interaction research. *Context and consciousness: Activity theory and human-computer interaction*. (1996), 17–44.
[308] Kuutti, K. and Bannon, L.J. 2014. The Turn to Practice in HCI: Towards a Research Agenda. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2014), 3543–3552.
[309] Lahlou, S., Langheinrich, M. and Röcker, C. 2005. Privacy and trust issues with invisible computers. *Communications of the ACM*. 48, 3 (Mar. 2005), 59. DOI:https://doi.org/10.1145/1047671.1047705.
[310] Langford, J. and McDonagh, D. eds. 2003. *Focus groups*.
[311] Langheinrich, M. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. *Ubicomp 2001: Ubiquitous Computing*. (2001).
[312] Lapoehn, S., Schieben, A., Hesse, T., Schindler, J. and Köster, F. 2014. Usage of Nomadic Devices in Highly-Automated Vehicles.
[313] Laudatio BigBrother Award 2008 in der Kategorie "Technik": 2008. *http://www.bigbrotherawards.de/2008/.tec?set_language=de*. Accessed: 2014-03-10.
[314] Laupichler, D., Vollmer, S., Bast, H. and Intemann, M. 2011. Das BSI-Schutzprofil: Anforderungen an den Datenschutz und die Datensicherheit für Smart Metering Systeme. *Datenschutz und Datensicherheit-DuD*. 35, 8 (2011), 542–546.
[315] Lederer, A.L., Maupin, D.J., Sena, M.P. and Zhuang, Y. 2000. The technology acceptance model and the World Wide Web. *Decision Support Systems*. 29, 3 (Oct. 2000), 269–282. DOI:https://doi.org/10.1016/S0167-9236(00)00076-2.
[316] Lederer, S., Hong, J.I., Dey, A.K. and Landay, J.A. 2004. Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing*. 8, 6 (2004), 440–454.

[317] Lederer, S., Mankoff, J. and Dey, A.K. 2003. Who wants to know what when? privacy preference determinants in ubiquitous computing. *CHI'03 extended abstracts on Human factors in computing systems* (2003), 724–725.

[318] Lemke, T. 2001. "The birth of bio-politics": Michel Foucault's lecture at the Collège de France on neo-liberal governmentality. *Economy and society*. 30, 2 (2001), 190–207.

[319] Lerner, J.I. and Mulligan, D.K. 2008. Taking the long view on the fourth amendment: Stored records and the sanctity of the home. *Stan. Tech. L. Rev.* (2008), 3.

[320] Ley, B., Ogonowski, C., Mu, M., Hess, J., Race, N., Randall, D., Rouncefield, M. and Wulf, V. 2015. At Home with Users: A Comparative View of Living Labs. *Interacting with Computers*. 27, 1 (Jul. 2015), 21–35. DOI:https://doi.org/10.1093/iwc/iwu025.

[321] Li, Y., Chen, M., Li, Q. and Zhang, W. 2012. Enabling multilevel trust in privacy preserving data mining. *IEEE Transactions on Knowledge and Data Engineering*. 24, 9 (2012), 1598–1612.

[322] Liccardi, I., Pato, J., Weitzner, D.J., Abelson, H. and De Roure, D. 2014. No technical understanding required: Helping users make informed choices about access to their personal data. *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (2014), 140–150.

[323] Lieberman, H., Paternò, F., Klann, M. and Wulf, V. 2006. End-user development: An emerging paradigm. *End user development*. Springer. 1–8.

[324] Lim, B.Y., Dey, A.K. and Avrahami, D. 2009. Why and why not explanations improve the intelligibility of context-aware intelligent systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2009), 2119–2128.

[325] Lin, H. and Fang, Y. 2013. Privacy-aware profiling and statistical data extraction for smart sustainable energy systems. *Smart Grid, IEEE Transactions on*. 4, 1 (2013), 332–340.

[326] Lin, J., Amini, S., Hong, J.I., Sadeh, N., Lindqvist, J. and Zhang, J. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012), 501–510.

[327] Locke, B.T. and Heppler, J.A. 2018. Teaching Data Literacy for Civic Engagement: Resources for Data Capture and Organization. *KULA: knowledge creation, dissemination, and preservation studies*. 2, 1 (2018), 23.

[328] Ludwig, T., Dax, J., Pipek, V. and Randall, D. 2016. Work or Leisure? Designing a User-centered Approach for Researching Activity "in the Wild." *Personal Ubiquitous Comput.* 20, 4 (Aug. 2016), 487–515. DOI:https://doi.org/10.1007/s00779-016-0935-7.

[329] Lull, James. 1990. *Inside family viewing : ethnographic research on television's audiences*. Routledge.

[330] Luna, J., Suri, N. and Krontiris, I. 2012. Privacy-by-design based on quantitative threat modeling. *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on* (2012), 1–8.

[331] Lynch, M. and Sharrock, W. 2011. *Ethnomethodology. Volume I*. Londres, Sage.
[332] Ma, Q., Johnston, A.C. and Pearson, J.M. 2008. Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*. 16, 3 (2008), 251–270.
[333] Mandinach, E.B. and Gummer, E.S. 2013. A systemic view of implementing data literacy in educator preparation. *Educational Researcher*. 42, 1 (2013), 30–37.
[334] Mandinach, E.B. and Gummer, E.S. 2016. *Data literacy for educators: Making it count in teacher preparation and practice*. Teachers College Press.
[335] Margulis, S.T. 2003. Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*. 59, 2 (Jul. 2003), 243–261. DOI:https://doi.org/10.1111/1540-4560.00063.
[336] Markham, A. 2018. Critical pedagogy as a response to datafication: Research methods as data literacy tools. *Qualitative Inquiry*. (2018), 1–12.
[337] Martin, S., Kelly, G., Kernohan, W.G., McCreight, B. and Nugent, C. 2008. Smart home technologies for health and social care support. *Cochrane Database Syst Rev*. 4, (2008).
[338] Massoud Amin, S. and Wollenberg, B.F. 2005. Toward a smart grid: power delivery for the 21st century. *Power and Energy Magazine, IEEE*. 3, 5 (2005), 34–41.
[339] Mattelmäki, T. 2006. *Design probes*. Aalto University.
[340] Mayer, P., Volland, D., Thiesse, F. and Fleisch, E. 2011. User Acceptance of'Smart Products': An Empirical Investigation. (2011).
[341] Mayer-Schönberger, V. and Cukier, K. 2013. *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
[342] Mayring, P. and Fenzl, T. 2014. Qualitative inhaltsanalyse. *Handbuch Methoden der empirischen Sozialforschung*. Springer. 543–556.
[343] Mazurek, M.L., Arsenault, J.P., Bresee, J., Gupta, N., Ion, I., Johns, C., Lee, D., Liang, Y., Olsen, J., Salmon, B. and others 2010. Access control for home data sharing: Attitudes, needs and practices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), 645–654.
[344] McAuley, D., Mortier, R. and Goulding, J. 2011. The dataware manifesto. *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on* (2011), 1–6.
[345] McDaniel, P. and McLaughlin, S. 2009. Security and privacy challenges in the smart grid. *IEEE Security & Privacy*. 3 (2009), 75–77.
[346] McKenna, E., Richardson, I. and Thomson, M. 2012. Smart meter data: Balancing consumer privacy concerns with legitimate applications. *Energy Policy*. 41, (2012), 807–814.
[347] Medaglia, C.M. and Serbanati, A. 2010. An overview of privacy and security issues in the internet of things. *The Internet of Things*. Springer. 389–395.
[348] Mendel, F., Rechberger, C., Schläffer, M. and Thomsen, S.S. 2009. The rebound attack: Cryptanalysis of reduced Whirlpool and Grøstl. *Fast Software Encryption* (2009), 260–276.

[349] Mennicken, S., Hofer, J., Dey, A. and Huang, E.M. 2014. Casalendar: a temporal interface for automated homes. *CHI'14 Extended Abstracts on Human Factors in Computing Systems* (2014), 2161–2166.
[350] Mennicken, S. and Huang, E.M. 2012. Hacking the natural habitat: an in-the-wild study of smart homes, their development, and the people who live in them. *International Conference on Pervasive Computing* (2012), 143–160.
[351] Mennicken, S., Hwang, A., Yang, R., Hoey, J., Mihailidis, A. and Huang, E.M. 2015. Smart for Life: Designing Smart Home Technologies that Evolve with Users. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (2015), 2377–2380.
[352] Mennicken, S., Kim, D. and Huang, E.M. 2016. Integrating the Smart Home into the Digital Calendar. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), 5958–5969.
[353] Mennicken, S., Vermeulen, J. and Huang, E.M. 2014. From today's augmented houses to tomorrow's smart homes: new directions for home automation research. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2014), 105–115.
[354] Merton, R., Fisk, M. and Kendall, P. 1956. The focused interview: a report of the bureau of applied social research. *New York: Columbia University*. (1956).
[355] Meyrowitz, J. 2002. Post-Privacy America. *Privatheit im öffentlichen Raum*. Springer. 153–204.
[356] Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*. 10, 7 (2012), 1497–1516.
[357] Mok, E. and Retscher, G. 2007. Location determination using WiFi fingerprinting versus WiFi trilateration. *Journal of Location Based Services*. 1, 2 (2007), 145–159.
[358] Moor, J.H. 1997. Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*. 27, 3 (1997), 27–32.
[359] Morgan, D.L. and Krueger, R.A. 1993. When to use focus groups and why. *Successful focus groups: Advancing the state of the art*. 1, (1993), 3–19.
[360] Mozer, M. 2004. *Lessons from an adaptive house*. Architectural Engineering.
[361] Müller, C., Hornung, D., Hamm, T. and Wulf, V. 2015. Practice - based Design of a Neighborhood Portal : Focusing on Elderly Tenants in a City Quarter Living Lab. *Proc. of CHI'15* (2015), 2295–2304.
[362] Müller, K.J. 2010. Gewinnung von Verhaltensprofilen am intelligenten Stromzähler. *Datenschutz und Datensicherheit-DuD*. 34, 6 (2010), 359–364.
[363] Müller, K.J. 2011. Sicherheit im Smart Grid. (2011).
[364] Müller, K.J. 2011. Verordnete Sicherheit—das Schutzprofil für das Smart Metering Gateway. *Datenschutz und Datensicherheit-DuD*. 35, 8 (2011), 547–551.
[365] Murata, A., Kanbayashi, M. and Hayami, T. 2013. Effectiveness of Automotive Warning System Presented with Multiple Sensory Modalities. *Digital Human Modeling and Applications in Health, Safety, Ergonomics, and Risk Management. Healthcare and Safety of the Environment and Transport* (Jul. 2013), 88–97.

[366] National Metrology Institute of German 2014. *PTB-Anforderungen PTB-A 50.8 Smart Meter Gateway*.

[367] Naumann, I. and Hogben, G. 2008. Privacy features of European eID card specifications. *Network Security*. 2008, 8 (2008), 9–13.

[368] Nederhof, A.J. 1985. Methods of coping with social desirability bias: A review. *European journal of social psychology*. 15, 3 (1985), 263–280.

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

[370] Nissenbaum, H. 2004. Privacy as contextual integrity. *Washington law review*. 79, 1 (2004).

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

[372] Norman, D.A. 1990. The'problem'with automation: inappropriate feedback and interaction, not'over-automation'. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences*. (1990), 585–593.

[373] O'Brien, J., Rodden, T., Rouncefield, M. and Hughes, J. 1999. At Home with the Technology : An Ethnographic Study of a Set-Top-Box Trial. *ACM Transactions on Computer-Human Interaction*. 6, (1999), 282–308. DOI:https://doi.org/10.1145/329693.329698.

[374] Ogonowski, C., Jakobi, T., Müller, C. and Hess, J. 2018. PRAXLABS: A sustainable framework for user-centered ICT development - Cultivating research experiences from Living Labs in the home,. *Socio-Informatics*. 592.

[375] Ogonowski, C., Jakobi, T., Müller, C. and Hess, J. 2018. PRAXLABS: A Sustainable Framework for User-Centered Information and Communication Technology Development-Cultivating Research Experiences from Living Labs in the Home. (2018).

[376] Ogonowski, C., Ley, B., Hess, J., Wan, L. and Wulf, V. 2013. Designing for the Living Room: Long-Term User Involvement in a Living Lab. *Proceedings of CHI '13* (New York, USA, Apr. 2013), 1539–1548.

[377] Ogonowski, O., Hennes, P. and Seiffert, M. 2016. Shop&Play Erlebnis im Smart Home: Nutzung statt Installationschaos. Workshop Usability für die betriebliche Praxis. (2016).

[378] Orientierungshilfe datenschutzgerechtes Smart Metering: 2012. *http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Orientierungshilfe_SmartMeter.html?nn=408920*. Accessed: 2014-02-07.

[379] Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N. and Myllymäki, P. 2012. Long-term effects of ubiquitous surveillance in the home. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012), 41–50.

[380] Pacific Gas & Electric. 2018. Find out how SmartMeterTM communicates with PG&E.

[381] Palen, L. and Aaløkke, S. 2006. Of pill boxes and piano benches: home-made methods for managing medication. *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (2006), 79–88.
[382] Palen, L. and Dourish, P. 2003. Unpacking privacy for a networked world. *Proceedings of the SIGCHI conference on Human factors in computing systems* (2003), 129–136.
[383] Pallas, F. 2012. Data Protection and smart grid communication-The European perspective. *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES* (2012), 1–8.
[384] Papakonstantinou, V. and Kloza, D. 2015. Legal protection of personal data in smart grid and smart metering systems from the European perspective. *Smart Grid Security*. Springer. 41–129.
[385] Patil, S., Norcie, G., Kapadia, A. and Lee, A.J. 2012. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (2012), 5.
[386] Patil, S., Page, X. and Kobsa, A. 2011. With a little help from my friends: can social navigation inform interpersonal privacy preferences? *Proceedings of the ACM 2011 conference on Computer supported cooperative work* (2011), 391–394.
[387] Patil, S., Schlegel, R., Kapadia, A. and Lee, A.J. 2014. Reflection or action?: how feedback and control affect location sharing decisions. (2014), 101–110.
[388] Petrlic, R. 2010. A privacy-preserving concept for smart grids. *Sicherheit in vernetzten Systemen*. 18, (2010), B1–B14.
[389] Pettersson, M., Randall, D. and Helgeson, B. 2004. Ambiguities, awareness and economy: a study of emergency service work. *Computer Supported Cooperative Work (CSCW)*. 13, 2 (2004), 125–154.
[390] Pfitzmann, A. 2001. Multilateral security: Enabling technologies and their evaluation. *Informatics* (2001), 50–62.
[391] Pfitzmann, A., Schill, A., Westfeld, A. and Wolf, G. 2000. Mehrseitige Sicherheit in offenen Netzen. *Grundlagen, praktische Umsetzung und in Java implementierte Demonstrations-Software*. (2000).
[392] Pfleging, B., Schneegass, S. and Schmidt, A. 2013. Exploring user expectations for context and road video sharing while calling and driving. (2013), 132–139.
[393] Pfleging, B., Schneegass, S. and Schmidt, A. 2012. Multimodal Interaction in the Car: Combining Speech and Gestures on the Steering Wheel. *Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (New York, NY, USA, 2012), 155–162.
[394] Pickering, C.A., Bumnham, K.J. and Richardson, M.J. 2007. A Review of Automotive Human Machine Interface Technologies and Techniques to Reduce Driver Distraction. *2007 2nd Institution of Engineering and Technology International Conference on System Safety* (Oct. 2007), 223–228.
[395] Pipek, V. 2005. *From tailoring to appropriation support: Negotiating groupware usage*. University of Oulu Oulu.
[396] Poole, E.S. 2012. Interacting with infrastructure. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work - CSCW '12* (New York, New York, USA, 2012), 759.
[397] Poole, E.S., Chetty, M., Grinter, R.E. and Edwards, W.K. 2008. More than meets the eye: transforming the user experience of home network management.

Proceedings of the 7th ACM conference on Designing interactive systems (2008), 455–464.

[398] Poole, E.S., Chetty, M., Morgan, T., Grinter, R.E. and Edwards, W.K. 2009. Computer help at home: methods and motivations for informal technical support. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2009), 739–748.

[399] Posthumus, S. and Von Solms, R. 2004. A framework for the governance of information security. *Computers & Security*. 23, 8 (2004), 638–646.

[400] Pötzsch, S. 2009. Privacy awareness: A means to solve the privacy paradox? *The future of identity in the information society*. Springer. 226–236.

[401] Prado, J.C. and Marzal, M.Á. 2013. Incorporating data literacy into information literacy programs: Core competencies and contents. *Libri*. 63, 2 (2013), 123–134.

[402] President's Council of Advisors on Science and Technology 2014. *Big Data and Privacy: A technological perspective*. Executive Office of the President.

[403] Rader, E. and Slaker, J. 2017. The importance of visibility for folk theories of sensor data. *Symposium on Usable Privacy and Security (SOUPS)* (2017).

[404] Randall, D. 2006. Living inside a smart home: A case study. *Inside the smart home*. Springer Science & Business Media. 227–246.

[405] Randall, D., Harper, R. and Rouncefield, M. 2007. *Fieldwork for design: theory and practice*.

[406] Rannenberg, K. 2001. Multilateral security a concept and examples for balanced security. *Proceedings of the 2000 workshop on New security paradigms* (2001), 151–162.

[407] Rao, A., Schaub, F. and Sadeh, N. 2015. What do they know about me? Contents and Concerns of Online Behavioral Profiles. *PASSAT '14: Sixth ASE International Conference on Privacy, Security, Risk and Trust* (2015).

[408] Rawnsley, A. 2018. Politicians can't control the digital giants with rules drawn up for the analogue era | Andrew Rawnsley. *The Guardian*.

[409] Reckwitz, A. 2008. *Subjekt*. transcript Verlag.

[410] Reckwitz, A. 2002. Toward a Theory of Social Practices: A Development in Culturalist Theorizing. *European journal of social theory*. 2002, 2 (May 2002), 245–265. DOI:https://doi.org/10.1177/13684310222225432.

[411] Rees, J., Bandyopadhyay, S. and Spafford, E.H. 2003. PFIRES: a policy framework for information security. *Communications of the ACM*. 46, 7 (2003), 101–106.

[412] Reidenberg, J.R., Breaux, T., Cranor, L.F., French, B., Grannis, A., Graves, J.T., Liu, F., McDonald, A.M., Norton, T.B., Ramanath, R., Russell, N.C., Sadeh, N. and Schaub, F. 2014. *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*. Technical Report #ID 2418297. Social Science Research Network.

[413] Reimer, H. 2012. Smart Meter—Smarter Datenschutz in intelligenten Stromnetzen. *Datenschutz und Datensicherheit-DuD*. 36, 3 (2012), 216–216.

[414] Reinisch, C., Kastner, W., Neugschwandtner, G. and Granzer, W. 2007. Wireless technologies in home and building automation. *Industrial Informatics, 2007 5th IEEE International Conference on* (2007), 93–98.

[415] Renner, S., Albu, M. and van Elburg, H. 2011. European Smart Metering Landscape Report. *Imprint*. February (2011).

[416] Rest, J. van, Boonstra, D., Everts, M., Rijn, M. van and Paassen, R. van 2012. Designing Privacy-by-Design. *Privacy Technologies and Policy*. B. Preneel and D. Ikonomou, eds. Springer Berlin Heidelberg. 55–72.

[417] Rial, A. and Danezis, G. 2011. Privacy-preserving smart metering. *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society* (2011), 49–60.

[418] Richman, W.L., Kiesler, S., Weisband, S. and Drasgow, F. 1999. A meta-analytic study of social desirability distortion in computer-administered questionnaires, traditional questionnaires, and interviews. *Journal of applied psychology*. 84, 5 (1999), 754.

[419] Rodden, T.A., Fischer, J.E., Pantidi, N., Bachour, K. and Moran, S. 2013. At home with agents: Exploring attitudes towards future smart energy infrastructures. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2013), 1173–1182.

[420] Rohde, M., Brödner, P., Stevens, G., Betz, M. and Wulf, V. 2016. Grounded Design–a praxeological IS research perspective. *Journal of Information Technology*. (2016).

[421] Roman, R., Zhou, J. and Lopez, J. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*. 57, 10 (2013), 2266–2279.

[422] Römer, B., Reichhart, P., Kranz, J. and Picot, A. 2012. The role of smart metering and decentralized electricity storage for smart grids: The importance of positive externalities. *Energy Policy*. 50, (2012), 486–495.

[423] Roßnagel, A. and Jandt, S. 2010. Datenschutzkonformes Energieinformationsnetz. *Datenschutz und Datensicherheit-DuD*. 34, 6 (2010), 373–378.

[424] Rost, M. 2011. Datenschutz in 3D. *Datenschutz und Datensicherheit-DuD*. 35, 5 (2011), 351–354.

[425] Rost, M. 2012. Standardisierte Datenschutzmodellierung. *Datenschutz und Datensicherheit-DuD*. 36, 6 (2012), 433–438.

[426] Rotella, P. 2012. Is data the new oil? *Forbes, April*. 2, (2012).

[427] Rottondi, C., Verticale, G. and Capone, A. 2013. Privacy-preserving smart metering with multiple data consumers. *Computer Networks*. 57, 7 (2013), 1699–1713.

[428] Rubinstein, I.S. 2011. Regulating privacy by design. *Berkeley Tech. LJ*. 26, (2011), 1409.

[429] Ruighaver, A.B., Maynard, S.B. and Chang, S. 2007. Organisational security culture: Extending the end-user perspective. *Computers & Security*. 26, 1 (2007), 56–62.

[430] Ruoti, S., Monson, T., Wu, J., Zappala, D. and Seamons, K. 2017. Weighing context and trade-offs: How suburban adults selected their online security posture. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). USENIX Association* (2017).

[431] de Ruyter, B. and Aarts, E. 2004. Ambient intelligence. *Proceedings of the Working Conference on Advanced Visual Interfaces - AVI '04* (New York, USA, May 2004), 203–208.

[432] Sanders, E. 2002. Ethnography in NPD Research: How "applied ethnography" can improve your NPD research process. *Visions magazine*. (2002).
[433] Sankar, L., Rajagopalan, S.R., Mohajer, S. and Poor, H.V. 2013. Smart meter privacy: A theoretical framework. *smart grid, IEEE transactions on*. 4, 2 (2013), 837–846.
[434] Sasse, M.A., Brostoff, S. and Weirich, D. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*. 19, 3 (2001), 122–131.
[435] Schaar, P. 2010. Privacy by Design. *Identity in the Information Society*. 3, 2 (Aug. 2010), 267–274. DOI:https://doi.org/10.1007/s12394-010-0055-x.
[436] Schaffers, H., Cordoba, M., Hongisto, P., Kallai, T. and Merz, C. 2007. Exploring business models for open innovation in rural living labs. *Proceedings of the International Conference on Concurrent Enterprising (ICE)* (2007).
[437] Schaub, F., Balebako, R., Durity, A.L. and Cranor, L.F. 2015. A design space for effective privacy notices. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (2015), 1–17.
[438] Schaub, F., Marella, A., Kalvani, P., Ur, B., Pan, C., Forney, E. and Cranor, L.F. 2016. Watching them watching me: Browser extensions impact on user privacy awareness and concern. *NDSS workshop on usable security* (2016).
[439] Scheibelhofer, E. 2008. Combining Narration-Based interviews with topical interviews: Methodological reflections on research practices. *International Journal of Social Research Methodology*. 11, 5 (2008), 403–416.
[440] Schiek, D. 2014. *The Written Interview in Qualitative Social Research*. Lucius Verlag mbH.
[441] Schmidt, A., Dey, A.K., Kun, A.L. and Spiessl, W. 2010. Automotive User Interfaces: Human Computer Interaction in the Car. *CHI '10 Extended Abstracts on Human Factors in Computing Systems* (New York, NY, USA, 2010), 3177–3180.
[442] Schütz, A. 1981. Der sinnhafte Aufbau der sozialen Welt [La construction sensée du monde social]. *Frankfurt/M.: Suhrkamp*. (1981).
[443] Schuurman, D. and De Marez, L. 2009. User-Centered Innovation: Towards a Conceptual Integration of Lead Users and Living Labs. *Proceedings of COST 298: The Good, The Bad and The Challenging* (Copenhagen, Denmark, 2009), 114–123.
[444] Schwartz, A. 2009. Looking back at P3P: lessons for the future. *Center for Democracy & Technology, https://www. cdt. org/files/pdfs/P3P_Retro_Final_0. pdf*. (2009).
[445] Schwartz, T., Denef, S., Stevens, G., Ramirez, L. and Wulf, V. 2013. Cultivating energy literacy: results from a longitudinal living lab study of a home energy management system. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2013), 1193–1202.
[446] Schwartz, T., Denef, S., Stevens, G., Ramirez, L. and Wulf, V. 2013. Cultivating Energy Literacy: Results from a Longitudinal Living Lab Study of a Home Energy Management System. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2013), 1193–1202.
[447] Schwartz, T., Stevens, G., Jakobi, T., Denef, S., Ramirez, L., Wulf, V. and Randall, D. 2015. What people do with consumption feedback: a long-term living

lab study of a home energy management system. *Interacting with Computers*. 27, 6 (2015), 551–576.
[448] Schwartz, T., Stevens, G., Ramirez, L. and Wulf, V. 2013. Uncovering practices of making energy consumption accountable: A phenomenological inquiry. *ACM Transactions on Computer-Human Interaction (TOCHI)*. 20, 2 (2013), 12.
[449] Schwartz, T., Stevens, G., Ramirez, L. and Wulf, V. 2013. Uncovering Practices of Making Energy Consumption Accountable: A Phenomenological Inquiry. *ACM Trans. Comput.-Hum. Interact.* 20, 2 (May 2013), 12:1–12:30. DOI:https://doi.org/10.1145/2463579.2463583.
[450] Schwichtenberg, S. 2015. „Pay as you drive "–neue und altbekannte Probleme. *Datenschutz und Datensicherheit-DuD*. 39, 6 (2015), 378–382.
[451] Seipp, D.J. 1981. *The right to privacy in American history*. Harvard University, Program on Information Resources Policy.
[452] Shay, R. and Bertino, E. 2009. A comprehensive simulation tool for the analysis of password policies. *International Journal of Information Security*. 8, 4 (2009), 275–289.
[453] Sheppard, S. 2003. The Selected Writings and Speeches of Sir Edward Coke. *Indianapolis: Liberty Fund*. 1, (2003).
[454] Shilton, K. 2009. Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*. 52, 11 (2009), 48–53.
[455] Shneiderman, B. 1996. The eyes have it: A task by data type taxonomy for information visualizations. *Visual Languages, 1996. Proceedings., IEEE Symposium on* (1996), 336–343.
[456] Shneiderman, B. and Hochheiser, H. 2001. Universal Usability as a Stimulus to Advanced Interface Design (2001). (2001).
[457] Silverstone, R. and Haddon, L. 1996. Design and the domestication of ICTs: technical change and everyday life. *Communicating by Design: The Politics of Information and Communication Technologies*. (1996), 44–74.
[458] Simon, H.A. 1991. Bounded rationality and organizational learning. *Organization science*. 2, 1 (1991), 125–134.
[459] Simon, H.A. 1982. *Models of bounded rationality: Empirically grounded economic reason*. MIT press.
[460] Siponen, M., Pahnila, S. and Mahmood, M.A. 2010. Compliance with information security policies: An empirical investigation. *Computer*. 43, 2 (2010).
[461] Smart Home Report 2018: *https://www.statista.com/study/42112/smart-home-report/*. Accessed: 2018-12-03.
[462] Smart Homes Market Size, Share| Future, Trends Estimate 2025: *http://www.transparencymarketresearch.com/smart-homes-market.html*. Accessed: 2017-09-16.
[463] Solove, D. 2008. Understanding privacy. May (2008).
[464] Solove, D.J. 2002. Conceptualizing Privacy. *California Law Review*. 90, 4 (Jul. 2002), 1087–1155. DOI:https://doi.org/10.2307/3481326.
[465] Sonnenberg, J. 2010. Service and User Interface Transfer from Nomadic Devices to Car Infotainment Systems. *Proceedings of the 2Nd International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (New York, NY, USA, 2010), 162–165.

[466] Spiekermann, S., Grossklags, J. and Berendt, B. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. *Proceedings of the 3rd ACM conference on Electronic Commerce* (2001), 38–47.

[467] Stalder, F. 2010. Autonomy and control in the era of post-privacy. *Open*. 19, (2010), 81–83.

[468] Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. 2005. Analysis of end user security behaviors. *Computers & security*. 24, 2 (2005), 124–133.

[469] Stein, M., Boden, A., Hornung, D., Wulf, V., Garschall, I.M., Hamm, T., Müller, C., Neureiter, K., Schorch, M. and van Velsen, L. 2016. Third Spaces in the Age of IoT: A Study on Participatory Design of Complex Systems. *Symposium on Challenges and experiences in designing for an ageing society, 12th International Conference on Designing Interactive Systems (COOP)* (2016).

[470] Stephenson, E. and Schifter Caravello, P. 2007. Incorporating data literacy into undergraduate information literacy programs in the social sciences: A pilot project. *Reference Services Review*. 35, 4 (Nov. 2007), 525–540. DOI:https://doi.org/10.1108/00907320710838354.

[471] Stevens, G. and Bossauer, P. 2017. Dealing with Personal Data in the Age of Big Data Economies. *Zeitschrift fuer Geistiges Eigentum/Intellectual Property Journal*. 9, 3 (2017), 266–278.

[472] Stevens, G., Bossauer, P., Jakobi, T. and Pakusch, C. 2018. Mehrseitiges Vertrauen bei IoT-basierten Reputationssystemen. *Mensch und Computer 2018-Workshopband*. (2018).

[473] Stevens, G., Jakobi, T. and Detken, K.-O. 2014. Mehrseitige, barrierefreie Sicherheit intelligenter Messsysteme. *Datenschutz und Datensicherheit*. 38, 8/2014 (2014), 536–544.

[474] Stevens, G., Pipek, V. and Wulf, V. 2009. Appropriation infrastructure: Supporting the design of usages. *End-user development*. Springer. 50–69.

[475] Stevens, G. and Wulf, V. 2009. Computer-supported access control. *ACM Transactions on Computer-Human Interaction (TOCHI)*. 16, 3 (2009), 12.

[476] Stevens, M., Bursztein, E., Karpman, P., Albertini, A. and Markov, Y. 2017. The first collision for full SHA-1. *Annual International Cryptology Conference* (2017), 570–596.

[477] Stevens, M., Karpman, P. and Peyrin, T. 2016. Freestart collision for full SHA-1. *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2016), 459–483.

[478] Strengers, Y. 2011. Negotiating everyday life: The role of energy and water consumption feedback. *Journal of Consumer Culture*. 11, 3 (2011), 319–338.

[479] Strengers, Y.A.A. 2011. Designing Eco-feedback Systems for Everyday Life. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2011), 2135–2144.

[480] Suryadevara, N.K., Mukhopadhyay, S.C., Wang, R. and Rayudu, R.K. 2013. Forecasting the behavior of an elderly using wireless sensors data in a smart home. *Engineering Applications of Artificial Intelligence*. 26, 10 (2013), 2641–2652.

[481] Sutanto, J., Palme, E., Tan, C.-H. and Phang, C.W. 2013. Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *Mis Quarterly*. 37, 4 (2013), 1141–1164.

[482] Swan, M. 2015. Connected Car: Quantified Self becomes Quantified Car. *Journal of Sensor and Actuator Networks*. 4, 1 (Feb. 2015), 2–29. DOI:https://doi.org/10.3390/jsan4010002.

[483] Sweeney, L. 2002. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*. 10, 05 (2002), 557–570.

[484] Taherdoost, H., Zamani, M. and Namayandeh, M. 2009. Study of smart card technology and probe user awareness about it: A case study of Middle Eastern students. *2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009* (Aug. 2009), 334–338.

[485] Takabi, H., Joshi, J.B. and Ahn, G.-J. 2010. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*. 6 (2010), 24–31.

[486] Tang, K., Hong, J. and Siewiorek, D. 2012. The implications of offering more disclosure choices for social location sharing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2012), 391–394.

[487] Tang, K.P., Lin, J., Hong, J.I., Siewiorek, D.P. and Sadeh, N. 2010. Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. *Proceedings of the 12th ACM international conference on Ubiquitous computing* (2010), 85–94.

[488] Tang, L.M. and Kay, J. 2017. Harnessing Long Term Physical Activity Data—How Long-term Trackers Use Data and How an Adherence-based Interface Supports New Insights. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 1, 2 (Jun. 2017), 1–28. DOI:https://doi.org/10.1145/3090091.

[489] Tapia, E.M., Intille, S.S. and Larson, K. 2004. *Activity recognition in the home using simple and ubiquitous sensors*. Springer.

[490] Teal, T.K., Cranston, K.A., Lapp, H., White, E., Wilson, G., Ram, K. and Pawlik, A. 2015. Data carpentry: workshops to increase data literacy for researchers. *International Journal of Digital Curation*. 10, 1 (2015), 135–143.

[491] The Universal Declaration of Human Rights: 1948. *http://www.un.org/en/universal-declaration-human-rights/*. Accessed: 2016-08-06.

[492] The world's most valuable resource is no longer oil, but data: 2017. *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*. Accessed: 2018-12-05.

[493] Thomas, W.I. and Thomas, D.S. 1928. The methodology of behavior study. *The child in America: Behavior problems and programs*. (1928), 553–576.

[494] Tolmie, P., Crabtree, A., Egglestone, S., Humble, J., Greenhalgh, C. and Rodden, T. 2009. Digital plumbing: the mundane work of deploying UbiComp in the home. *Personal and Ubiquitous Computing*. 14, 3 (Dec. 2009), 181–196. DOI:https://doi.org/10.1007/s00779-009-0260-5.

[495] Tolmie, P., Crabtree, A., Rodden, T., Colley, J. and Luger, E. 2016. "This has to be the cats": Personal Data Legibility in Networked Sensing Systems. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (2016), 491–502.

[496] Tolmie, P., Crabtree, A., Rodden, T., Greenhalgh, C. and Benford, S. 2007. Making the home network at home: Digital housekeeping. *ECSCW 2007*. Springer. 331–350.
[497] Tony Romm, Brian Fung, Aaron C. Davis and Craig Timberg 2018. 'It's about time': Facebook faces first lawsuit from U.S. regulators after Cambridge Analytica scandal. *Washington Post*.
[498] Townsend, D., Knoefel, F. and Goubran, R. 2011. Privacy versus autonomy: a tradeoff model for smart home monitoring technologies. *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE* (2011), 4749–4752.
[499] Tsormpatzoudi, P., Berendt, B. and Coudert, F. 2015. Privacy by Design: From Research and Policy to Practice–the Challenge of Multi-disciplinarity. *Annual Privacy Forum* (2015), 199–212.
[500] Ur, B., Jung, J. and Schechter, S. 2014. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-entryway Surveillance. *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (New York, NY, USA, 2014), 129–139.
[501] Ur, B., Jung, J. and Schechter, S. 2013. The current state of access control for smart devices in homes. *Workshop on Home Usable Privacy and Security (HUPS)* (2013).
[502] Ur, B., McManus, E., Pak Yong Ho, M. and Littman, M.L. 2014. Practical trigger-action programming in the smart home. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2014), 803–812.
[503] Ur, B., Pak Yong Ho, M., Brawner, S., Lee, J., Mennicken, S., Picard, N., Schulze, D. and Littman, M.L. 2016. Trigger-action programming in the wild: An analysis of 200,000 ifttt recipes. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), 3227–3231.
[504] U.S.C 1974. *Privacy Act of 1974*.
[505] Veiga, A.D. and Eloff, J.H. 2007. An information security governance framework. *Information Systems Management*. 24, 4 (2007), 361–372.
[506] Wan, L., Müller, C., Wulf, V., Randall, D.W., Wan, L., Müller, C., Wulf, V. and Randall, D.W. 2014. Addressing the subtleties in dementia care. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14* (New York, New York, USA, 2014), 3987–3996.
[507] Wang, S., Cui, L., Que, J., Choi, D.-H., Jiang, X., Cheng, S. and Xie, L. 2012. A randomized response model for privacy preserving smart metering. *Smart Grid, IEEE Transactions on*. 3, 3 (2012), 1317–1324.
[508] Wang, X. and Yu, H. 2005. How to break MD5 and other hash functions. *Annual international conference on the theory and applications of cryptographic techniques* (2005), 19–35.
[509] Ware, W.H. 1973. *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. US Department of Health, Education & Welfare.
[510] Warren, S.D. and Brandeis, L.D. 1890. The right to privacy. *Harvard law review*. (1890), 193–220.

[511] Wass, C. and Kurz, T. 2012. Digitale Hilfsmittel für mehr Transparenz bei der Verarbeitung personenbezogener Daten. *Datenschutz und Datensicherheit-DuD*. 36, 10 (2012), 748–752.
[512] Weber, R.H. 2010. Internet of Things–New security and privacy challenges. *Computer Law & Security Review*. 26, 1 (2010), 23–30.
[513] Weeks, B.E., Ardèvol-Abreu, A. and Gil de Zúñiga, H. 2017. Online influence? Social media use, opinion leadership, and political persuasion. *International Journal of Public Opinion Research*. 29, 2 (2017), 214–239.
[514] Weiser, M. 1991. The computer for the 21st century. *Scientific american*. 265, 3 (1991), 94–104.
[515] Weiss, R.S. 1995. *Learning from strangers: The art and method of qualitative interview studies*. Simon and Schuster.
[516] Werlinger, R., Hawkey, K. and Beznosov, K. 2009. An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*. 17, 1 (2009), 4–19.
[517] Westin, A.F. 1970. Privacy and freedom. (1970).
[518] Whitman, M.E. and Mattord, H.J. 2011. *Principles of information security*. Cengage Learning.
[519] Whitten, A. and Tygar, J.D. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium* (1999), 16.
[520] Why Data Is The New Oil: *http://fortune.com/2016/07/11/data-oil-brainstorm-tech/*. Accessed: 2018-12-05.
[521] Wissner, M. 2009. *Smart metering*. WIK, Wiss. Inst. für Infrastruktur und Kommunikationsdienste.
[522] Witzel, A. and Reiter, H. 2012. *The problem-centred interview*. Sage.
[523] Woo, J. and Lim, Y. 2015. User experience in do-it-yourself-style smart homes. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2015), 779–790.
[524] Woo, J. and Lim, Y. 2015. User Experience in Do-it-yourself-style Smart Homes. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (New York, NY, USA, 2015), 779–790.
[525] Wright, D. 2011. A framework for the ethical impact assessment of information technology. *Ethics and information technology*. 13, 3 (2011), 199–226.
[526] Wulf, V. 1997. *Konfliktmanagement bei Groupware*. Springer.
[527] Wulf, V., Müller, C., Pipek, V., Randall, D., Rohde, M. and Stevens, G. 2015. Practice-Based Computing: Empirically Grounded Conceptualizations Derived from Design Case Studies. Springer London. 111–150.
[528] Wulf, V., Rohde, M., Pipek, V. and Stevens, G. 2011. Engaging with practices: design case studies as a research framework in CSCW. *Proceedings of the ACM 2011 conference on Computer supported cooperative work*. (2011), 505–512.
[529] Wunderlich, P., Veit, D. and Sarker, S. 2012. Adoption of Information Systems in the Electricity Sector: The Issue of Smart Metering. *AMCIS 2012 Proceedings*. (Jul. 2012).
[530] Yang, R. and Newman, M. 2013. Learning from a learning thermostat: lessons for intelligent systems for the home. *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. (2013), 93–102.

[531] Yonego, J.T. 2014. Data Is the New Oil of the Digital Economy. *Wired*.
[532] Yoshihisa, T., Fujita, N. and Tsukamoto, M. 2011. HEMS toolkit: A toolkit for constructing a home energy management system. *2011 IEEE Consumer Communications and Networking Conference (CCNC)*. (Jan. 2011), 822–823. DOI:https://doi.org/10.1109/CCNC.2011.5766612.
[533] Zandbergen, P.A. 2009. Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning. *Transactions in GIS*. 13, s1 (2009), 5–25.
[534] Zhang, D., Gu, T. and Wang, X. 2005. Enabling context-aware smart home with semantic web technologies. *International Journal of Human-friendly Welfare Robotic Systems*. 6, 4 (2005), 12–20.
[535] Zhang, X., Wuwong, N., Li, H. and Zhang, X. 2010. Information security risk management framework for the cloud computing environments. *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on* (2010), 1328–1334.
[536] Zhou, S. and Brown, M.A. 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.
[537] Ziamou, P.L., Gould, S. and Venkatesh, A. 2012. "Am I Getting It or Not?" The Practices Involved in "Trying to Consume" a New Technology. *Journal of Product Innovation Management*. 29, 2 (2012), 216–228.
[538] Zurko, M.E. 2005. User-centered security: Stepping up to the grand challenge. *Computer Security Applications Conference, 21st Annual* (2005), 14–pp.
[539] Zurko, M.E. and Simon, R.T. 1996. User-centered security. *Proceedings of the 1996 workshop on New security paradigms* (1996), 27–33.