Empowering Privacy in the Connected Home

Communal Use of Smart Technologies

Martin Johannes Krämer

Linacre College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Hilary 2022

Acknowledgements

No research is done in isolation. It benefits from countless discussions and conversations with others, either in person or while engaging with their published work.

First and foremost, my gratitude goes to my supervisors for their continued guidance, support, and encouragement. I'm grateful to Professor Ivan Flechais for taking me on as a student and showing confidence in my abilities as a researcher when I had little to show for myself. I'm also most grateful to Dr Helena Webb for daring to join this journey when it already had started. Thank you, Ivan and Helena, for endless discussions, ideas, and your commitment to developing me as a researcher.

Countless conversations with other researchers have shaped this work. Thank you, Professors Max Van Kleek and Reuben Binns for "cheer-leading" this work (your words), and for allowing me to collaborate on amazing projects. Many thanks to Professors Marina Jirotka and Andy Simpson for providing valuable feedback, ideas, and insightful discussions during transfer and confirmation of status evaluations. I'm also grateful for insightful discussions with researchers at the Centre for Doctoral Training (CDT) in Cyber Security and with colleagues from the Human-Centred Computing theme at the Department of Computer Science. My special thanks to my collaborators Dr Norbert Nthala, Dr William Seymour, and George Chalhoub. Finally, it was a privilege and pleasure to discuss this work with my examiners Professor Marina Jirotka and Dr Ewa Luger.

My gratitude goes out to the wider Human-Centred Computing research community. I'm grateful for enriching conversations with Professors Irina Shklovski and Helen Nissenbaum who helped me appreciate the complexity and beauty of researching privacy. I'd like to thank the ACM SIGCHI community at large for discussions, feedback, and encouragement; particularly, the amazing cohort and faculty of the 2018 Doctoral Consortium.

Research is not possible without institutional support. My studies were funded by an CDT Cyber Security Scholarship, courtesy of the University of Oxford and the EPSRC UK (EP/P00881X/1). Grants from the Research Institute for Sociotechnical Cyber Security (RISCS) and the Information Commissioners Office (ICO) UK allowed me to conduct my empirical work. Thank you to Professor Andrew Martin and the CDT as well as the Department of Computer Science at the University of Oxford for providing an amazing research environment. To David Hobbs and Mauren York on behalf of all administrative staff, thank you so much for your dedication.

This thesis would not have been possible without the support of friends and family. My gratitude goes to Elakshi, Cedric, and Aline whom I was lucky to befriend while at Edinburgh University. I'm also grateful to Oliver for his friendship and guidance

over the years. Through your encouragement, I found the confidence to start this journey in the first place.

It was truly a privilege to spend almost five years beneath the dreaming spires of Oxford. Thank you to Linacre College and the Common Room for an amazing time. Thank you to the members of Oxford University Walking Club for great trips and good conversations. A huge thanks also to all of Linacre Boat Club. I've learned as much spending time at the club as I have during my studies. My Oxford experience would not have been the same without you.

To my dear friends I made at Oxford. Reino, James, and Will for many relaxing board game nights, runs/walks, and other social hours we spent. Jack, Monica, and Gla for various trips, long conversations, and challenging discussions. To the residents of Great Mead during the first nation-wide lockdown in the wake of the COVID-19 pandemic, thank you for keeping up good spirits and for a genuinely amazing time. Thank you to the residents of Walton Well Road, particularly Sylvia and Cleo, for making the second lockdown and my thesis writing so much more enjoyable. To all my friends, in Oxford and elsewhere, thank you for sharing your questions, thoughts, and kind words.

To my closest friends who dared to stick out the whole journey with me. Kwang, finding your friendship at Oxford has been the most incredible and enriching experience. I cannot describe the countless ways in which you helped me become a better person and a better researcher. To my best friend Andy who has always been there over the years, thank you for challenging me when I needed it, picking me up when I fell, and listening to me when I wanted to talk.

None of this would have been possible without the incredible support of my family. Huge thanks to my siblings, their partners, and to my godfather. Your care, interest, and curiosity have always been comforting and inspiring at the same time. My heartfelt gratitude goes to my parents for their endless love, their kindness, and for the values and work ethic they have instilled in me.

Abstract

The latest wave of internet-connected smart home technologies promises convenience and control over a diverse network of different systems, such as appliances, utilities, and entertainment devices. Striking the balance between convenience and control proves to be a minefield for product designers. Firstly, the data needs of these technologies amplify concerns over improper data collection and processing practices, highlighting a power imbalance between users and manufacturers. Secondly, convenience and control favour specific practices of use that manifest in related power differentials among household members. Additionally, devices are sometimes utilised for coercive control or domestic abuse.

These are issues of information and interpersonal privacy that surface in the home. However, due to the rapid evolution of technology, the nature of these issues remains under-explored. To fill in this research gap, we ask: 'How can households living in connected homes be empowered in their privacy?' Because privacy is a concept that invites many different definitions and interpretations, the thesis adopts an exploratory and inductive approach. It approaches the overarching research question in four steps: (1) 34 semi-structured interviews inquiring people about their internet-connected and smart device usage practices; (2) a six-month ethnomethodologically informed study of six households' experiences with smart home devices; (3) a conceptual framework to position emerging findings for research and design; and (4) two case studies that demonstrate the applicability of this framework to privacy in smart homes.

Inductive thematic analysis of interview data provided insights into the ways in which technology use in the home was communal. Building on these insights and their relationship to privacy, we used grounded analysis to analyse and present data from home visits, individual diaries, and observations. Sensitising concepts from ethnomethodology provided focus and perspectives on the establishment of communal use. Key findings include (1) fluid divisions of labour (planned and unplanned) that contributed to the construction of roles with respect to devices; (2) the ways in which household members' interactions contribute to a sense of normalcy (e.g. appropriate use) and to the management of relationships inside and outside the home; (3) that household members sometimes articulated this normalcy in rules to highlight expectations of use and everyday considerations of privacy. We used conceptual framework analysis to link these insights with salient concepts from existing literature on privacy for smart technologies. The framework offered an additional agentic perspective and sensitising concepts to inform innovation in research and design. The case studies drew on the framework to discuss strengths and weaknesses of research contributions. The insights gained from the study offer implications for data protection regulations along with academic debates on interpersonal power imbalances in the home.

Contents

List of Figures

List of Tables

1 Introduction

Contents

My friend Cayla hit the markets as the "World's Best Talking Doll" in 2014, and subsequently won the innovative toy of the year prize in the UK (Toy Retailers Association) [1]. The doll used speech recognition backed by an internet search engine ("Ask her questions about herself, people, places, and things!"), and was claimed to have the personality of a seven-year-old girl who likes to visit, among other places, Disneyland [2]. When children started asking for trips to the theme park, parents started voicing their concerns and security researchers later hacked the doll's voice interface. State authorities such as the United States Federal State Commission and the German Bundesnetzagentur launched investigations following these reports of security vulnerabilities. Genesis Toys, the US distributor of the toy, faced allegations of child and data protection laws violation where the doll was found to be an "immediate threat

to the safety and security of children" [3, p. 1] and classified as an illegal transmitting device by German authorities [4] that could be used to spy on children.

Threats of surveillance are, of course, not limited to states, organisations, or parents and their children but can also affect relationships between adults [5]. For example, a businessman was found guilty of having spied on his estranged wife using a wall-mounted iPad [6]. There is an increased recognition of concern for internet-connected technology being abused by not only entities external to the household but also those who live inside it [7]. Even members of the same household can misappropriate devices in ways that harm one another's freedom of expression, autonomy, and independence even though the initially intended use was benign [8, 9].

These two cases are symptoms of a larger problem: (1) a knowledge and power imbalance between individuals and businesses, and (2) a related power imbalance among individuals with regard to access, use, and processing of information. Genesis Toys, the doll manufacturer, was ignorant of sensitivities around data collection and processing, especially towards children. The estranged husband deliberately broke social norms, faced legal allegations of stalking, and was convicted for harassment [10]. In both cases, technology was used to violate individuals' privacy.

As the two examples suggest, the home is one of the places where technology and society overlap. The market for smart home technology grows rapidly [11] and a diverse set of increasingly unobtrusive and ubiquitous internet-connected devices becomes widely available. Household members share use of and housekeeping efforts for any devices like televisions, computers, or newer internet-connected appliances. No unique form of a household exists. Short-term lodging, single & dual-income families, multi-generation households, and other forms of cohabitation are inherently different social structures with different requirements on how the use of technology can be incorporated in daily life. Different forms of cohabitation and emerging technologies bring new complexity to the relationship between households, their members, and service providers.

Research has asked and partly answered a broad array of questions following such perceived privacy violations: How do they come about? How can they be explained?

Are they sustained? Are they justified? Are they reasonable? Should they be considered or neglected? Because of its social and technical complexity, the smart home is a particularly interesting context for privacy research.

1.1 Research Problem

The perceived violations of privacy are symptoms of a larger problem, a knowledge and potentially power imbalance between companies and households, and a power imbalance among users of the same household. Companies amass data generated by the users of their products and trade this data on markets, arguably more to their own benefit than the users'. In the European Union such practices are now subject to regulations under the General Data Protection Regulation (GDPR) [12]. While regulating collection and use of data is meant to shift the power balance towards the users, it also burdens them with more information and responsibility. At the same time, the GDPR includes a household exemption, scoping out use of devices and considerations of data flows in domestic environments. The research problem is characterised by a number of observations in relation to these power imbalances.

Firstly, users are expected to understand *a priori* the significance of their preferences and decisions on sharing data—something they are known to struggle with [13]. Accessible means of exercising the required level of control are required and radical propositions to re-architecture the internet have been put forward to address such gap, e.g., the Databox project [14]. Despite these efforts, the major challenge of making such approaches usable for everyone persists. Secondly, while approaches like Databox promise the opportunity of *in-situ* decision-making to avoid the need to state generic *a priori* preferences [14], more research is needed to understand how such decision-making can be enabled and facilitated [15]. Thirdly, the knowledge and power imbalance brought about by the very same devices also exists among household members where the use of technology is deeply entrenched in its social organisation and order [16–18]. Influenced by their abilities, knowledge, and attitudes, inhabitants deal with technology in their own ways. At times, these knowledge and power imbalances can facilitate coercive and abusive behaviours [7, 9]. Lastly, there is a gap in the literature on

understanding household privacy. As householders share resources and responsibilities, understanding how they manage their individual and shared privacy is essential in addressing the power imbalance.

While privacy can serve as a perspective for understanding these power imbalances, the concept itself is complex and multifaceted: researchers describe privacy as a concept in disarray (e.g., [19]); that researching privacy can invoke many possible interpretations of the word (e.g., [20]); and that privacy is commonly regarded as highly situational (dependent on social, physical, and technical contexts) and evolving over time (e.g., [21, 22]). In light of these observations this thesis asks: *"How can households living in connected homes be empowered in their privacy?"*. We approached our overarching question empirically using the following three main research questions which we refined over the course of our study (Chapter 3).

RQ–1 What is the nature of the relationship between internet-connected technology use and privacy in the home?

RQ–2 How does the nature of the relationship between internet-connected technology use in the home and privacy manifest in-situ?

RQ–3 How can the resulting findings inform innovation in research and design for privacy in the home?

1.2 Research Politics

The main research question asks how households can be *empowered* to address *power* imbalances between users and with manufacturers. The thesis thereby enters the political territories of conceptualising power relationships and designing technologies for the home (e.g. [7, 23–25]).

Empowerment appears unequivocally positive on first sight, but on reflection needs to be considered carefully. Interventions can accidentally mark disadvantaged minorities and appear overburdening when the help offered is undesired [26]. Empowering households also raises the question of 'who within the household will be the recipient of the empowerment'. Because "intimate relationships have inherent, dynamic power differentials, backed by explicit or implicit authority" [7], empowerment

through design needs to carefully weigh the risks of amplifying pre-existing power differentials [7, 23]. Researchers and designers need to reflect on "the underlying ethical maxims of empowerment" [24].

Power itself is a contested concept in social and political theory under significant influence of feminist theory [27]. To explain the use of power and empowerment in this thesis, we will draw on a common, albeit contested, distinction between power-to and power-over. *Power-over* describes the ability to get another person to do something. The means by and conditions under which this act happens differ largely between definitions. For instance, Weber [28] defines the term as ability to act "despite resistance" while Allen [27] discusses the term from feminist perspectives, defining it as 'power as domination'. We adopt Dahl's [29] definition of power-over as the ability to get another person to do something they otherwise would not do (omitting the use of force). Proponents of the *power-to* stance define the concept in terms of people's capacity, ability, or potential to achieve something. We adopt Pitkin's [30] definition which suggests "that power is a something – anything – which makes or renders somebody able to do, capable of doing something. Power is capacity, potential, ability, or wherewithal" [30, p. 276].

This thesis aims to achieve empowerment by decreasing opportunities of power-over and increasing opportunities of power-to. Its general orientation follows a "reconceptualization of power as a capacity or ability, specifically, the capacity to empower or transform oneself and others" [27] advocated for by feminists "as an alternative to putatively masculine notions of power-over" [27]. Our ethical maxim of empowerment can be broadly described following Nussbaum and Sen's [31] *equality of opportunity to access resources.* This research understands empowerment as "a process by which people, organizations, and communities gain mastery over issues of concern to them" [32].

Transparency of research and design politics as well as reflection during the design process are paramount when conceptualising and designing interventions. Considering Wartenberg's [33] response to feminist conceptualisations of power as capacity or ability (power-to), this need becomes evident. The author suggests such feminist conceptualisations of power as *transformative capacity* are only distinct from *power-over* in the sense that they seek to empower others rather than dominating them. The

difference is simply the intention of those exercising the power. As research on intimate relationships and abusive behaviour documents, the same technology design can enable supporting and controlling behaviour [7, 23]. These consequences of empowerment and effects of design interventions require careful consideration and anticipation as demonstrated in Chapter 6 and Chapter 7.

1.3 Research Scope and Terminology

The thesis initially considers all internet-connected devices and forms of cohabitation to explore technology use in the home (Chapter 4). As our research progresses, we identify *communal use of smart devices* as one of the most complex features in this relationship. Chapter 5, therefore, focuses on the communal use of smart home devices in close-tie relationships (i.e., families with/without children). The chapter includes devices with communal implications because of their affordances or data collection practices (e.g., smart security cameras or thermostats), and devices that are *inherently shareable* [34] (e.g., smart televisions or voice assistants). It excludes inherently personal devices (e.g., fitness trackers) and general purpose computers (e.g., smart phones or tablets). Note that all of these devices might be shared, and this thesis' findings are still relevant to them.

As we will elaborate in Chapter 2 and further explain in Chapter 3, the overall research approach adopted to make sense of people's lived experiences is empirical and exploratory. We take lived experiences to include everything to which people frequently relate as well as concepts and artefacts on which they draw when conducting their everyday lives. We would not challenge the existence and need for analytic concepts of privacy manifested in certain areas of law, policy, and engineering. However, believing that an understanding of how privacy manifests itself in everyday life is required to effectively empower privacy in the home, we refrain from drawing on existing conceptualisations in our approach to development of such understanding. This thesis therefore focuses on everyday interactions in which the concept of privacy is constituted.

Connected homes harbour one or more *internet-connected devices* (e.g., desktops, laptops, phones, and many more) while *smart homes* include smart technologies. *Smart*

technologies offer not only remote-controllability (emic perspective) but are also interconnected, communicable to other devices, and provide at least one of the following: intelligence, automation, or assistance (etic perspective) [35][1]. *Smart devices* embed smart technologies and fall in *at least* one of these categories: entertainment, energy management, security management, health/home care, communication, controlling appliances, or increasing comfort levels [36]. They offer one or more modes of interaction, requiring a form of set-up and configuration using a smart phone application that includes creating an account with their manufacturer)[2]; *Smart devices* are often remote controllable via smartphone interfaces and sensors while also offering a range of different interaction modes, including haptic/capacitive touch interfaces, voice control, gestures, or proximity-based controls.

1.4 Research Contributions

This research is situated in the emerging field of Human Centred Computing (HCC), drawing on methods commonly used in the subfields of HCI and Computer-Supported Cooperative Work and Social Computing (CSCW) to advance the scholarship on privacy across these fields. As such, its contributions are also relevant to the emerging 'meta-discipline' of cyber security [38]. In summary, the contributions of this research are:

An Everyday Perspective on Communal Use and Privacy – Chapters 4 and 5 provide empirical insights on communal use of internet-connected technologies in the home. The organisation of communal use as constituted in interactions among household members and with devices stretches the divisions of labours and reflects everyday concerns. Privacy is not a concern explicitly oriented to but implicated in the social goals and values that underpin everyday interaction. Across a fluid division of labour, roles and rules assume particular social functions that are different from their use in system design. These insights contribute to the field of sociology of

[1] e.g. https://uk.pcmag.com/smart-home/85/the-best-smart-home-devices-for-2020

[2] As discussed in, e.g., [37], the authors note that a smart home landscape is in flux with differing device capabilities, modalities, and eco-systems across manufacturers. We also note that some smart devices offer multi-user functionality.

technology, usability and privacy research in HCI, development and use of access control mechanisms in system design, and implications for data protection legislation.

A Research Approach to Everyday Technology Use – Our grounded analysis as motivated in Section 3.2.2.2 and implemented in Chapter 5 is informed by sensitising concepts from Ethnomethodology (EM). The quality of our findings has made evident its power in analysing reports and observation of *in-situ* interactions and grounding challenges of communal use in everyday interactions. The approach can, for example, inform future HCC research and the use of EM and Grounded Theory (GT) in social research more broadly when applied to different cultural contexts or other kinds of technologies.

The Conceptual Framework "Communal Privacy in Smart Homes (CoPriSm)" The present research has contributed a conceptual and descriptive framework CoPriSm that facilitates privacy empowerment through innovation in design and research. The framework complements the everyday perspective of interactions with an agentic view—a perspective favoured in related disciplines of system design and data protection legislation. In highlighting three principled ways for empowering communal use by design (community members manage, technologies enable, and information is embodied) and linking them with active research areas, the research has contributed to design practices and research in HCC in the following respects: (1) a design thinking process provides guidance for user experience and system design efforts; (2) the framework can be used to understand requirements of new artefacts; and (3) the framework can serve as a 'boundary object' [39] for interdisciplinary discussions. Demonstrating the use of Responsible Research and Innovation (RRI) in constructing the framework, we highlight the need for responsible innovation in empowering households, suggesting an RRI process be used alongside the design thinking approach.

Low Fidelity Prototypes as Design Interventions – Chapter 7 presents two low-fidelity prototypes resulting from design thinking processes with CoPriSm framed by an RRI approach. The chapter also demonstrates the value of an RRI approach to anticipate, reflect, engage, and act when innovating with CoPriSm. It highlights that

ethical considerations of empowerment must not be seperated from design challenges of communal use.

Theoretical Contributions to Research and Practice in HCC – Chapters 6 and 7 have contributed toward ongoing academic debates on privacy in HCC and cybersecurity. The discussion highlights the strength of designing for social negotiations to foster purposeful device use. It postulates that negotiated goals and purposes offer opportunities to reconcile the GDPR's 'purpose limitation' with everyday concerns of interactions. Normalising social negotiation also addresses the issues of interpersonal power imbalances such as 'function creep' [40] or the 'blank slate' [7] problem. We also highlight how conceptualising communities of users as manifested in proxy relationships can overcome analytic privacy dilemmas (e.g., who should have what level of access), suggesting that proxy relationships present opportunities in which household members empower one another with support from design.

1.5 Thesis Outline

The structure of this thesis is depicted in Figure 1.1. The literature review in Chapter 2 draws on the subfields of HCI and CSCW to identify a gap in the literature on privacy in smart homes, particularly in light of interpersonal and informational privacy illustrated in terms of the two power imbalances mentioned above. The review not only identifies and motivates the three main research questions but also notes the power of inductive, exploratory, and observatory research approaches evident in prior contributions. Based on these insights, Chapter 3 reviews research strategies to identify, motivate, and justify the research design of this thesis. Following a four-step process, the findings chapters seek to *explore, unpack, inform, and empower* privacy in connected homes.

Chapter 4 *explores* technology use in the home using inductive thematic analysis of semi-structured interviews to outline the ways in which technology use in the home is communal. The chapter notes that privacy is rarely explicitly oriented to but implicated in concerns of everyday use. These insights motivate the ethnomethodologically informed study of six households' experiences with smart technologies in Chapter 5 where the grounded analysis leverages EM sensitising concepts to *unpack* the

social organisation of communal use. The chapter provides a framework of the social organisation of communal use, highlighting interactions between household members that reflect the dynamics of everyday use and related concerns that at times manifest in the articulation of social roles and rules. It also highlights the relationship between previously reported challenges of communal use (e.g., power imbalances) and the social organisation and the nature of smart technologies itself. Again, privacy is rarely directly oriented to but reflected in mundane, everyday concerns. Chapter 6 identifies the need to inform innovation in research and design in order to empower households' privacy. The chapter not only acknowledges the uncertainty around outcomes of innovations that can work to empower or disempower households but also motivates the use of the RRI framework to guide efforts in research and innovation. To this end, the chapter expands on the social organisation of communal use by providing CoPriSm—a conceptual framework that complements the hitherto interaction-focused perspective on communal use with an agentic view. It relates to prevalent research and design perspectives in HCC to motivate interventions where community members are managed, smart technologies enabled, and information embodied. Proposing a design thinking approach, the chapter highlights the relevance of these perspectives and the opportunities they offer in empowering privacy through innovation. Because the effects of such interventions are hard to anticipate, the chapter suggests framing research and design efforts with CoPriSm using RRI. Chapter 7 evaluates CoPriSm in two case studies, including the review of existing and the creation of new interventions in public policy, research in HCC, and system design. The chapter draws on insights from these case studies and previous findings chapters to highlight the relevance of our work and the benefit of RRI in addressing the two power imbalances. In concluding this thesis, Chapter 8 summarises our research efforts and offers opportunities for future investigations.

1.6 Publications

The following publications arose from this thesis. First authorship implies efforts for research planning, data collection, data analysis, and write-up. Where content of a chapter has previously been published, this is highlighted at the start of the chapter.

- Martin J Kraemer, Ivan Flechais, and Helena Webb. “Exploring Communal Technology Use in the Home”. In: *Proceedings of the Halfway to the Future Symposium 2019*. HTTF 2019. Nottingham, United Kingdom: ACM, Nov. 2019
- Martin Johannes Kraemer, Helena Webb, George Chalhoub, and Ivan Flechais. “"It Becomes More of an Abstract Idea, this Privacy" - Informing the Design for Communal Privacy Experiences in Smart Homes”. In: *SSRN Electronic Journal* (2022), ***under review***
- Kraemer, Martin J., Helena Webb, and Ivan Flechais. “Innovating for Privacy in Communal Use: A Research and Design Framework”. In: (2022), ***under submission***

The researcher contributed to the following publications that are not part of this thesis.

- M.J. Kraemer and I. Flechais. “Researching Privacy in Smart Homes : A Roadmap of Future Directions and Research Methods”. In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. Institution of Engineering and Technology, 2018, pp. 1–10
- Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. “Further Exploring Communal Technology Use in Smart Homes: Social Expectations”. In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI EA ’20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–7
- William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. “Informing the Design of Privacy-Empowering Tools for the Connected Home”. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI ’20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–14
- Martin Kraemer. “Beyond the Individual: Exploring Data Protection by Design in Connected Communal Spaces”. In: *2020 USENIX Conference on Privacy Engineering Practice and Respect (PEPR 20)*. USENIX Association, Oct. 2020
- George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. ““It Did Not Give Me an Option to Decline”: A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products”. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI ’21. Yokohama, Japan: Association for Computing Machinery, 2021

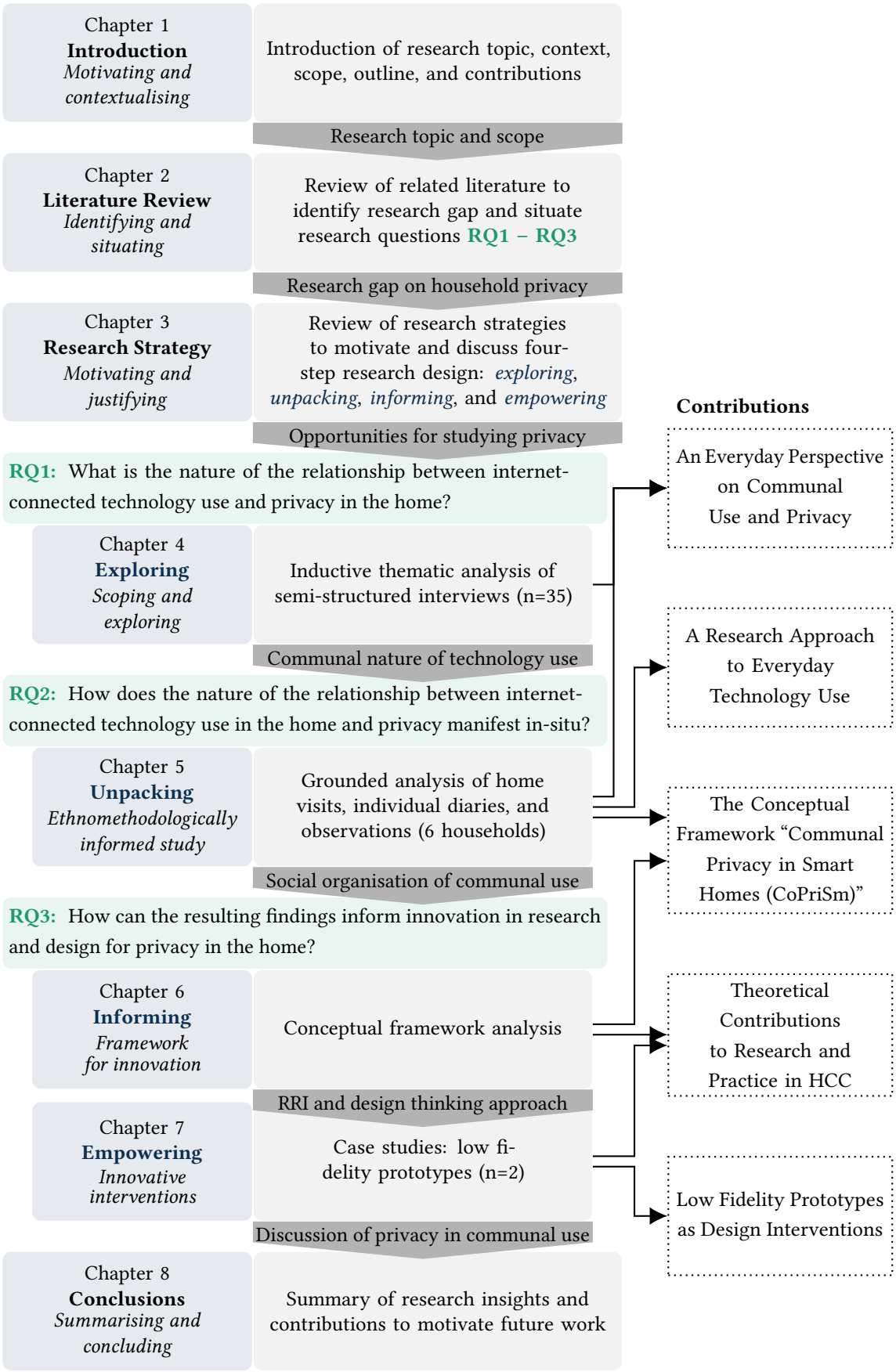


Figure 1.1: Thesis overview with research questions, research methods, and contributions

2

A Literature Review of Privacy in the Connected Home

Contents

2.1 Introduction

The research questions introduced in the previous chapter (main research question: *How can households living in connected homes be empowered in their privacy?*) motivate the literature review presented in this chapter. Situating this work in the interdisciplinary context of HCC, the review characterises privacy as a philosophically contested socio-technical phenomenon constituted in contemporary legislation and regulation. It further characterises the contested phenomenon of privacy in light of theories from sociology, information sciences, and media studies, highlighting conceptualisations of networked privacy from HCI and CSCW. Across these disciplines, privacy is understood as situated and interactional in character, bringing forth normative considerations that call into question teleological aspects of interactions. These socio-technical facets of privacy motivate a review of system design approaches that can serve to not only understand the concept and empower users but also reflect the contested nature and value of privacy. The chapter identifies the home as a community in its own right and therefore a complex and highly dynamic socio-technical research context for privacy in HCC. With regard to the two power imbalances that motivate this thesis, the chapter finds further evidence in related literature from HCI and CSCW on technology use and privacy in connected homes. This chapter therefore highlights a research gap in HCC across subfields of HCI and CSCW that needs to be filled in order to empower households in their use of smart technologies at home.

2.2 Privacy

A concept in disarray [49] and a multifaceted problem that changes and evolves over time, privacy has long posed complex challenges for system design [50]. This section provides a brief overview of research developments.

2.2.1 A Brief History

Scholars have argued that the origins of privacy can be traced back to medieval [51] and even ancient times [52, 53]. During these times, bedrooms and houses respectively emerged as places of retreat, and social norms around the meaning of these spaces evolved. The phenomenon of privacy is social in nature, and not a set of "psychological primitives" [51]. While the concept has been borne out of considerations of space, DeCew and Zalta note "there remains confusion over the meaning, value, and scope of the concept of privacy" [54].

Indeed, the concept has radically developed since the late 19th century when mass media and photography changed the information landscape, and Warren and Brandeis published their seminal work "The right to privacy" [55] in the US. The authors' aim was to find provisions in existing law that would afford an individual's protection from unwanted interference by other individuals. They argued that such provisions existed as the right to life, the right to freedom from physical restraint (liberty), and the right to property. Recognising that the scope of these rights had already broadened to include "man's spiritual nature", the authors argued for "the right to be let alone" [55, p. 193]. They thereby proposed the principle of "inviolate personality" affording protection of tangible and intangible possession [55]. This notion of informational privacy by Warren and Brandeis has laid the groundwork for privacy in US legislation [49, 56].

The interdisciplinary debate over a right to privacy and the nature of privacy itself is ongoing (e.g., [49, 54, 57]). One prominent interpretation building on the "right to be let alone" [55] is 'privacy as control over information' [54, 55, 58]. Following this view, privacy is understood as individuals' ability to control which information about oneself is communicated how and when to others. Alan Westin explored this interpretation in

his works (e.g., [59]) to inform policing of information technology, thereby sparking debates in related disciplines of system design and human-centred computing.

2.2.1.1 Legislation

Today, changes in US privacy law follow the principal of harmful intervention [60]. Some scholars have argued that the resulting US case law essentially encourages self-regulation, and personal information is often readily available as a consequence [61]. The landscape of privacy legislation in the US has therefore been described as patchwork and limited [54]. While sector specific legislation exists (e.g., the Health Insurance Portability and Accountability Act of 1996), universal approaches to data protection are in their infancy (e.g., the California Consumer Privacy Act [62]).

Legislation in the European Union has followed an alternative approach, protecting consumers and individual privacy against economic interests of large corporations [63]. The goal of the EU's GDPR—adopted as Data Privacy Act 2018 in the UK—is to protect values at the core of the fundamental and individual right to privacy in many modern societies, i.e., human dignity, liberty, and autonomy [64]. While the GDPR is focused on data protection and privacy as individual rights, the California Consumer Privacy Act 2018 [62] notably includes *households* as consumers from whom personal data can be collected as protect-worthy. In the EU, households are not considered data subjects and neither are individual household members considered data controllers [65].

2.2.1.2 Guidelines and Regulations

Over the past 30 years, ever-growing concerns of mass surveillance have accompanied the emergence of internet-connected technologies. Policy makers have addressed these concerns over the years through rules for data collection, processing and storage such as the guidelines by MITRE corporation and the National Institute of Standards and Technology (NIST) [66] or the Fair Information Practice Principles (FIPP) and Privacy-by-Design [67, 68]. The GDPR codified these rules as data protection principles which are to be observed by design and by default. The legislation constitutes a shift in legal

responsibility for data protection from the individual to the data controller who need to make their practices accountable to users.

While these laws and regulations favour an understanding of informational privacy as concern of understanding the implications of data collection, processing, and storage on an individual, data protection legislation "originates from the right to privacy and both are instrumental in preserving and promoting fundamental values and rights" [64]. While this relationship with the wider concept of privacy might need not be considered from a compliance perspective, it warrants attention from those wishing to truly empower their users.

2.2.1.3 Nature and Value

"Preserving fundamental [privacy] values and rights" [64] remains a difficult task. The contemporary scholarly debate on privacy is driven by different views on its nature (state or right), its value (individual and society), and how 'better' privacy can be achieved. Researchers from legal, sociological, and information/media science put forward different understandings of privacy to explain preferences, concerns, decision-making, and human behaviour.

There is a disagreement among scholars whether privacy is a right or merely a state. DeCew and Zalta [54] summarise important philosophical contributions. According to them, if privacy is a right, then it needs to be understood as moral and normative. If privacy is a state, then its nature is descriptive. Those who subscribe to a normative and moral account arguing for the value of privacy in western-style democracies either promote the understanding of a personal state or endorse the idea of privacy supporting other values (e.g., autonomy or freedom of speech).

While privacy sceptics argue that privacy does not exist, the value of privacy for society has been widely accepted [54]. Nissenbaum [21] discusses the value of privacy for autonomy, social relationships, and society. In relation to privacy, autonomy is seen as conceptual (e.g., self-presentation [69] and identity formation [70, 71]) and causal (e.g., effects on agency in consideration [72, 73] and action [74]). Similar to the formation of autonomy, privacy provides value for social relationships by enabling "respect, love,

and trust" [75], and according to Goffman [70] to maintain relationships [76]. Regan [77] sees the value of privacy for society as (1) common (freedom of speech, religion, association), (2) public (importance for democratic institutions), and (3) collective (regulated marketplaces).

2.2.2 Privacy Theories

A number of theories and perspectives have shaped academic research and debates in HCC. However, lack of consensus on the nature and value of privacy is reflected in a number of coexisting privacy theories as well as disagreement over the trustworthiness of the research they informed. Consequently, the debate on how to achieve 'better' privacy is convoluted.

2.2.2.1 Privacy as Control over Information

A line of argument predominantly used in the context of socio-technical systems builds on 'privacy as control over information,' in which privacy is often interpreted as a state. In this view, information flow controls and user access controls are often considered the panacea of privacy and security employed to empower the user [21, 54]. There is a myriad of computer science system research subscribing to this understanding (e.g., [78–82]).

The Privacy Paradox This perspective continues to face the challenges of explaining the *privacy paradox* [21, p. 103]—a perceived dichotomy of attitude/preference and behaviour. Starting with Westin's [59] privacy classification, researchers from various fields have investigated user preferences and behaviours. For example, Acquisti, Brandimarte, and Loewenstein [13] have addressed policymakers' discussions of the impact of users' uncertainty, the power of data holders, and the context-dependency of privacy. Calling for a synthetic, metamodel, Kokolakis [83] have provided a comprehensive review of literature on the paradox, making contributions spanning behavioural economics (privacy calculus), psychology (cognitive biases and heuristics, bounded rationality, incomplete information), and information systems (information asymmetry). Other reviews have focused on specific systems. Barth and Jong [84] have, for instance, concluded

that mobile computing required faster decision-making, rendering the paradox more complex. The internet of things and privacy has been reviewed by Aleisa and Renaud [85] who built on Ziegeldorf, Morchon, and Wehrle's [86] application of Westin's [59] categories. Finally, Smith, Dinev, and Xu [80] have argued for the need of an overarching, context-neutral framework based on an investigation of privacy behaviour outcomes.

While there are those espousing the paradox, many have denied its existence or claimed solutions. Hill, Fishbein, and Ajzen [87] have highlighted the differences between generic attitudes and specific behaviours in attempt to invalidate research approaches trying to compare both. Researchers have documented how users showed resignation because they felt disempowered [88, 89], followed the sharing behaviour of their social group [90] or failed to act appropriately due to lack of social representation [91]. Under certain circumstances, the paradox has been dissolved using privacy calculus [82] or the Theory of Planned Behaviour [92].

These approaches have aimed to explain behaviours by modelling the context, assuming that privacy was a state people desired to achieve under a specific set of circumstances. A similar orientation has inspired the creation of many privacy controls such as permission settings in smartphone or notice and consent forms. While these efforts have gradually improved peoples' ability to manage privacy by contextualising decision-making, they have also revealed further problems (e.g., assuming users' ability to comprehend an analytic concept and act accordingly, which depends, however, on effects of personal characteristics [93] or socio-demographic differences [94]).

2.2.2.2 Privacy as Boundary Work

Privacy as boundary work has its roots in sociology where scholars describe the ways in which individuals influence interactions with their environment. Goffman has considered the self as co-constructed within its social environment, that is, individuals are inescapably exposed to social and cultural influences. When entering the front stage (a social situation), individuals have limited influence over the emergence of their "performed character's self". In the eyes of an audience, "the self is a product of all of these arrangements, and in all of its parts bears the marks of this genesis" [70, p.2 53].

Altman's understanding of *privacy as dialectic process* as dynamic boundary regulation process has been used to explain behaviours of information disclosure [95]. The process of boundary regulation refers to individuals who manage their privacy with groups constantly to achieve desired levels of social contact. Contrary to Goffman, Altman ascribes more agency to individuals. In "The environment and social behavior", Altman argues for privacy as the key concept to understand the relationship between behaviours and the physical and social environment [96]. To Altman, privacy is regulated through an optimisation process. An individual can have either too much or too little privacy, and frequently enters situations to concede or retain privacy. Privacy is functional in serving: "(a) control and management of interpersonal interactions, (b) plans, roles, and strategies for dealing with others, and (c) features of self-identity" [95, p. 12].

While the theory has been influential in scholarly debates across disciplines (e.g., in HCI [89, 97]), it has also remained fairly abstract and general, thereby requiring further appropriation by researchers [98]. For example, because Altman's theory predates the internet age, researchers have struggled to consider power imbalances between users and manufacturers as part of the self-regulation process (e.g., power imbalances brought about by meaningless choice controls [99]).

Inspired by Altman's theory [100], Petronio's Communication Privacy Management theory (CPM) states that disclosure of information is based on five principles: ownership, control, privacy rules, shared ownership, and boundary turbulence. CPM argues that people base their disclosure decisions on a rule-based management system with rules being negotiated on disclosure. If expectations of managing shared information do not align, 'boundary turbulence' or feelings of distress occur. However, CPM has been successfully applied to researching power imbalances between users and manufacturers (e.g., [101, 102]). One criticism for CPM is its descriptiveness, slow response to privacy turbulence, and lack of guidance and forward-looking anticipation.

These theories highlight the interactional character and situatedness of privacy. Note that we use 'situated' as opposed to 'contextualised' since none of these theories attempt to fully articulate context to predict privacy behaviours.

2.2.2.3 Privacy as Contextual Integrity

One theory that is both descriptive and forward-looking is Nissenbaum's [21] privacy as *Contextual Integrity* (CI). In this theory, CI is preserved if new systems follow existing context-dependent *informational norms*. Informational norms

> regulate the flow of information of certain types about an information subject from one actor (acting in a particular capacity, or role) to another or others (acting in a particular capacity or role) according to particular transmission principles [21, p. 141].

Furthermore, context is understood as

> structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes) [21, p. 132].

In capturing norms, CI is powerful in anticipating peoples' attitudes toward the use of new technologies in established contexts. However, where established norms conflict with data flows introduced by new technologies, context-sensitive informational norms are violated and contextual integrity is lost. Since the goal is to uphold contextual integrity, the theory appears conservative in nature, or what is also referred to as *tyranny of the normal* [21]. To identify situations in which a breach of context-sensitive informational forms is acceptable, Nissenbaum offers *moral legitimacy* as a solution. If the breach of existing informational norms is deemed politically or morally superior, it might still be put in place. Practices "supporting, achieving, or promoting relevant contextual values" [21, p. 166] are considered superior. Broadly speaking, if the novel systems serve the goals of the context, realising these goals need not align with the consumer's goals.

CI has been applied successfully in various research contexts, from eliciting user preferences with regard to information flows (e.g., [103]) to informing system engineering (e.g., [104]). Barkhuus [20] has applied CI to suggest the use of different vocabularies for investigations of privacy. They have found that using privacy can potentially blur the discussion by invoking many different interpretations of the phenomenon.

2.2.3 'Networked' Privacy

While the theories discussed above recognise privacy as inherently social and interactional, they focus on privacy behaviours and preferences from an individual perspective. An array of privacy-themed workshops at CHI and CSCW have discussed the gap between academic research and industry solutions for privacy-by-design [105], the development of privacy design heuristics [106], collaborative privacy [107], interpersonal privacy for networked settings [108], and networked privacy [109]. To accommodate co-produced or shared data (e.g., pictures in social networks showing several individuals), researchers have coined terms to describe practices and approaches considering privacy beyond the individual [110].

First, the term *group privacy* considers actions of other individuals surrounding a person such as at home or in public places [111]. The term has since been adopted in differential privacy where groups are of latent or apparent nature [112, 113]. More closely related to users' privacy practices and their interactions are the following terms: *collective privacy* refers to the collaborative management of privacy settings [114]. For example, researchers have used contextual integrity to highlight a shared understanding of appropriate information flows [115–117]. *Networked privacy* considers data sharing practices in the age of social media. Boyd [118] advocates considerations of managing usage and interpretation by others where full control becomes infeasible. A related issue is sharing social media accounts among household members, which requires coordination of communication with the outside world [119]. Similarly, *interdependent privacy* relates to effects of others' sharing practices on individuals in online social networks [120]. The term *privacy stewardship* refers to parents' responsibility for their children's online presences, holding family and friends accountable to their standards [121]. In the internet of things, *interpersonal privacy* shifts focus towards peoples' sense-making of multi-subject data created by multiple people using the same device actively or passively [122]. In similar vein, *multiple subject privacy* simply describes personal data that apply to multiple individuals [123].

These different notions of privacy beyond the individual demonstrate the complexities of the problem space, emphasising the entanglement of privacy with social and

cultural considerations. The contributions discussed in the previous paragraph consider common goals, shared data (or shared inferred information), shared access to devices and accounts, a shared sense of community across online and offline spheres, physical proximity with other people, and feelings of duty of care for others.

2.2.4 Summary

The concept of privacy in academic literature is debated in terms of its nature (state or right), value (individual or societal), and how privacy can be better achieved. Privacy as 'control over information' (considering privacy as a state) is the predominant interpretation adopted by the current legislation for system design, though the purpose of data protection to provide for privacy (in the wider sense) is highlighted. Existing privacy theories highlight the interactional character, situatedness, and teleological orientation of actions that bring about normative aspects of privacy. Interpersonal notions of privacy ('networked' privacy) emphasise how privacy is entangled with social and cultural considerations.

However, the lack of consensus with regard to the nature and value of privacy is evident in a number of competing privacy theories and perspectives in HCC. Relatedly, there is disagreement regarding appropriate research approaches and the trustworthiness of findings they yield. The key aspect of these debates in HCC is the role of system design which is reviewed in the next Section.

2.3 Design and Privacy

Design is difficult to define. It is the creation of an experience, the process of that creation, and the result [124]. American designer Charles Eames said, "design is a plan for arranging elements in such a way as best to accomplish a particular purpose" [124]. Sociologist and early HCI researcher Herbert Simon described design as devising "courses of action aimed at changing existing situations into preferred ones" [125, p. 111]. Today, the concept of design in HCC refers to a broad range of different practices. These practices serve particular design goals and are based on assumptions over how to meet them. This section discusses how some of these practices are carried out by system

designers, user experience designers, or interaction designers. It highlights their value for privacy design and identifies their shortcomings. Given the importance of the politics of design when designing for political outcomes, Wong and Mulligan [126] identify five different design approaches in which purposes, design politics, and the relationship to privacy are described [126].

Redesign, reappropriation, and resistance approaches are employed to solve problems, critic the present, and propose critical alternatives. Their premise is to treat privacy as a contested concept that does not resonate with "needs, beliefs, and lived experiences of stakeholders" [126]. Speculative and critical design research proposes to consider futures in which specific design objects exist. These artefacts serve as 'boundary objects' to facilitate discussions over values, practices, and politics implicated in systems and their developments.

While we do not question the potential of these approaches to understand and empower privacy, our concern is with an everyday perspective on privacy interactions. We are not so much interested in criticising and redefining conceptualisations of privacy (arguably none is appropriate for the context of the home as we discuss later) as we are in understanding how current issues associated with privacy (e.g., the two power imbalances) relate to the use of technology in the home. Investigating these issues through perspectives of systems and software engineering, user-centred design, participatory engagement, and value-centred design is therefore more suitable.

2.3.1 Software and systems engineering

System architects and software/systems engineers typically start with a well-defined understanding of privacy grounded in laws and theories of privacy. This understanding informs engineering requirements addressing access control mechanisms or other privacy enhancing technologies.

Privacy by design has mostly been approached by emerging practices and research in privacy engineering. The field has a strong policy and engineering focus, aiming to translate regulatory guidelines and requirements provided by standardisation bodies into engineering practices [126, 127]. For example, Spiekermann and Cranor

[128] identify three different approaches including architecture, policy, and interaction. Danezis et al. [129] have also proposed design strategies while Kroener and Wright [130] have linked engineering best practices with privacy impact assessment and privacy enhancing technologies to make privacy-by-design goals verifiable and measurable. Best practices have been provided by the MITRE corporation and the National Institute of Standards and Technology (NIST), emphasising the importance of privacy risk evaluation to "achieve freedom from conditions that can create problems for individuals with unacceptable consequences" from processing personal information [66]. These guides advocate for risk modelling to identify and mitigate privacy and security threats. Prominent frameworks that inform risk modelling through identifying privacy goals include design principles, Solove's taxonomy of privacy harms [131], and privacy theories such as contextual integrity [21]. These approaches have been criticised for their 'check-list' character [132], and design perspectives in research and practices have been considered narrow in their focus on privacy as control over information of an individual [126].

2.3.2 User-centred design

User-Centred Design (UCD) is a process often employed by designers in HCI to solve a specific problem or to support and inform privacy decision-making. UCD has also been used to explore privacy with and for people in specific situations. The approach has emerged from cognitive science and human factors (1st and 2nd HCI paradigms [133] – see also Section 3.1.1). The underlying assumption of UCD is that systems that are "more usable or better align with users' expectations of privacy" [126] result in people making more privacy-preserving decisions.

Having been at the heart of HCI for decades, this approach has informed improvements of privacy notices (e.g., [134, 135]), privacy policies (e.g., [136, 137]), and other choice controls. Researchers have generally aimed to align mental models with system design, improving on usability and efficiency while at the same time reducing the cognitive burden. Researchers have also frequently elicited users' expectations (e.g., [138]), drawing on theories such as Norman's [139] gulfs of evaluation

and execution to highlight necessary improvements. This approach focuses on an individual's "understandings, preferences, and behaviours related to privacy that affect their ability to control personal information" [126].

2.3.3 Participatory Engagement and Value-Centred Design

Considering privacy as a property of context (social, cultural, and institutional), users, and stakeholders, these two approaches have been used to build systems that solve privacy problems or inform and support privacy decision-making by engaging stakeholders, lending themselves to exploring "the relevance of privacy to people and situations" [126]. Motivated by the need to overcome a narrow view on privacy as a compliance issue, Luger et al. [140] have developed ideation cards to facilitate discussions on data protection and privacy with designers.

Participatory design (PD) as a practice has been applied across research contexts (e.g., workplace, design environment, or workshops) [141]. Shilton et al. [142] have employed PD to engage participants in meaningful negotiations of social context as an important part of privacy. Mir, Shvartzshnaider, and Latonero [117] have proposed contextualised participatory privacy by design as an approach informed by contextual integrity that aims to "empower communities in negotiating and articulating their privacy norms". Yao et al. have employed participatory design to explore privacy perceptions and designs of smart home owners [144] and bystanders [143].

Ethnographic studies have also been influential in providing novel ways of understanding privacy. Crabtree, Tolmie, and Knight have attested to a concern of relationship management (not with privacy) across digital and social worlds implicated in an "array of methods to manage the potential attack surface of the digital on everyday life" [145]. In these ways, people manage "accountability in the sharing of personal data" and minimise "intrusions into everyday life from the online world at large" [145]. In "Rethinking Privacy", Dourish and Bell have found "effective privacy protection cannot be 'grafted onto' a system because it is a pervasive aspect of how that system is designed" [146]. They argue for a perspective of collective information practices that considers which "information should be shared, managed, and withheld" [146, p. 159].

These practices are not about privacy but social actions, deriving meanings from other "concerns for risk, danger, trust, secrecy, identity, morality, and power" [146, p. 159]. Information practices (and privacy) cannot be separated from these concerns.

To align with this design orientation, privacy needs to be a "pervasive aspect" of system design. Researchers, then, propose holistic approaches that challenge designers to rethink privacy; for example, approaches that support the ways in which people manage relationships in the digital and social world when interacting with devices.

2.3.4 Summary

The review of literature on privacy highlights how the concept of privacy has changed and evolved over time. This section reviewed different design approaches to highlight their relationship to privacy. Risk-based engineering approaches (largely adopted in privacy engineering) have been criticised as too narrow to fully consider these notions. User-centred design focuses on individuals and their ability to control personal information. However, researchers argue for privacy to be a pervasive aspect of a system, not 'grafted' onto it. Because of its pervasive nature, a discussion of privacy may invoke multiple interpretations of the word, thereby hindering, rather than helping, research investigations. These interpretations are also reflected in other ethical concerns that are inseparable from privacy.

Social considerations such as trust and morality cannot be separated from privacy but should be equally reflected in the meaning of practices around systems. Privacy by design needs to be facilitated by approaches that focus on practices and interactions allowing for considerations of privacy as a "pervasive aspect" of design rather than those that define privacy from the outset. Thus, designing a system to empower users requires more than the expertise of a system architect or software and systems engineer. The discipline of design offers the required methods and approaches, but the work of user experience designers is also needed. They carry out user research to inform visual design, information architecture, interaction design, usability, and content strategy.

2.4 'The Home'

The home as a research context poses particular challenges for system design and privacy. The social dynamics of the home have challenged design patterns, methods, and even tools initially developed for work environments. For example, a power imbalance between users is considered unwelcome in the home but an established norm at work. At the same time, the home is considered one of the most private spaces as it foregrounds several privacy-related considerations such as the right to be let alone and free from external power and influence or the right to informational self-determination. We begin to unpack such complexity in this section.

2.4.1 Households as Moral Economies

A value-laden and meaningful place for people [147], the home is a place that provides 'ontological security' for its inhabitants, a sense of confidence that the world really is as it appears [148]. An important question becomes: 'who is participating in "being-at-home, creating or making home" [147]?'

In our contemporary society, *the* family or *the* household cannot be defined. Different forms of family (e.g., 'traditional', same sex, or single parent) and cohabitation (e.g., married couple, cohabiting couple, lone-parent household, shared accommodation/multi-family, one-person households) have evolved over the past decades. Definitions of cohabitation in traditional sociology literature which refers to a couple "living together in a sexual relationship without being married" [148, p. 234] are no longer accurate [149].

> This idealistic notion of a 'typical' traditional family is somewhat mythical, and in contemporary society a range of different family types exist. [150, p. 454]

The concepts of family and household cannot be used interchangeably. Households are "groups of people sharing common facilities" [151]. In households, awareness of each other's times and schedules contributes to a sense of identity. Much of this household life requires constant negotiation and coordination, particularly between adults [152]. Through this ongoing coordination and negotiation, households establish routines that accommodate for the complexity of life in the home [153]. Because

households "possess a tradition, a moral order which frames and guides behaviour as well as the use of household facilities and technologies" [154], they are called communities in their own right. In this sense, household members can also be called *community members*. In this work, we use household to refer to a group of people inhabiting the same (physical) place. This includes, but not limited to, couples (inclusive of any sex and gender), single-person households, flat sharing, temporary sub letting, and other forms of lodging.

2.4.2 Households as Communities

The literature offers a myriad of definitions of communities (e.g., [155]). Communities are characterised as having common residence, common interest, common identity, or any combination of these factors. While members of communities synchronise their activities to allow people to come together, they are dynamic and people participate with varying degrees of involvement over time [156]. Membership of a community, then, is to some degree exclusive (thinking of insiders and outsiders). In fact, the discussion is fundamental to sociology as evident in early controversial debates between a German sociologist, Tönnies, and a French sociologist, Durkheim, on the nature of communities and societies (or "Gemeinschaft" and "Gesellschaft" in German words) [157]. The debate has evolved around the questions of whether societies are organic in nature or artificial, and what the nature of the continuum between societies and communities is. While Tönnies has conceived "Gemeinschaft" (community) as a theoretical/ideal type (differing from actual/real types), its characterisation in roles, values, and beliefs that take shape in interactions between members of a community is reflective of Silverstone, Hirsch, and Morley's [159] households as "moral economies" that inhibit a unique set of values, routines, and practices [154, 160]. Crucially, community members orient their actions to a common purpose whereas members of a society ("Gesellschaft") use others' expertise to meet their own goals [158].

This thesis defines households as "moral economies" that necessarily strive to share a set of values, routines, and practices so as to allow people to come together. Note that household communities consist of members that can be part of other communities, and that even the household itself can be part of a larger neighbourhood community.

Further note that each of these communities maintains its own moral economy, i.e., has its own moral order.

2.4.3 Moral and Social Order

Durkheim, the founding father of sociology, describes moral order as the expressed collective consciousness of society which relies on an established understanding of "shared goals, values, norms, and beliefs, about words, deeds, and actions considered 'normal,' 'right,' and those considered 'wrong'" [161, p. 5052]. It is difficult to discuss the nature of this social and moral order without getting into disputed territories in the social sciences, i.e., questions over the primacy of either structure or agency [162, 163].

From a phenomenological perspective, this moral order takes shape in everyday interactions ("moral concepts are embodied in and are partially constitutive of forms of social life" [164, p. 1]). The moral order as such is not a static construct but an inherently dynamic one [154]. Ethnomethodologists highlight that interactions that previously have demanded explanation ("moral order as perceivedly normal courses of action" [163, p. 225]) can later be considered naturally accountable and vice-versa. In this perspective, moral order is not an external structural entity that can exist in isolation but is 'reflexively' established in coordinated action: "we are talking of criteria, presuppositions, and understandings that operate as the constituents of action, but which reflexively, in the very conduct of social life, in the very particulars by which actions and settings are produced, are themselves reconstituted, reaffirmed, played out and made relevant" [165, p. 236]. As Goulden [166] summarises for the home, "the moral ordering [is] reliant on delicate, only occasionally explicit, negotiation of what is normal, what must be accounted for and what should be left unseen" [166]. Everyday concerns along the lines of 'being a good neighbour' or 'a great parent' as *social goals* are often implicated in moral order.

From an analytic perspective, moral and social order may constitute in different categories used to describe organisations and behaviours across different homes. In this perspective, social structures are often coloured by gendered roles, relationships, and power structures, e.g. [147, 167, 168]. Power structures within the home can be

seen in relation to domains of control. For example, the husband traditionally provides for the family while the wife stays at home to take care of the households and kids. This situation has introduced dynamics to household decision-making based on the role assignments (in the sense of who typically does what) [169]. Other domains of control have traditionally exhibited different power structures (e.g., housework [148, p. 218]). Deviating from these 'traditional' roles, responsibilities in the home have shifted while the underlying feelings of duty have remained (e.g., [170]). Power structures and roles are destined to remain a very dynamic construct. Scott and Clery [171] document a drastic change in gender roles and responsibilities in the UK over the past decades [171, p. 128] and conclude that roles and responsibilities will continue to evolve. Mikula et al. [172] have found similar distributions of the household work in mixed gender student households, even though time commitments and contributions to the household bursary were equal outside [172].

Whatever the nature of moral and social order in the home, there exist notions of 'right' and 'wrong', of appropriate conduct in relation to the needs, desires, and practices of others within and outside the home. While such notions are, perhaps, best described in abstract/categorical ways across households to help frame research problems or inform social policy, what these categories are trying to achieve is to capture fundamentally dynamic social phenomena by glossing over what might be involved in roles, what signifies relationships, and what makes for power structures on an everyday basis.

2.4.4 Summary

This section has introduced the home as a value-laden space where people 'allow' each other to come together. To this end, households can be regarded as moral economies that share a tradition, establish a moral order, and share facilities and resources. Households are then communities in their own right. These communities are 'organised' (and self-organise) in interactions between members, thereby establishing moral and social order. A better understanding of these interactions will help gain insights into related structural concerns such as gender influences or power structures.

2.5 Technology Use

Technology studies in the home gained more attention when the home computer became common during the 1980s. Since then, researchers in HCC have explored the use of connected technology in the home, with the advent of smart devices bringing about a new wave of research [173–175].

2.5.1 Domestication

Researchers have adopted the perspectives of technology adoption, appropriation, and domestication to study the relationship between households and their technologies. For example, Venkatesh [176] has explored households' everyday life in 'cyber space', providing the oft-cited quote on the 'dominance of the social':

> Don't assume that what the technology can do in the household is the same as what the household wants to do with the technology. [...] Adoption of technologies may be a socially motivated decision rather than a purely utilitarian decision. [176, p. 52]

Building on the technology acceptance model (e.g.,[177]), Venkatesh conceptualised social transformation as subject to usage patterns evolving through interaction at the intersection of technology and social space. These perspectives have eventually evolved to take environmental factors into account. For example, the process of domesticating technologies involves four stages: appropriation (acquisition of an object, revealing in possession and ownership), objectification (placement and usage practices), incorporation (used when, by whom, and for what purposes; situating in household's moral economy according to household values) and conversion (how devices are displayed to others in talk and action) [159].

Domestication theory describes the 'taming' of 'wild' technologies in the home. Households appropriate technology to suit their needs and routines, thereby embedding devices into social and cultural practices [178]. For example, Hargreaves, Wilson, and Hauxwell-Baldwin [18] characterise the process of domesticating technologies as continuously ongoing as household needs evolve. Household members carry out cognitive (knowing about technology), practical (learning how to use technology), or

symbolic work (integrating technology with lives and identities). When household members become users, they negotiate the use and navigate conflicts as routines change and evolve [18].

While domestication theory describes the work involved in appropriating devices, it does not describe effects of the introduction of technology on existing moral and social order in the home. A key question becomes whether users should accommodate for technology or technology should accommodate for their needs [179]. Existing moral and social order is challenged by the introduction of new devices to the home [154]. For example, a study by Harper et al. [180] reported that changes of usage practices of personal computers can influence the social structure in the home.

However, household members gradually appropriate devices in ways that 'work' for them, which are not necessarily the ways in which designers imagined their use. The 'dominance of the social' foregrounds the importance of considering social processes and somewhat refutes 'technocratic dreams' of successfully reforming society through 'technology push' [181, 182]. To anticipate how devices might be used, it is therefore pivotal to understand the social context in which they are embedded.

2.5.2 Everyday Interaction

The social embeddedness of technology use is unpacked in research that focuses on the establishment of social and moral order in the home. Researchers have highlighted how connected technologies become embedded in everyday interactions among household members despite the fact that these technologies can be unfitting at times (e.g., [183]). For example, Tolmie et al. [184] describe the home network as a shared resource that requires 'digital housekeeping', including locating the technology, managing access and security, managing digital media, and restoring when technology breaks down. Those carrying out the task are challenged with having to consider the moral order of the household [184]. Grinter et al. [185] have further illustrated efforts to make the home network accountable to the moral order by planning for change in balance with other tasks and responsibilities [185].

Crabtree et al. [16] have argued that the home network does not offer natural social accountability (in the sense of intelligibility or explainability [186]) while the use of the network has become necessarily unremarkable to household members. Households in their study establish a "presumptive set of differential rights", and inhabitants possessing these differential rights are "require[d] to [use] them when necessary" [16]. The authors stress that the use of home networks needs to become unremarkable [187] to better fit in with household routines.

Additionally, Crabtree and Rodden [153] have discussed how design can better accommodate the unremarkable nature of routines in the home. They characterise routines as situated courses of action such that the same course of action in a different situation might carry a different meaning. For example, what happens right before 'a knock on the door' signifies to members of a setting what might happen next, e.g. someone leaving the house or a parcel delivery arriving [153]. Crabtree et al. [188] have discussed the social nature of rules in the home, highlighting that rules are not prescriptive orders but "devices invoked to account for order" [188, p. 205]. The authors use this insight to explore design that makes the "network accountable to users and to enable user control" [188, p. 214].

These ethnographic studies of the home network provide valuable insights that sensitise design to the ongoing accomplishment of moral order in the home. We suspect that these insights on responsibilities (differential rights), rules, roles, and routines also become relevant to smart technologies that enter our homes. Design can benefit from these and other sensitising concepts.

2.5.3 Ownership, Power, and Control

Taken as analytic objects, rules, roles, and responsibilities have been used to highlight challenges of *smart* technology use in the home.

Household members who assume responsibilities of setting up and configuring systems can feel a burden of accountability towards their cohabitants [18]. Generally, the domestication of connected technologies has led to disagreement over purposes and goals of using devices [152]. This sometimes results in limited use or abandonment

of devices altogether [189–191]. Mennicken and Huang [192] have also reported how unfamiliarity among users can cause feelings of powerlessness and difficulties in getting high quality advice.

Power imbalances result where individuals hold privileges exclusively, exert more knowledge, or are more apt in their use of devices. In these situations, other users rely on their actions and good intentions [5, 193]. Perceptions of *ownership* that justify exercising privilege can contribute to these imbalances [7], allowing individuals to prescribe ways of using and holding others accountable for their use [34, 194]. For example, parents could hold their children accountable for their use of smart door locks [8]. An increasing body of anecdotal reports and research papers on the role of technology in intimate partner violence and domestic abuse illustrates how this power can be used without any regress, evidencing the severity and significance of this kind of appropriation [7, 195, 196].

Researchers have stipulated that these differences in usage might be brought about—or at least facilitated—by not only differing attitudes and preferences with regard to technologies [34, 197] but also through the design of smart devices themselves [25, 174]. Page et al. [197] have investigated differences in perceptions and adoption of smart devices between parents and their children. They report two somewhat opposing stances reflecting participants' expectations: a user-centric stance favouring control and an agent-centric stance appreciating device-driven behaviours (automation) in combination with control. Strengers et al. [25] have documented how interest in and uptake of smart devices are contingent on addressing gendered challenges. For example, the adoption of smart home devices can alter the "landscape of responsibilities" by requiring men to spend more time on 'digital housekeeping'. The same men therefore have less time to contribute to other (possibly traditional feminine) household tasks [198]. The authors argue for more "diverse expressions and performances of gender" to be considered by design. Rode and Poole [199] have also highlighted how gendered roles, responsibilities, and displays of technology ability are co-constructed between partners. An individual's choice to present or hide levels of agency in light of their self-identity becomes part of

this construction. At times, individuals might choose to downplay their own abilities to further the identity of their partner [199].

Having reviewed smart home users and their challenges, Wilson, Hargreaves, and Hauxwell-Baldwin [174] provide three different views on the smart home: functional, instrumental, and socio-technical. The authors highlight the importance of considering the users' values on the design of technologies, and Pierce [200] has extended this perspective of value to include manufacturers design politics (see also [166]). They suggest that research vocabulary must expand to include social and ethical issues [200].

2.5.4 Summary

The research contributions discussed in this section have highlighted how technology use in the home is necessarily and inseparably embedded in social and moral order. This process is not without its challenges. Through the act of design, devices carry the politics and values of their manufacturers. From an analytic perspective, processes of domestication are reflective of ethical issues including power, control, ownership, and gender. When these new technologies arrive in the home, household members work to domesticate them, thereby re-establishing local, moral, and social order that work with and around manufacturers' design politics and values.

2.6 Privacy in Connected Homes

This section reviews recent scholarly work on privacy in connected homes, touching on many of the insights presented in Section 2.2 and Section 2.5.

2.6.1 Individual Perspective

Apthorpe et al. [103] have used a factorial vignette survey based on Nissenbaum's [21] Contextual Integrity to discover informational norms in smart homes in the US. These norms represent a snapshot of the societal landscape of privacy preferences and attitudes (e.g., data use for advertising can violate informational norms; any data flow should support primary device functionality or familiarity; market penetration and consent broadly improve acceptability of information flows). With regard to communication

with third parties (e.g., manufacturers), research on smart home device use has shown that privacy is not a main concern of users because it is overruled by concerns for physical security [193] or trust in brands and convenience/connectedness [17, 191, 201]. Researchers have suggested unawareness—particularly with regard to data inference practices by manufacturers (i.e., incomplete mental models)— and a lack of appropriate controls as the reasons for poor privacy postures [17, 191, 193, 202]. However, Tabassum, Kosinski, and Lipford [191] have reported that even when participants are aware of threats and know about countermeasures, they frequently do not act (c.f. [203]). Instead, participants justify their inaction by classifying it as negligible risks because much (of their) data is already available on the web. The authors suggest that users should not only be better equipped with increased awareness and control but also informed about the implications of data collection [191].

Researchers have proposed several interventions to raise awareness, enable control, and educate users with respect to smart home technologies. Despite being a widely discussed and contested intervention [48], notice and consent is (by law) the minimum privacy protection that smart technologies offer. Because information on privacy is often difficult to locate and to understand, Emami-Naeini et al. [204] have proposed privacy labels on smart home products that inform users about privacy implications at the time of purchase. Jakobi et al. [205] have researched accountability and information needs from a user perspective, documenting shifts in information needs over time. They apply end-user-development iteratively and suggest that awareness mechanisms take into account shifting demands in information. Seymour et al. [46] have proposed a new class of privacy assistants that provides awareness of data flows, educates users, and provides control mechanisms. A recent line of research is concerned with the physical dimensions of awareness, considering new kinds of affordances and positioning of devices in the home [206]. While these interventions have been well received by participants and the authors have reported increased levels of awareness, knowledge, and control, the perspective of 'privacy as control over information' is unsurprisingly not without challenges. For example, questions remain with regard to

how much control is a good level of control, and how can data demands by companies and for devices be balanced against individuals' desire for privacy.

2.6.2 Beyond the Individual

Data collection, sharing, and processing fuels the development, innovation, and functioning of smart technologies. Without data sharing, many smart technologies cannot exist. The importance of data sharing is recognised by researchers proposing revised architectures of the internet. Initiatives like Databox [15] or Solid/Inrupt[1] have been proposed to enable users as economic actors that gain full control over their data. In the home, this is not without challenges because data may become interpersonal [122, 207]. While we believe this is a much needed shift, it also highlights the challenge of coordinating issues of privacy among different household members [15, 207]. This interpersonal perspective amplifies the challenges of privacy as control over information, warranting the need to accommodate for primary and secondary users, bystanders, and non-users [143, 208–212]. One important aspect is a power imbalance between different users in which those with more access than others can exercise power and control [5, 34, 193, 205, 213, 214]. This is even more so the case when those setting up the smart home only consider their own goals and values leaving others to use what is made available to them [215]. Proposed interventions for this interpersonal power imbalance include physical controls for bystanders ('tangible privacy' [211]), better access-control models [5, 213], multi-user support [214], and efforts to guide and restrict the actions of primary users [215].

To this end, much hope has been placed on access control as a means of control over information and a way to map interpersonal relationships in the home. For the smart home, researchers have proposed and surveyed models for particular cohorts inside and outside the home (e.g., [216, 217]). However, those who have field-tested more dynamic models highlight the implicit and social characteristics of regulating access. Access to devices and services is found to be socially managed rather than technically enforced [213]. Previously, access control has been reported to be intimately

[1] https://inrupt.com/solid/

"bound up with the subtleties of relationships" [160] and an "especially nuanced way of managing moral accountability" [16] within the home. This is also manifested in sharing behaviours. Researchers have found frequent everyday sharing of accounts and devices, suggesting that access control is not commonly used [194].

2.6.3 Summary

While the studies mentioned above provide valuable insights, there is still a lack of empirical and longitudinal studies that focus on household privacy in-situ [5, 205]. Prior research supports the need for 'in-the-wild' studies by highlighting complex relationship of privacy with other social goals (e.g., protecting the home [8] or being a responsible parent/good child [218]). Researchers have attempted to answer difficult questions like whose privacy to protect [143]; what "kinds of privacy demands are being made, in what circumstances, by whom, and why", and what users should be able to see about one another [205]; or how to design for positive household norms in ways that facilitate negotiation of device use and avoid conflicts [213]. These are important questions for empowering privacy in connected homes.

2.7 Conclusion

This chapter has reviewed literature relevant to this thesis. In so doing, it has identified and discussed a power imbalance among members of the same household and with service providers. The review also highlighted a lack of consensus over key issues of privacy such as its nature, value, and how it could or should be researched. From an everyday perspective, the two power imbalances are inseparable because data in the home becomes interpersonal. While there are extensive amounts of research on privacy issues between individuals and manufacturers, fewer studies have investigated issues related to privacy between members of the same household. Hence, our goal is to take both perspectives into account.

While the scholarly discussion on privacy is ongoing, challenging its nature, its value to society, and the means to achieve 'better' privacy, existing privacy theories have already provided some useful insights such as the interactional character, situatedness,

and teleological orientation of actions that bring about normative aspects of privacy. These facets require further unpacking in light of design politics and efforts. When considered for system design, privacy cannot be 'grafted' onto a system but becomes a pervasive feature of that system. Furthermore, privacy is inseparable from other ethical and everyday concerns that provide meaning to privacy 'behaviours'. Risk-centred approaches or privacy as control over information often fall short of accounting for this pervasiveness. There is much hope that observational and in-situ approaches like ethnographic approaches can provide the required new kinds of insights.

Considerations of values and social issues are part of a home's moral order which is constantly negotiated among household members. The complexity of privacy in the home is subject to its moral economy and moral order in negotiating shared resources and 'allowing household members to come together'. Interactions that constitute privacy in the home are inevitably part of this economy. A better understanding of these interactions can also yield a better understanding of analytic and structural concerns (e.g., issues of gender, power, and control). These concerns are interpersonal, reflecting also in design politics and values of the manufacturers entering the home embroidered in smart technology design. They influence the ways in which members of a household continuously establish moral and social order. Inevitably, they affect the actions that constitute privacy in the eyes of users.

The connected home, particularly the advent of smart technologies, offers a unique environment to research these issues. Novel devices exhibit design features that reportedly are perceived as particularly privacy invasive (i.e., causing discomfort, disapproval, or disbelief when learned about). These devices also enter the home 'community' (with its own moral economy). Based on these insights, we suggest refraining from any direct inquiry of privacy as a phenomenon but to focus on everyday interactions that allow us to capture what privacy means and is in the eyes of users. To this end, prior work has successfully employed exploratory and observational, inductive, and in-situ research approaches. We further suggest that a better understanding of interactions constitutive of privacy in the eyes of household members can enable design

to empower households holistically, that is, the power imbalances between users and eventually between households and companies are fully addressed.

The next chapter reviews research strategies on privacy in HCC to discuss and justify the choice of research strategy for this thesis. It outlines a process that seeks to understand household members' interactions in-situ in order to ultimately inform research and design that empowers privacy in the home.

3
Research Strategy

Contents

The literature review conducted in the previous chapter shows a gap in the literature on privacy in HCC. This gap is characterised in terms of two power imbalances in the home, one between manufacturers and consumers and the other among household

members. The latter is particularly under-researched and also described in relation to issues of privacy in interpersonal relationships.

Interactions of device use in the home are subjected to and become part of its moral order—the values and goals that are constantly negotiated among household members. The same values and social goals are also reflected in structural and analytic concerns such as issues of gender and power. The most recent wave of smart home technologies reflects these concerns in particular ways. For example, devices introduced to the home by a single administrator but used by many household members have design features that are perceived as privacy invasive.

In addition, the multifaceted nature of privacy, a concept that invokes different interpretations when inquired, has to be taken into account; and while there are attempts of grafting privacy onto a system, researchers point towards the advantages of considering privacy as a pervasive phenomenon of human-device-interaction. Particularly where no appropriate theory of privacy is available from the outset or existing conceptualisations of privacy can be challenged, the strengths of research approaches that are participatory, exploratory, and inductive play out [126]. Hence, researchers advocate considerations of privacy as a pervasive feature through longitudinal, in-situ, and practice-oriented investigations.

To empower home users, there is a need to investigate technology use in-situ. We also note that (often EM informed) everyday perspectives concerned with user interactions have provided strong, insightful contributions to the field. This chapter reviews research paradigms and trends in HCC to arrive at an appropriate research strategy.

3.1 Research Strategies

Technology use and privacy have been popular topics for both HCI and CSCW as subfields of HCC. This section therefore reviews the history of HCI as a field in its own right, trying to structure its roots, development, and projecting its future (e.g., [133, 219–222]). Note that this review also accounts for the 'turn to the social' that paved the way for the field of CSCW to emerge from HCI [223, 224]. Here we provide a cursory review (based

on [133, 222]) to point out key differences in methodological orientations, research movements, and types of contributions that become relevant for our research design.

3.1.1 Research Paradigms

Kuhn [225] has defined research paradigms as a set of problems under study, useful questions to ask about the problem, structured approaches suited to answer these questions, and a framing for the interpretation of results. While these criteria to identify research paradigms are well suited for the natural sciences, Harrison, Tatar, and Sengers [133] have suggested using Agre's [226] metaphors for research in HCI. Because metaphors encompass the breadth of different orientations in HCI research, paradigm shifts are better identified by shifts in the "underlying metaphor of interaction" [133]. Harrison, Tatar, and Sengers [133] argue that at the centre of each paradigm in HCI is a metaphor that describes:

> What phenomena constitute important descriptive qualities of interactions, what questions are interesting to ask about interaction, what methods are appropriate for studying and designing interaction and what validation procedures are required to establish knowledge claims about interaction.

While these metaphors bring different issues to attention, they also marginalise others and thus could be considered as co-existing and complementary rather than contradictory. Table 3.1 [133] provides an overview of these paradigms.

The *first* paradigm follows a metaphor of interaction as man-machine coupling. This paradigm was originated when engineers realised that users did not always follow anticipated and expected behaviours. Studies following this paradigm typically focus on issues that cause disruption. Harrison, Tatar, and Sengers [133] note that non-disruptive issues of usability are not typically considered by this paradigm.

The *second* paradigm of HCI stems from cognitive psychology. *Classical cognitivism/information processing* follows the understanding that human minds are essentially information processors, and therefore one can model information flows across human and machine. Harrison, Tatar, and Sengers [133] note that this was, at the time of their writing, a common line of thinking in HCI. Within this paradigm, researchers

Table 3.1: HCI research paradigms compared

	Paradigm 1	**Paradigm 2**	**Paradigm 3**
Metaphor of interaction	interaction as man-machine coupling	interaction as information communication	interaction as phenomenologically situated
Central goal for interaction	optimising fit between man and machine	optimising accuracy and efficiency of information transfer	support for situated action in the world
Typical questions of interest	How can we fix specific problems that arise in interaction?	What mismatches come up in communication between computers and people? How can we accurately model what people do? How can we improve the efficiency of computer use?	What existing situated activities in the world should we support? How do users appropriate technologies, and how can we support those appropriations? How can we support interaction without constraining it too strongly by what a computer can do or understand? What are the politics and values at the site of interaction, and how can we support those in design?

Table 1 in [133, p. 10]

typically wonder what information is available, how people make sense of the information, how this sense-making result in actions, and how relevant information can be communicated effectively [133]. Research in this tradition frequently talks about user awareness, increasing awareness and understanding, or understanding intention to drive actions. The paradigm has found wide-spread adoption in privacy research starting from Westin's [59] categories of users. However, this paradigm somewhat struggles to advance the debate on privacy beyond descriptions of situations in which privacy is lost. Researchers often highlight privacy's situated character, enumerating important contextual factors and highlighting paradoxical behaviour [83, 126].

Identified byHarrison, Tatar, and Sengers [133], the *third* paradigm in HCI spans a wide array of research approaches that include, for example, participatory design, activity theory, User eXperience (UX) design, EM, interaction analysis, and critical design. At its core, the third paradigm is concerned with understanding phenomena. This orientation has influenced how the findings and implications are presented by researchers. For example, an ongoing debate in HCI concerns appropriate ways to

provide generalisable and transferable findings from what appear to be highly subjective insights from the second paradigm's perspective (e.g., [227, 228]). This perspective has helped advancing the debate on privacy, highlighting aspects of a phenomenon that stretches beyond narrowly scoped definitions and preferred perspectives of specific research areas (e.g., informational privacy in data protection law [126, 143]).

As summarised in Table 3.2 [133], epistemological and ontological commitments between the second and third paradigms are fundamentally different. The premise of the third paradigm is to take a close-up look at situated actions to explain their meaning whereas the second paradigm favours an information-theoretic view ([229, 230] as cited in [133]). It becomes clear that these two perspectives are inherently and fundamentally different. Furthermore, the third paradigm also requires its own appropriate measures of evaluation. That is, a task-based evaluation is inappropriate when the nexus of an investigation is not to complete specific tasks. Instead, the third paradigm's contributions require cogent evaluations that closely tie collected data to a question under investigation.

The third paradigm has its own intellectual commitments [133]. In addition to the construction of meaning in interaction, the paradigm also widens the view on users as seen in their settings. It considers how design might accommodate context rather than how context influences actions. In considering situated meaning of interaction, it also emphasises the roles of researchers as co-creators of meaning and knowledge. Frequently, researchers explicitly consider values as embodied in design (e.g., gendered nature of technologies), and whilst theory is considered necessary, much of existing theories are inadequate. Finally, critical considerations of existing theories are the starting point of an investigation rather than the conclusion. Inclusive of multiple perspectives (including theories) and their relationships, the third paradigm considers interaction as means to support situated action and meaning, thereby focusing on meaning and meaning creation while foregrounding human experience.

In summary, the three paradigms complement each other. The underlying metaphors illustrate the shift in the centre of attention for research and design. Recognising this shift is valuable for producing and evaluating research insights. That is,

Table 3.2: Epistemological distinctions between HCI research paradigms

	Paradigm 1: Human Factors	**Paradigm 2: Classical Cognitivism/ Information Processing**	**Paradigm 3: Phenomenologically Situated**
Appropriate disciplines for interaction	Engineering, programming, ergonomics	Laboratory and theoretical behavioural sciences	EG, EM, ethology, action research, partice-based research, interaction analysis
Kinds of methods strived for	Cool hacks	Verified design and evaluation methods that can be applied regardless of context	A palette of situated design and evaluation strategies
Legitimate kinds of knowledge	Pramatic, objective details	Objective statements with general applicability	Thick description, stakeholder "care-abouts"
How you know something is true	You try it out and it works.	You refute the idea that the difference between experimental conditions is due to chance.	You argue for the relationship between your data and what you seek to understand.
Values	Reduce errors, Ad hoc is OK, cool hacks desired	Optimisation: Generalizability wherever possible; Given that design can be structured to reflect paradigm, principled evaluation is better a priori than ad hoc; Structured design is better than unstructured; Reduction of ambiguity; Top-down view of knowledge	Construction of meaning is intrinsic to interaction activity; What goes on around the system is more interesting than what's happening at the interface; "Zensign" – what you don't build is as important as what you build; Goal is to grapple with the full complexity around the system

Table 2 in [133, p. 14]

rather than confusing epistemological and ontological orientations across paradigms, contributions in either paradigm need to be measured against the paradigm's standards.

Researchers have employed both second and third paradigm thinking to research privacy in the home. However, we note that the goal to provide insights into the nature of power imbalances is well-aligned with third-paradigm considerations of values embodied in design, situated action, and meaning creation in interaction.

3.1.2 Research 'Turns'

As the literature review has illustrated, privacy researchers have drawn on fields such as psychology, sociology, behavioural economics, or even philosophy. Recognising that privacy fundamentally constitutes in interactions among people and with technology,

it is worthwhile to review how HCI incorporates scientific insights and methods from adjacent fields of anthropology, sociology, psychology, design, and others (Table 3.2).

Over the last four decades, several 'turns' have made a long-lasting impact on the field of HCI. These 'turns' involve the arrival of new methods and theories introduced by researchers from an adjacent discipline taking interest in HCI as research context. Rogers [222] notes that there are at least fives turns, including social, design, culture, wild, and embodiment. We briefly discuss the 'Turn to the Social' that has contributed to the emergence of CSCW as a subfield and the 'Turn to the Wild' as the most relevant movements for a perspective of practices/interactions.

3.1.2.1 'Turn to the Social'

Prominent among these turns features the turn to the social in the 1980s [222, 231]. Suchman's [230] "Plans and Situated Actions" has frequently been cited as one of the most influential books exploring the relationship between knowledge and action in ways cognitive psychology-informed HCI research was not able to. In her book, Suchman [230] artfully demonstrated the relevance of specific circumstances in and through which knowing and acting took place.

Ethnography Suchman's [230] work was mainly ethnographic in nature as she reported on observations, interviews, video and audio data, and field notes of a particular setting. Her work was the foundation of a movement that advocated for the use of *situated action* to compare previously favoured models and descriptions of device use with actual use of devices. Researchers were enabled to critique "idealised models against the backdrop of how work is accomplished" [222]. These works provided details of work practices that have contributed towards the movement which manifested in the third research paradigm, considering interaction as a way of meaning-making in the world. While researchers were initially focused on workplaces and workers' interpretive and problem-solving efforts, methods and approaches of this orientation have since been applied to other contexts.

Until the turn to the social, EG had emerged from its origin in social anthropology and found a place in sociology. Most notably, the 'Chicago School' [232] had established theory-informed ethnographic approaches for urban sociology. It has since found adoption in HCI and CSCW. Contemporary ethnographies appropriate a range of theories from adjacent disciplines to build analytic frameworks (e.g., Marxist, feminist, or postmodernist) [222], and continue to provide "novel ways of seeing the setting under investigation" [233].

While the term EG has been originally understood as "writing about people, or writing an account of the way of life of particular people" [234], it has later been understood as a way of doing research, too. Researchers are sometimes said to use ethnographic methods to highlight this difference. Since its original meaning of 'going native' with a tribe or group of people, the understanding of EG has advanced. Contemporary EGs include elements of (e.g., [222, 234]): 'in-the-wild' studies/ studies in everyday contexts; combination of a range of data sources; "unstructured" data collection followed by inductive, exploratory analysis; focus on a small number of cases; and analysis involving interpretation of the meaning of actions given the particular contexts.

Ethnomethodology A particularly influential movement in the turn to the social and Ethnography (EG) in HCI, Ethnomethodology (EM) is a 'perspective' or 'practical paradigm' in sociology. Building on Schultz's phenomenology, a philosophical perspective which posits that objects' existence is socially constructed and that the fundamental features of everyday life should be described as they are understood by ordinary people through their everyday routines, EM was coined by a sociologist, Harold Garfinkel, to describe "the practical methods through which members of a particular social group accomplish 'organisation'" [235]. Garfinkel opposed traditional social science approaches that "account for social order by proposing theoretically derived concepts that are removed from concrete activities themselves" [235, p. 3]. He argued that constructs such as values, norms, or rules are not to be understood as "independent explanations of social situations, but as *features* of them" [235, p. 3].

> Ethnomethodology's 'incommensurate' [...] theoretical proposal is that there is a self-generating order in concrete activities, an order whose scientific appreciation depends upon neither prior description, nor empirical generalization, nor formal specification of variable elements and their analytic relations. From an ethnomethodological standpoint, 'raw' experience is anything but chaotic, for the concrete activities of which it is composed are coeval with an intelligible organization that actors 'already' provide and that is therefore available for scientific analysis. [236, p. 387]

Debates on Significance However, the relationship between EG and cognitive sciences that inform HCI was a difficult one from the very beginning (e.g., [237]). An early criticism of these ethnographic efforts was a lack of operationalisable and generalisable findings [222]. While these challenges to validity and applicability of findings can be seen in light of paradigmatic differences, i.e., the desire to evaluate third-paradigm findings using second-paradigm standards, they are ever more so relevant for design. Desires to have reusable and transferable knowledge that informs a range of different projects and products arise from disciplines of design and system engineering.

Researchers have answered this call for abstract, rather than detailed, insights, which provides engineering and design audiences with some organising dimensions for insights derived from thick descriptions [228, 238], as well as a principled way in which the relationship between EG and design can be discussed [239]. Hughes et al. [238] suggested three dimensions to organise empirical ethnographic findings: distributed coordination, plans and procedures, and the awareness of work. Button and Dourish [239] have suggested a fruitful relationship between ethnomethodological abstractions (sensitising concepts that capture some aspects of the sociality of work) and abstractions in system engineering. However, whether implications for design are the appropriate vehicle to demonstrate the value of EG in HCI (e.g., [227]), and what kind of EG is suited for which purposes in HCI remain the topics of ongoing debates (e.g., [240, 241]).

Grounded Theory Another methodology that is often related to the social nature of interactions and also ethnographic data collections is Grounded Theory (GT) (e.g., [222, 242]). GT was originally proposed by Glaser and Strauss in response to the needs for qualitative analysis in a research environment of the 1960s that was strongly

influenced by positivist tendencies from the natural sciences [243]. They proposed GT as a methodology that could provide an abstract yet accurate representation of participants' accounts. Later on, Strauss and Corbin published a handbook on how to conduct GT, but it was perceived by many as too prescriptive and structural. Glaser himself was among the most vocal critiques, saying that the data should rather speak for themselves [244]. Charmaz provided her account of GT, moving away from positivist tendencies towards interpretative social sciences [245]. Her constructionist GT is located in time, space, and circumstances but not separated from its origins as positivist tendencies would convey. Charmaz's GT aims to produce understanding rather than explanation and prediction, following the understanding that researchers are part and parcel to the data collection; that facts and values are connected; and that there are multiple interpretative views. Clark discussed a postmodernist approach to GT, suggesting that theory is not discovered but constructed. In this perspective, researchers cannot free themselves from prior theoretical knowledge and their own research agenda for a specific topic. Rather, they investigate one of multiple realities, and perspectives are therefore partial, situated, and constructed such that the situation of inquiry becomes the unit of analysis.

Despite their different paradigmatic orientations, these approaches share a set of strategies [242]. This includes: (1) data collection and analysis go hand in hand; (2) themes emerge early during this process; (3) the goal is to discover social processes in the data; (4) these processes are subsumed in abstract categories; and (5) categories are linked by causes, conditions, and consequences to build a theoretical framework.

3.1.2.2 'Turn to the Wild'

The turn to the social was accompanied by a turn to the wild in the mid 2000s. Moving out of the laboratory, "new technologies were designed, prototyped, and implemented" [222, p. 73] in the context of their intended use one of the key differences of ethnographic studies 'in the wild' was the focus on the ways in which "people react, change and integrate" [222, p. 73] new technologies as part of their daily routines. In-the-wild studies employ inductive research approaches to critique existing HCI theories for

their shortcomings in the real world. They help to rethink the relationship between technology, design, and behaviour [222].

Lately, the advent of ambient internet-connected technology has driven investigations into everyday use of artefacts. These investigations are also concerned with discovering possibilities for technology rather than finding solutions for established problems. A core aspect of in-the-wild study is to report on behaviour changes over time, in-situ, and as part of everyday practices [222].

While this approach allows the researcher to take the back seat and foreground the participant ("the locus of control shifts from the experimenter to the participant" [222, p. 73]), some methodological considerations remain to be addressed. Studying technologies in the wild requires considerations of a large array of dependencies and contingencies in situated human behaviours (e.g., Tolmie and Crabtree's [246] comments on challenges of deploying research technologies in the home).

3.1.3 Research Contributions

While the field of HCC is still nascent, researchers in HCI recognised a variety of different contributions to the field:

Empirical – Based on observations and other means of data gathering from a variety of sources (experiments, user tests, field observations, interviews, surveys, focus groups, diaries, ethnographies, and others), empirical contributions are evaluated based on the soundness of their methods and the novelty of their findings.

Artefactual – These contributions include inventions such as prototypes, new systems, architectures, tools, interaction techniques, and many more. The contribution to the body of knowledge is manifested in the artefact itself and the documented means by which it is created and supported. Artefactual contributions are evaluated by types (e.g., design probes in user studies or new mock-ups/sketches) and based on how insightful and innovative they are in portraying an idea.

Methodological – Methodological contributions describe novel or improved ways in which any of the contributions discussed here are achieved. These contributions are

evaluated based on their strengths in producing said contributions and measured against their expected qualities (e.g., reliability, validity, or reproducibility).

Theoretical – Theoretical contributions include concepts, definitions, frameworks, principles, or models. Theoretical contributions are often evaluated based on their predictive, descriptive, and explanatory powers.

Dataset – A source of analytic information that can benefit the research community. They are evaluated by their ability to enable forms of research for the community (e.g., their capacity to establish baselines for benchmarks).

Survey – Forms of meta analysis and synthesis of existing literature that capture the state of the art of a research field. These contributions are evaluated by how well they organise an existing body of knowledge and draw out avenues for future research.

Opinion – Essays or arguments that seek "to change the mind of readers through persuasion". The goal of opinion contributions is to persuade and inform reflection, discussion, and debate.

This list of contributions has become a reference point for many PhD students. However, it is important to consider the means of evaluation listed above against the backdrop of the research paradigms discussed before. For example, while Rogers [222] recognise conceptual frameworks as the most successful type of HCI theory contribution, these frameworks do not necessarily aspire to meet the standards of scientific theories advocated by Wobbrock and Kientz [247].

3.2 Research Design

In this section, we justify and describe our research design based on our review of prior work and research paradigms above. The main purpose of this section is to motivate our methodological decisions by providing a rationale behind the chosen research approach for each research question. Details on methods and implementation of the respective studies are provided in the findings chapters.

3.2.1 Overall Approach and Rationale

The epistemological and ontological orientation of this thesis is situated in HCI's third paradigm. However, the paradigm is by no means prescriptive for methodology. As established in the literature review, investigations into privacy in connected homes need to consider context to capture the full spectrum of social and technological aspects that influence informational privacy in the home. Of particular complexity and importance is the social nature of the home—an understanding that technology becomes part and parcel of relationships within.

This is an opportune moment for privacy research in the home. At home, however, several other social phenomena are interleaved with privacy while no tried-and-tested theory on privacy is available—existing privacy theories not only complement and compete with one another but also invoke a broad array of tacit interpretations of the word. At the same time, our goal is to empower privacy, and we intend to deliver on this promise by effectively informing research and design to empower users through innovation.

Our research is positioned within the third paradigm in HCI [133] where the meaning of privacy is constructed at the intersection of technology and society in ways that Harrison, Tatar, and Sengers [133] describe as "what goes on around a system is more interesting than what's happening at the interface." Our goal is to "grapple with the full complexity around the system" in and around the home (Table 3.2). To address our overarching research question (RQ: *How can households living in connected homes be empowered in their privacy?*), the research approach of this thesis therefore needs to be exploratory, qualitative, and inductive.

Because 'empowering' privacy for users presumes an understanding of "What is privacy?" in the eyes of users, this research aims to achieve that by bridging users' different approaches to privacy and interpretations of privacy in the adjacent disciplines that contribute to "what [was] happening at the interface" [133] (e.g. system design). Our goal is to provide a better understanding of privacy and technology use in the home by investigating everyday interactions. This thesis therefore refrains from appropriating any existing (privacy and other) theory.

Finally, the orientation of this research has to take into account interpersonal relationships in and around the home. This consideration of relationships is extended to relationships mediated by devices, e.g., between humans or between humans and manufacturers. Since the third paradigm suggests that interactions be considered as meaning-making processes, research approaches that focus on practical action may be suitable for understanding this kind of social complexity.

3.2.2 Structure of the Study

We use a four-step approach to address our overarching research question: ***exploring, unpacking, informing, empowering***. Our approach (Figure 3.1) is structured by our research questions. We introduce and justify the chosen research methods for each research question in this section.

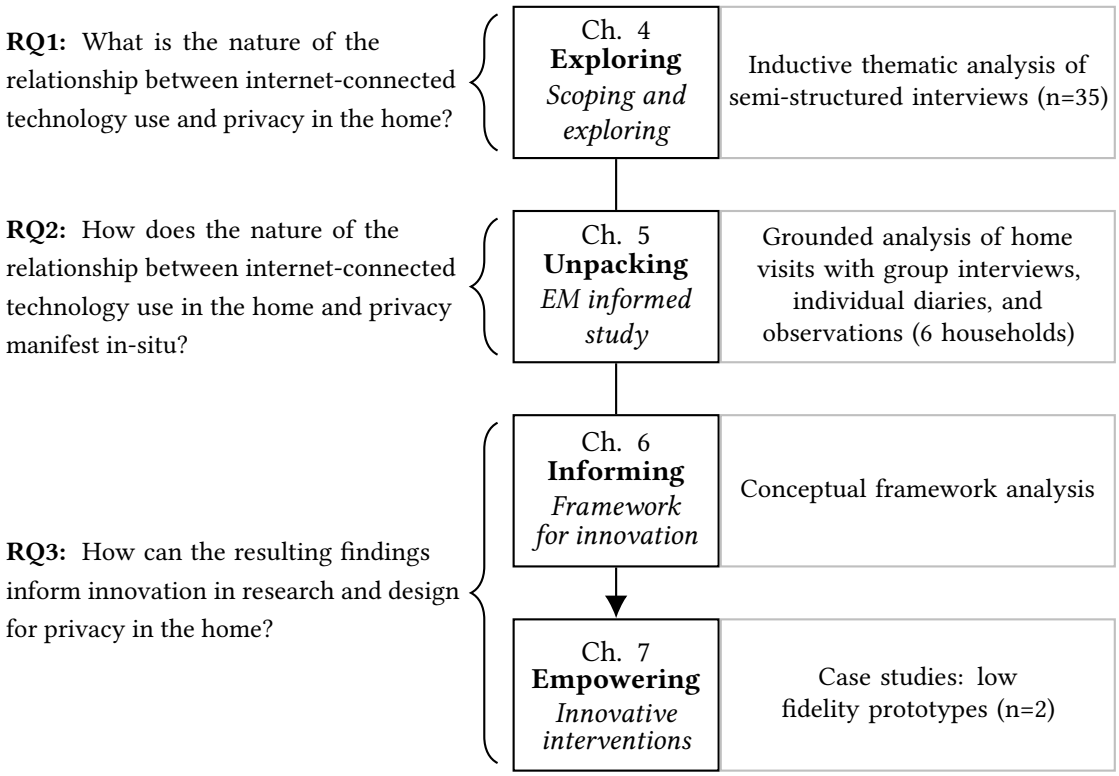


Figure 3.1: Overall research approach and overview of methods used in this thesis

3.2.2.1 Research Question 1

The purpose of this research question (Figure 3.1) is to understand the socio-technical nature of smart technology use and privacy in smart homes from our participants' point of view. To better understand the social aspects of interaction with devices, the three sub-research questions are chosen to reflect our orientation towards interaction between people and with devices as a meaning-making process.

RQ-1.1 *What are practices of internet-connected technology use in the home?*
RQ-1.2 *How are these practices organised and oriented to in the home?*
RQ-1.3 *What is the relationship of these practices with privacy?*

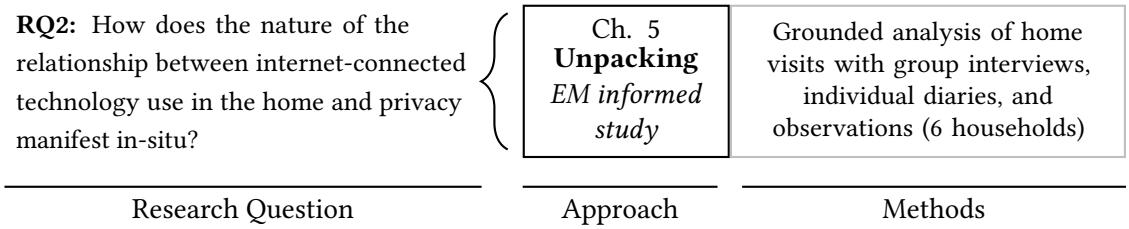
To address these research questions, any research approach (empirical, exploratory, qualitative, and inductive) must be in line with our rationale discussed earlier. In choosing the word 'practices', we highlight the importance of practical work, that is, the actual interaction with devices rather than attitudes or preferences. The words interactions and practices are used interchangeably throughout this thesis, and can be understood as 'situated actions' [230]. Research methods that allow for the investigation of practices are typically also of observational nature.

We acknowledge that "practices are only accessible through observation; interviews and narratives merely make the accounts of practices accessible" [248, p. 215], and that our participants are unlikely to provide an accurately self-report since their interaction with devices are based on their own reflections and their memory. However and for reasons of feasibility, we decide to carry out semi-structured interviews to provide feasible access to participants' experiences with technology in a time and cost appropriate way for a scoping study. The interview guide can be found in the appendix (Figure A.1).

To scope out the research area of technology use and privacy in the home, we apply exploratory and inductive thematic analysis [78], which allows us to identify and better understand important social and socio-technical facets of the problem space. Thematic analysis provides "accessible and systematic procedures for generating codes and themes from qualitative data" [78]. Descriptive coding is first conducted followed by interpretative coding and theme building [249]. The method suits our purposes because of its flexibility in identifying patterns across cases and with a focus on

participants' lived experiences. Thematic analysis allows us to follow an inductive and exploratory approach, focusing on peoples' interactions without requiring a theoretical research framework.

3.2.2.2 Research Question 2



The first study provides a key insight into the ways in which technology use in the home is communal, and how household members have established their own understanding of what constitutes 'normal'/appropriate behaviours and actions around the use of technology. While our participants discussed past privacy experiences and reported on privacy practices, the social phenomenon of privacy was not salient in their everyday concerns. If privacy is not salient but occasionally discussed and oriented to, then the question of how it 'manifests on the ground' is an important one.

Almost in parallel to our own research efforts, others have also investigated conceptualisations of privacy (e.g., as control over information) in the context of smart homes. Similar to our findings, they showed how devices could be misappropriated and sometimes even abused in ways that violate the privacy and curtail the agency of cohabitants [17, 193]. This results in power imbalances between large corporations and users, *and* between members of the same household [5]. However, an account of how these power imbalances have come about and how they could be addressed is missing from the literature.

In light of these insights, we refined our second research question as follows:

RQ-2.1 *How is communal use of smart devices in and around the home organised?*
RQ-2.2 *How is privacy oriented to as part of this organisation?*
RQ-2.3 *What are implications for product design and development?*

To address these research questions, we require a research approach that allows a close focus on both household members' use of devices and their interpersonal relationships in-situ (sometimes called 'in the wild') and over time. While there exists a large array of research methods for in-situ research (e.g., home tours, experience sampling, or design probes), the nature of our research questions calls for rich insights on household members' interactions.

To obtain rich and detailed insights, we choose home visits with group discussions and individual diaries as data collection methods. Data from observations and accounts of social interactions between household members, reported behaviours, and occasional demonstrations of interactions with devices are well suited for our exploratory and inductive research approach.

These data collection methods allow us to gain an 'in-situ perspective' and focus on understanding social actions and processes as constituted by everyday interactions in a social domain. At the same time, these methods are appropriate for the home as research context since they 'optimise' the time we need to spend at each research location: occasional interviews and diaries are 'less intrusive' than extended periods of observation and, therefore, more desirable when researching households' domestic technology use and privacy. These data collection methods are also more feasible to implement, particularly for a single researcher.

The goal of this research effort is to understand the *nature of the relationship* between internet-connected technology use in the home and privacy *and* to understand *how this nature manifests in-situ*. EM's analytic orientation aligns well with the second part of this question. However, the nature of the relationship is not just communal but can also be characterised by the two power imbalances that frame this research. Issues of power and empowerment are part of the overarching research question. These issues raise analytic and structural questions which we approach by presenting insights from our *EM informed study* following the process of GT. We motivate and explain our approach below.

Background and Motivation A multitude of research approaches in HCI aim to provide insights on 'how the nature of technology use manifests in-situ'. EM informed approaches to HCI, particularly Suchman's work [230], were introduced before the advent of mainstream sociology spurred a debate on the relationship between empirical insights from ethnographic studies and the practices of design in HCI.

Implications *for* design from these accounts typically serve to 'defamiliarise', 'tell exotic tales', or 'critically reflect' [240]. 'Defamiliarisation' studies help designers rethink the assumption built into domestic technologies. It is questionable in how far an approach turning naturally accountable interactions into analytic objects can play an active part *in*, rather than a critique *of*, the design process [240]. The proposition of these studies is to "provide an alternative view point on assumptions in the design process itself" [250, p. 154]. While serving as the root of ethnography in anthropology, 'exotic tales' are criticised in HCI for their failure to provide actionable insights for designers due to their lack of sufficient detail and attention to interactions. 'Exotic tales' often surface descriptions that offer "grossly observable features of a setting or culture" [240, 251]. 'Critical reflection' encourages designers to consider 'new values' beyond productivity and efficiency [240, 252]: "Critical reflection *itself* can and should be a core principle of technology design for identifying blind spots and opening new design spaces" [p. 49][253].

EM proponents criticise these perspectives for undermining the value an ethnographic perspective can provide *in* design, urging researchers to "move from design critique to design practice" [239]. Crabtree et al. [240] position the *EM informed* 'critical interpretative frame' as the result of uncovering the natural accountability of members' actions and not as the result of an analyst's interpretation of data (see also Section 3.1.2.1). This perspective follows Lucy Suchman's seminal work on 'situated action' [230] and has made significant contributions to the field [254]. The perspective allows us to focus on how actions and interactions of household members are organised in their particular setting [230, 255].

The main part of our research question aligns well with an EM informed study *within* system design. However, any discussion of the *nature* of the relationship

between technology use and privacy can also benefit from 'defamiliarisation' and 'critical reflection', raising the question as to how EM informed findings can offer implications *for* user experience and interaction design more broadly in these ways.

System designers benefit from EM informed approaches that provide operationalisable, generalisable, reusable, and transferable insights [228, 254, 256, 257]. In regard to reusability, the debate centres on how to operationalise the naturally accountable character of everyday work. Button and Dourish [239] suggest 'technomethodology' as an effort to align "system design [...] with the details of the means by which [...] working practices arise and are constituted". This intriguing perspective and the research effort required has proven difficult to realise and thus seen limited uptake. Hence, Crabtree [258] proposes a hybrid approach that avoids the challenge of having to integrate EM with the product development life-cycle. In their 2012 practical guide "Doing Design Ethnography", Crabtree, Rouncefield, and Tolmie [228] distinguish between *situated* implications for design (e.g., providing details for requirements engineering) and *generic* implications for design (e.g., can be oriented to but require further exploration through ethnography). They also suggest concepts of distributed coordination, plans and procedures, and awareness of work as a framework to communicate generic implications with designers [228]. Generic implications for design invite to defamiliarise and critically reflect through their grounding in an EM tradition.

Insights from this debate are important for our methodological considerations. Firstly, EM's powerful, tried-and-tested approach can provide insightful and actionable findings on the sociality of work. Secondly, there exists an inherent challenge of making these findings available to system designers and developers. Lastly, insights and implications from EM studies can take different forms, such as situated or generic implications for design.

As the study is an evaluation of existing design efforts (not dissimilar to a single iteration of Crabtree's [258] 'hybrid approach'), interaction with designers and product developers is not part of this study. Moreover, our findings need to enable user experience and interaction designers to consider privacy as a pervasive feature of product design and

development (see Section 2.3). Hence, an additional goal to inform future design efforts arises: designers should be able to navigate and reconstruct the findings independently.

We need to present key insights that are operationalisable, generalisable, reusable, and transferable [228, 254]. These insights should allow for critical reflection and familiarisation, i.e., they need be generic implications [228], presented with clear and efficiently navigable links between findings and their implications. Beneficial are representations that can be efficiently navigated bottom up (anecdote to insight) or top down (insight to anecdote).

GT provides structured and focussed representations that let 'the data speak for itself' and highlight emerging social phenomena [242]. GT is used frequently to explore socio-technical phenomena and to inform design through structured, empirically-grounded representation of interaction (e.g., [259–261]). GT's inductive theorisation suggested by Charmaz [262] based on [263] maintains the heritage of arriving at "concepts and theories through analytic construction [rather than] through empirical generation" [264]. As Ten Have [264] explains, GT traditionally employs a fundamentally different analytic orientation as

> ethnomethodology does not strive to 'add' anything to the social life it studies, no 'theory', no 'concepts', not a different level of reality. It just brings to light what is already available for all to see; it is, then, just an eye-opener. [264, p. 12]

Yet, GT and EM can engage in a synergistic relationship. We suggest the notion of theory building be replaced by 'plugging' EM's analytic perspective into GT's process. The overarching GT protocol not only encourages us to pay close attention to observable and reportable interactions but also provides guidance in organising and navigating our record of interactions. In this sense, we recommend using the GT protocol to frame the "empirical generation" [264] of 'generic implications for design' [228]. The approach reminds us to stay focussed on "what people do and how they organize action and interaction in particular settings of relevance to design" [240]. The rest of this section further explains the approach to which we will refer as 'grounded analysis' henceforth.

Our Grounded Analysis In discussing some key insights and challenges, we further unpack the synergistic relationship between GT and an EM informed approach.

Integrated Analysis GT invites researchers to form a logically integrated theoretical analysis of their setting [263]. While Glaser assumed that there were single unifying themes that could explain variations in data, this is not always the case and might be undesirable particularly in the context of ethnographic and EM informed research ("The world may not be as simple as the sense we make of it." [242]). As highlighted above, it is neither desirable nor required to exercise 'analytic construction' [264] that tends to undermine the value of empirical insights for design [228, 254]. EM informed approaches are particularly powerful in providing 'generic' and 'situated' implications for design [228].

Effects of Existing Theories GT holds that researchers should only engage with the literature once they have established their own theory. However, this is impractical for junior researchers (who tend to be strongly inspired by earlier work) and senior researchers (who are typically more familiar with existing research) alike. Therefore, the term abductive theory building is sometimes preferred (e.g., [265]). Whatever the researcher's predisposition, the emphasis of 'letting the data speak' [266] provides a useful guidance on how to purposefully draw on existing theories. The intention of engaging with existing literature late in the process aligns well with the desire for 'empirical generation' of insights [264] and 'indifference' to sociological analysis [267] of EM informed approaches. While our orientation is by and large indifferent to existing theory, we draw on existing literature (including analytic theory) where this is opportune to discuss the value of our insights for the practices of design.

Writing the Results EM informed studies usually provide thick descriptions or 'praxeological accounts' [228] that empirically 'generate' [264] implications for design. Despite being embedded in a coherent narrative, theoretical codes and categories are considered more important than the narrative itself in GT. Our goal is not to produce

theoretical codes as a result of GT analytic construction [243, 263], but as representation of a naturally accountable sensitising concept in the sense of 'generic implications' [228].

As parts of the empirical representation are readily discernible, readers are able to assess the logical links of the social organisation of the setting as well as the interactions and social processes which consitute it. The empirically grounded representations add to the trustworthiness of our findings. Incorporating some GT structures in the write-up of an EM informed study improves readability among our target audience. At the same time, the writing of results is part of the analytic process (as it is in EM informed approaches) because dealing with structured representations can enable a deeper and more outcome-oriented exploration of the data.

Challenges for Grounded Analysis The outlined approach along with considerations discussed above addresses common critiques of GT , (e.g., [242, 262, 265, 268–270]). Drawing on [265], we review these challenges below.

Inadequate grasp of theoretical sampling Theoretical sampling encourages the researcher to sample data in ways that serve to advance an emerging theory. For example, if the emerging concept or dimension appears isolated or underdeveloped, the researcher should select data that can help strengthen its links and add to its understanding. Muller [270] observes three patterns of GT in HCI that also reflect this problem. The first approach is probably closest to the original idea where data is collected and analysed purposefully as theory emerges. The second approach draws on existing data sets without the possibility of collecting more data. The authors suggest that iteratively querying large data sets while building theory can be "very similar to theoretical sampling" as the researcher continues to find new insights [270]. In the third approach, GT is used only as "gloss or mantra" [242] to gain credibility without having followed a rigorous GT approach. The authors consider this approach problematic by as it reflects an inadequate use of GT.

An EM informed approach of 'empirical generation' aligns with the idea of 'iteratively querying' by paying close attention to the 'natural accountability' of social phenomena. Note that the use of sampling here does not serve the goal of analytic

construction of theory, but reminds the researcher to pay close attention to the details of situated action.

Lack of analytic diagrams GT invites the creation of analytic diagrams that show relationships between categories and/or theoretical concepts. These diagrams are important for documenting the research process to provide 'internal validity' for the construction of the theory. They also serve as 'boundary objects' that coherently capture the theory and its core concepts. While providing analytic diagrams of the final theory is an important part of documenting GT, presenting diagrams for our empirically grounded representation can equally benefit discussions where boundary objects can be used.

Misalignment of research paradigms It is crucial the paradigmatic difference between GT approaches highlighted earlier (Section 3.1.2.1) be taken into account. Glaser's positivist tendencies are not reconcilable with our orientation to HCI's third paradigm in which actions are considered as places of meaning-making and a constructivist approach like Charmaz's [242, 262] is favoured. For Charmaz and Mitchell, paradigmatic differences explain much of the debate on researcher reflexivity and the nature of theory between Glaser and Strauss/Corbin (i.e., 'does it exist out there?' (Glaser) or 'is it constructed by the researcher?'(Strauss and Corbin)). Charmaz and Mitchell also add to Glaser's assertions with regard to context. To him, context cannot be considered from the outset but must emerge as a factor through analysis. These positivist tendencies are extensively criticised by constructivist and postmodernist GT methodologists. Ultimately, the challenge lies in a proper alignment of paradigmatic orientation and research methodology.

In principle, EM informed approaches are indifferent to these debates. We sidestep this debate using an EM informed grounded analysis as motivated and explained throughout this section. It is important to recall that our insights are not derived as much from analytic construction as from empirical generation [264].

Importing Sensitising Concepts We further detail the engagement with EM as part of our grounded analysis. EM informed research pays particular attention to the accomplishment of social order in everyday interaction and is therefore well suited to understand communal settings. As Maynard and Clayman [236] put it, EM postulates "there is a self-generating order in concrete activities" that provides for an "intelligible organization" and which is "available for scientific analysis".

Using sensitising concepts in conventional GT analysis reduces the complexity of the analytic task as it helps provide focus and guidance for the analytic process through a focused perspective on data [262].

> Consistent with Blumer's (1969) depiction of sensitizing concepts, grounded theorists often begin their studies with certain research interests and a set of general concepts. These concepts give you ideas to pursue and sensitize you to ask particular kinds of questions about your topic. [262, p. 16]

We use sensitising concepts of 'everyday activities', 'natural accountability', and 'dimensions of work' to help us ask specific questions about the data and guide our analytic efforts. The concepts outlined below allow us to focus on specific issues or phenomena that are relevant to our research question.

Everyday activities Everyday activities are subject of EM investigations in that they constitute recurring practices. Implicitly, the focus is not with actors that carry out actions (for particular reasons under specific conditions etc.) but with practices and actions themselves. Fuchs explains, "members of ordinary society do not so much act as enact the social practices of common sense" [162, p. 61].

Individuals become members through mastery of language [271]. They are able to render their talk and actions observable and reportable phenomena to other members who share the same common-sense knowledge of everyday activities. They are also able to grasp what is implicated in the use of language that provides its meaning and shows some of its intention. Members who speak the same 'language' are able to grasp that meaning and intention without having to explicate the particulars glossed by the speaker.

GT allows the researcher to draw on any kind of data in creating codes and categories. This can include cognitive and observational perspectives but also create

methodological misunderstandings. This sensitising concept of *everyday activities* suggests a strong focus on action, one that almost disregards actor agency. It fits well with our research goal in which 'privacy behaviour,' rather than attitudes or preferences, is focused.

Natural accountability Members of the setting "are supposed to design their actions in such a way that their sense is clear right away or at least explicable on demand" [186]. Natural accountability refers to the observable nature of interaction—members' ways of making their everyday activities 'visibly-rational-and-reportable-for-all-practical-purposes' [255, p. 7]. Accountability is an inherent property of social action rather than something that can be attributed to or used to describe a particular kind of social action. Accountability refers to the ways in which ordinary members of the society participate in "rational social behaviour" [272]. This behaviour is rational and social in that *everyone knows that everyone knows* what is being accomplished as part of a particular social action [272].

Natural accountability informs our research orientation in many ways. It highlights the ways in which actions are self-explanatory to other members, and how this kind of accountability provides a sense of normalcy. It also helps to capture unmet expectations of normalcy (or 'background expectancies' in EM terms) that surface when members readily provide oral explanations when explanation is demanded or lack of naturally observable accountability anticipated.

Dimensions of work Hughes et al. [238]'s dimensions for the presentation of empirical work can equally be appropriated to guide analytic insights. The following notions are taken from [228, pp. 127-128] and appropriated for the home context:

- *Distributed coordination* refers the organisation of activities in the home that are part of the division of labour. The "manner and means" by which these activities are organised is of particular interest in EM.
- In work settings, objectives might be laid out by *plans and procedures* such that capturing what is actually involved in accomplishing them becomes an import consideration for EM. In the home, plans and procedures are more dynamic and

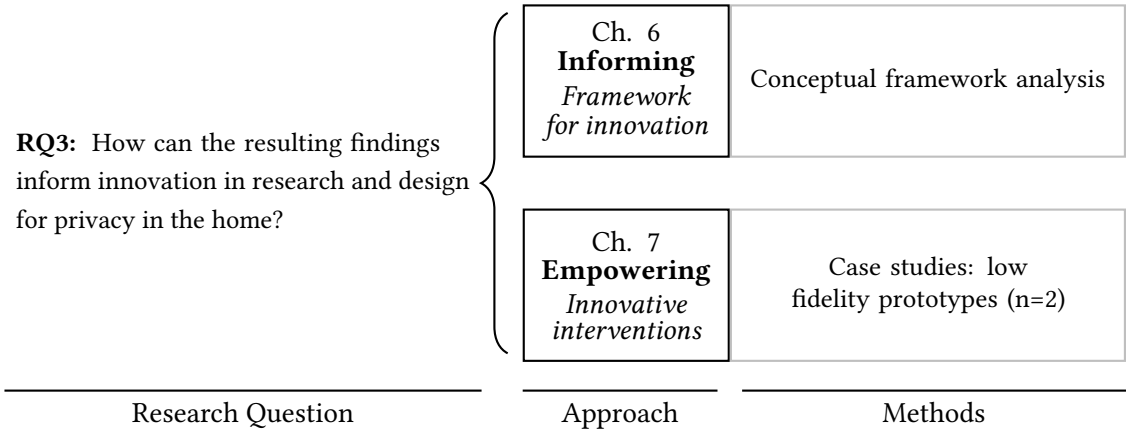
rarely codified. However, even paying attention to "what is actually involved in 'getting the job done'" is important.

- *Awareness of work* refers to the ways members make each other aware of the work that has been accomplished in the distributed division of labour. Of interest are the means by which this awareness is achieved, emphasising "the fundamentally social and accountable nature of work".

The concept of *natural accountability* encourages investigation of social processes that contribute to a sense of normalcy and orderliness for the organisation of everyday life. Together with the *dimensions of work* which provide starting points for investigating how that sense is achieved, they offer a useful lens through which researchers can use to consider how emerging concepts might relate to one another (through the dimensions of work).

Ultimately, these concepts offer directions for the emerging representation, sensitising the researcher to social processes that need to be understood in order to make sense of the social organisation of a setting. For example, they sensitise the researcher to questions of what it is that people 'do' that contributes to and represents the sense of normalcy when 'following' social processes, and how such processes can be supported or enabled.

3.2.2.3 Research Question 3



Our efforts to answer this research question are guided by two observations: (1) the need to innovate to empower privacy in communal use while (2) keeping in mind the status quo of privacy engineering.

For design researchers and practitioners to effectively address issues of 'communal privacy' in smart homes, innovation is needed. However, successful innovation that causes fewer occurrences of unwelcome social phenomena requires that design researchers and practitioners be able to orient their efforts to the practical ways in which households organise their use. Needed is a perspective that recognises "interaction not as a form of information processing but as a form of meaning making" and one whose primary goal is to account for "situated action in the world" [133].

As part of privacy engineering, innovation for privacy is mainly driven by regulatory guidelines on data protection which narrowly focus on individual's ability[1] to control the flow of their information [126, 127]. While researchers apply Value Sensitive Design (e.g., [140]) and Participatory Design (e.g., [117, 143, 144]) to explore situations without a clear definition of privacy upfront [126], UX designers lack structured and systematic approaches to identify, ideate, and define solutions [274, 275]. Crucially, an understanding of how these solutions are situated in the social organisation of the home and manifested in everyday interaction is lacking.

We refine our third research question as follows:

RQ-3.1 *What is the context for innovation in design and research for privacy in communal use?*
RQ-3.2 *What are opportunities for empowerment within that context?*
RQ-3.3 *How can design seize these opportunities to empower households?*

To address these research questions, we decided to create a conceptual framework to set the scene for research and design innovation to empower privacy in communal use. As Rogers [222] notes, frameworks are "a set of interrelated concepts and/or a set of specific questions that is intended to inform a particular domain area". Our goal is to create a "skeletal framework" which provides an "internal structure [...] as a starting point for observations and interview questions, and for analysis" [276] in further research and design efforts. Conceptual frameworks in HCI serve as 'sensitising

[1]The GDPR has a household exemption ([63], Recital 18). Legal issues related to data control and ownership in smart homes are subject of ongoing research [65, 273].

concepts', boundary objects, and sources for inspiration and discussion. The extent to which our framework has fulfilled these purposes was documented in the process of design thinking and demonstrated in our two case studies.

Conceptual frameworks appearing in HCI literature do not always include information on the methods behind their construction (e.g., [277–279]) but follow a process of systematic literature review, qualitative coding, thematic analysis, and sense-making instead (e.g., [280]). Such processes are formalised by Jabareen [281] who proposed a GT based approach called conceptual framework analysis. The strength of their approach is the power of GT that allows the researcher to move beyond "quantifying and tallying" the presence of a concept [281]. Conceptual framework analysis then allows for grounded theorisation of both concepts and relationships between them—something other conventional approaches cannot provide to the same extent (e.g., conceptual analysis or meta-synthesis). Hence, we apply conceptual framework analysis to build our framework.

Our second observation motivates the inclusion of HCI's second-paradigm thinking (i.e., interaction as information processing in light of influences from cognitive sciences). Given that the nexus of data protection as manifested in regulation favours an information flow control perspective which is also akin to requirements for abstractions [145, 239] discussed above, we direct our efforts to bridging the paradigms by making available third-paradigm insights and thinking to those more familiar with second-paradigm stances. To this end, we review contributions from social psychology, using these insights as additional backdrop for our framework.

Note that our use of second-paradigm theory is still in the service of third-paradigm thinking; the ways we lean on social psychological theories in building the framework are reflective of creating and managing meanings in interactions. We aim to demonstrate a mutually beneficial and complementary relationship between an agentic/cognitive perspective and one that focuses on meaning-making in interactions and practices. These perspectives complement each other in that cognitive approaches have strong task focus whereas interaction-centred research sets centre-stage aspects of context. We limited our approach to RQ2 to investigate the reflexive organisation

of social order in the home as it constitutes itself in interactions between people and with devices. The 'why' of any action in that perspective is assumed to be part of an individual's natural reasoning and thereby evaluated against a sense of normalcy [162]. Individuals do "not so much act as enact the social practices of common sense", and "members [are] outcomes of practices but not authors" [162, p. 61].

However, questions of why and how people perceive, use, or even do not use devices become contingencies for any intervention to change their behaviour; for example, in policy and design where household members can be supported to better anticipate consequences of their actions. While 'why' and 'how' are questions that could well be approached from a cognitive perspective, which actions and which goals should be considered are better reflected in interactions. For example, when household members carry out tasks on behalf of the household, 'why' and 'how' they act become contingent (e.g., within which boundaries might children be allowed to use devices).

It is on these grounds that we consider second-paradigm views as beneficial for attaining empowerment through innovation in research and design.

3.3 Ethical Considerations

The two participatory research projects presented in Chapter 4 (reference number: R54434/RE003) and Chapter 5 (reference number: R59140/RE001) were reviewed by the Oxford University Central Research Ethics Committee.

The purpose of ethics reviews was to protect the well-being of research participants, i.e., adults and children that volunteered their time for our research. The researcher carefully drafted, submitted, and reviewed ethics applications for the respective projects based on university standards and guidelines, which included research processes involving participants. Prior to each interview, participants were informed of the projects outline, goals, their role as participant, the role of the researcher, what to expect, and how to address emerging issues related to the study (e.g., withdrawing from the study). This information sheet was created to be age and audience appropriate, using 'plain and easy' language.

The researcher conducted all interviews (Chapter 4) and home visits (Chapter 5). At the start of each first session, participants were verbally reminded of the study outline and other details from the information sheet. Participants were asked to sign a participant consent form (or assent from for children) provided and explained by the researcher. During this process, the researcher also reminded the participants that all collected data were anonymised and stored according to the university's data protection guidelines.

One possible issue in interviews and group sessions with households was sensitive topics. We emphasised repeatedly that participants could change the subject or refrain from answering any of our questions at any point during the conversation. Besides, we refrained from 'intrusive' questioning and generally let participants steer conversations. To further minimise tensions in group sessions, we emphasised that participation of any household members was entirely voluntary. Should issues occur between sessions or participants change their opinions after a meeting, they were able to contact the main researcher or principal investigator by phone or email.

For the EM-informed household study with children, particular safe-guarding measures were put in place. The principal investigator assumed the role of a "Safeguarding Lead" making sure that all involved researchers underwent appropriate training and followed the university's code of practice. In collaboration with the author of this thesis, a comprehensive risk assessment was put in place. The researcher familiarised himself with the University's Safeguarding Code of Practice, completed OSCB's (Oxfordshire Safeguarding Children Board) online training, and received clearance from the UK's Disclosure and Barring Service. Research data was managed according to standards of the university and the UK Data Privacy Act 2018. Recordings were not kept longer as strictly needed, stored encrypted on a local drive, and only accessed by the researcher. The researcher also kept consent forms and other participant information in a secure storage, replacing real names with pseudonyms in transcripts.

Additional questions regarding data protection arose from the study in Chapter 5. Off-the-shelf smart devices were gifted to households for installation in their home. These devices were fully owned and overseen by the participants. The research team did not have access to any of the accounts they used or data they collected. Participants

were not required to install and use any device if they did not want to. It was particularly the process and the experience of participants independently dealing with devices that we were interested in. However, we made sure to only recommend devices for which no known security vulnerabilities had previously been reported.

Finally, participants in either study were incentivised appropriately for their participation. Interview participants received a voucher after the session, and households received monetary payments in instalments throughout the six-month duration of the study. Ethics application, approval, and supporting documents for the study can be found in the Appendix A and B.

3.4 Trustworthiness

The methodological approach to this thesis requires appropriate criteria for the evaluation of qualitative research. Guba and Lincoln [282] suggest four main concerns with regard to trustworthiness of a scientific enquiry involved: truth value, applicability, consistency, and neutrality. Guba [283] discuss how these concerns need to be addressed in naturalistic/phenomenological as opposed to rationalistic/scientific research approaches (overview in Table 3.3). We use Guba's [283] discussion of credibility, transferability, dependability, and confirmability to inform our research design. We discuss our effort to meet these criteria below and provide a summary in Table 3.4.

3.4.1 Trustworthiness in Qualitative Research

Table 3.3: Scientific and naturalistic terms corresponding to the four aspects of trustworthiness (Table 1 in [283])

Aspect	Scientific Term	Naturalistic Term
Truth Value	Internal Validity	Credibility
Applicability	External Validity Generalisability	Transferability
Consistency	Reliability	Dependability
Neutrality	Objectivity	Confirmability

Credibility

To establish the *truth value* of the findings, qualitative/naturalistic researchers establish *credibility* of their findings against/with their data sources (ensuring isomorphism of findings from data according to the multiple realities of respondents) [283]. Means to achieve credibility are prolonged engagement, persistent observation, peer-debriefing, triangulation, and member checks.

Transferability

Rationalist research aims to make "chronological and situational variations irrelevant" [283, p. 80] to achieve external validity or generalisability. The naturalistic paradigms deem these aspirations unattainable because of the situatedness of phenomena. However, transferability between contexts is possible on the basis of "essential similarities" [283, p. 81], and that "thick descriptions" to capture the situatedness of contexts are a prerequisite [284].

Dependability

In a rationalistic context, validity is a direct function of reliability, and it is essential for determining consistency. The naturalist inquiry is challenged when the researchers need to account for "evolving insights and sensitivities" [283, p. 81] of their human instruments and participants. In this regard, the researchers have to see consistency as "trackable variance" that can be ascribed to specific sources. Dependability captures aspects of reliability and trackability. Means to establish dependability include overlapping methods, step-wise replication, production of audit trails, and auditing the analytic process.

Confirmability

Within the rationalistic paradigm, neutrality is commonly understood as objectivity, and thus presumed by methodology (replicable, open to scrutiny, and investigator biases accounted for). However, this narrow understanding holds true in neither rationalistic

nor naturalistic research where investigator's predispositions in experiment design often affect outcomes [283]. Naturalistic inquiries expect data to be confirmable rather than expecting the investigator to be objective (the latter not being possible). Naturalistic researchers employ triangulation and practise reflexivity to establish confirmability.

3.4.2 Establishing Trustworthiness

While answering the three main research questions, concerns of trustworthiness are reflected and addressed by various different means. Table 3.4 provides a summary of the efforts discussed below. Further details are available in respective findings chapters.

Table 3.4: Employed measures for trustworthiness of research approaches

Aspect	**Inductive, thematic analysis (Chapter 4)**	**Grounded analysis of ethnomethodologically informed study (Chapter 5)**	**Conceptual framework analysis (Chapter 6)**
Credibility	peer-debriefing after interviews; triangulation with prior research	prolonged engagement, persistent observation, triangulation, and peer-debriefing	triangulation between research papers, news stories, and empirical data
Transferability	structured, rich descriptions & quotes	comprehensive descriptions of phenomena (see comments on writing in 3.2.2.2)	comprehensive descriptions of phenomena
Dependability	coding workshops & examination of audit trail (peer-reviewed)	documentation of grounded analysis and framework building process & examination of audit trail (peer-reviewed)	
Confirmability	triangulation with other research; see also 'Role of the researcher'	examination of audit trail (peer-reviewed); see also 'Role of the researcher'	examination of audit trail (peer-reviewed)

Inductive, Thematic Analysis

To establish trustworthiness in Chapter 4, the researcher regularly debriefed interview sessions with peers and supervisors. To further contribute to the credibility of findings, we triangulated our findings with existing research. With regard to the transferability of findings, we provided rich, structured descriptions supported by quotes in Chapter 4. To ensure our findings were sufficiently supported by the data collected, we ran

coding workshops and discussed emerging codes and themes with other researchers at the department[2]. However, the study's purpose was scoping, ultimately requiring further investigations that illustrated and supported its findings (such as but not limited to findings presented in Chapter 5).

Grounded Analysis

The grounded analysis in Chapter 5 is detailed in Section 5.2.3. The credibility of our findings is supported by a prolonged engagement of more than six months per household; member checks during and sometimes after visits; triangulation of field notes, diaries, and interview transcripts; regular peer-debriefing with supervisors during data collection (discussion of field notes and early memos); and a rigorous coding process (two researchers jointly coded all transcripts and each quotation was discussed prior to coding). The transferability of findings is achieved via detailed and grounded-in-data descriptions of categories. We used a number of vignettes in the chapter to illustrate the richness of our findings. We also documented the coding process provided in diagrams/networks. This audit trail was peer-reviewed regularly such that our review discussions contributed to dependability and confirmability of our findings. Further comments are included in Section 3.5.

Conceptual Framework Analysis

Trustworthiness of the conceptual framework analysis in Chapter 6 is derived from its creation process (building on GT) [286]. The process allows for triangulation between empirical data, news stories, and prior research contributions to establish credibility. The researcher applied GT to derive concepts from these sources, and in turn validated these concepts against data sources. Concepts were also linked to one another, and comprehensive descriptions of concepts were provided. The process was documented and the resulting audit trail was peer-reviewed. Concepts as well as the resulting framework were discussed with other researchers at the department.

[2]We deemed measures of inter-coder-reliability as inappropriate for capturing any aspect of trustworthiness as codes were not the product but the process of the analysis [285].

3.5 Role of the Researcher

Researcher reflexivity is an important exercise that sensitises ethnographers to the impact of their personal characteristics, predispositions, and prior experiences on the researcher-participant relationship and the data collection. As a graduate student, the researcher is an outsider to participating individuals and their families. However, as a smart technology user, he has become an insider who is able to relate to some of their experiences.

The researcher's knowledge of and experiences with particular smart technologies prior to this research were limited. In fact, he had only obtained some of the devices used in Chapter 5 when it was weeks into the study and after the first three households had deployed their devices. In this regard, the researcher was able to portray himself as somewhat knowledgeable but not fully experienced with all of the smart devices. By showing genuine curiosity to learn from participants' experiences, he was able to establish good rapport with the participants in Chapters 4 and 5.

The researcher's positioning in the ethnomethodologically informed study is probably best described as 'passive participation' [287, p. 28]. The researcher's engagement was limited to keeping conversations on topics related to issues with smart technologies but otherwise assuming a passive listener role. Occasionally during conversations, the researcher may be required to assume the role of an interviewer rather than that of an observer. For instance, on one occasion the researcher had to become actively involved in supporting a household to overcome their struggles of setting up a device. The decision was made to enable the household to get started with using the device in order to avoid missing the opportunity to observe social interactions around the use of the device. Note that the same household did set up a device of the same brand and product family later on independently.

Although the researcher grew up in Western culture (in Germany) between the 90s and 2000s, he was not familiar with much of the UK's cultural heritage. Hence, where cultural nuances in conversations appeared important, he was able to pay closer attention to the background information. That said, this kind of information was frequently volunteered by participants and the extent to which it was relevant to

the use of technology could be discussed further. In another example, because smart home devices are also interfaced with building infrastructure, the UK housing stock represented another cultural backdrop with which the researcher was not entirely familiar. By engaging in conversation with other researchers and participants, the researcher was able to clarify related questions. Note that these kind of insights allowed the researcher to be fully immersed in the research context and study and thus able to see the world through its members' eyes.

The researcher's life situation as a postgraduate student was of course also inherently different from that of the participants. Even though good rapport was built, some distance remained between the researcher and participants. Shown in conversations was how the relationship with participants may be shaped by the researcher's personal characteristics. For example, the researcher found himself 'doing talk among experts' when participants, adult male in particular, offered 'demonstrations of knowledge' rather than sharing past experiences. Though not being a key defining feature of the experiences of interactions, these comments to some degree reflect the home's moral and social order and was thus considered in the analysis.

The researcher was acutely aware of the power dynamics in the home, e.g. those discussed in Section 2.5.3. Part of these dynamics were undoubtedly performances of gender [199], and the researcher naturally took part in these performances during household visits. The 'demonstrations of knowledge' could, in part, be attributed to the researchers' and demonstrators' gender as similar attempts were rare from the female counterparts. Participants' performances of gender also corroborated with existing literature. For example, we noticed divisions of labour between adults that correlated with gender as reported in the results section. To engage with these challenges the researcher took several measures. During the visit, he took note of any perceived imbalance, e.g., differences in household members' talking time. The researcher made effort to rebalance the talking time such that all genders had equal opportunity to present their perspectives. After the visits, the researcher used his notes detailing occurrences in question, comparable instances from other participating households, and data from prior visits for discussion and reflection with a gender-diverse group of

researchers at the department. The process regularly took place between visits and in coding workshops allowing us to critically reflect on our contribution to performances of gender, e.g., considering whether the reported performance of knowledge was mainly a reflection of our gender.

While other performances we observed such as who got to set up which device in Chapter 5 may have indicated a performance of gender, they could have also arisen as a result of any circumstance such as social anxiety, personal preference, or opportunity. While we were aware of issues of gender, our analytic perspective in Chapter 5 did not allow for a direct discussion of gender in our data analysis since household members made no explicit or implicit reference to gender. We wanted to analyse what was observable. It is only later in Chapter 6 and 7 when findings are triangulated with prior research that we open up our perspective to such interpretative framing of our observations. We do so in service of relating our contribution to existing research, rather than contributing to a research agenda on gender and technology. As important as it is, the agenda is grounded in a different analytic perspective not taken in this study.

When one household member demonstrated significantly more knowledge than others, this was taken as an opportunity to check the experiences and understanding of other household members. While the kind of accounts received from other household members may be influenced by the researcher's personality (e.g., [287]), this is naturally the effects of the researcher-participant relationship that are inherently part of the data collection. To mitigate these effects, the researcher regularly took descriptive field notes that were annotated with reflective thoughts. These notes were juxtaposed with diaries and interview transcripts during the analysis.

3.6 Discussion

This chapter has introduced and described our overall research design as phenomenological oriented. That is, we are interested in understanding how meaning is created in interaction, postulating that this orientation would serve us well in researching privacy in smart homes.

In re-introducing our three research questions, we have unfolded the methodological progression of the present study. By applying inductive thematic analysis, the first of the four findings chapters has revealed the key insight that smart devices are used communally in the home. This insight motivated our grounded analysis of interview, diary, and observation data to document the constitution of privacy in communal use of smart technologies. In response to much needed innovation in research and design, we have motivated the application of conceptual framework analysis, thereby bridging the third-paradigm research insights with the second-paradigm questions. A case study approach was then selected to evaluate the applicability of our framework.

Framing the contributions of this thesis are its ethical and trustworthiness considerations. By positioning concerns of trustworthiness within the third HCI paradigm, we briefly discuss the ways in which such considerations have informed our research design. Finally, we discuss our positionality to address key questions around researcher reflexivity.

The following chapters demonstrate the application of the research approach motivated and justified in this chapter. They document how the chosen research methods were put into practice to provide insightful results that lead to important contributions. The depth and quality of these findings have demonstrated the value of the particular research approaches.

Publications arising from this chapter:

- *Martin J Kraemer, Ivan Flechais, and Helena Webb. "Exploring Communal Technology Use in the Home". In:* Proceedings of the Halfway to the Future Symposium 2019. *HTTF 2019. Nottingham, United Kingdom: ACM, Nov. 2019*

4

Exploring Everyday Practices of Technology Use

Contents

4.1 Introduction

Use of technology in our homes has been researched extensively. More than two decades of research on personal computers illustrate the influence of technology adoption on social structure and power relationships in the home [151, 176, 180, 227]. More recent research on ubiquitous and internet-connected technology in our homes have reported how new generations of computing technology are turning our homes into 'smart homes' [18, 174, 175, 288].

To achieve a proper design, the use of ubiquitous technology in homes, then, requires an understanding of individual and shared use [16, 145, 146, 188, 193, 227]. Distributions of roles and responsibilities with regard to set-up, use, and maintenance of smart home devices have been found to lead to tensions between household members [5, 191, 192]. Some prior works have also focused on individual experiences, perceptions, and attitudes in relation to smart home technology use [18, 289, 290]. Members of a household usually establish their own ways of sharing resources and dividing labour; 'taking care of internet-connected devices' is consequently not a task carried out by each user equally [151, 193, 227]. These differences influence the use (or non-use) of technology and can lead to tensions between householders [5, 18, 192].

However, questions of how exactly the use is organised and how privacy is managed as part of connected technology use in the home have not yet been researched. With smart technologies currently arriving in our homes, this is an opportune time for research. This study is an initial exploration, designed to scope out the complex problem space of individual and shared technology use in the home (see Section 3.2.2.1). To obtain a better understanding of people's lived experiences of technology use in the connected home, we answer the following research questions:

RQ-1 *What is the nature of the relationship between internet-connected technology use and privacy in the home?*
- ***RQ-1.1*** *What are practices of internet-connected technology use in the home?*
- ***RQ-1.2*** *How are these practices organised and oriented to in the home?*
- ***RQ-1.3*** *What is the relationship of these practices with privacy?*

In the following sections, we first present our interview methodology and related findings. We discuss insights from interviews to unpack elements of the communal

nature of technology use in the home. We conclude with implications for the focus and methodology of our subsequent studies.

4.2 Method

We conducted semi-structured interviews with members of the general public. We were interested in their experiences and behaviours with internet-connected technology in the home, in general and specifically with regard to smart home devices. We put particular focus on the social interaction around use of devices, asking about not only their own experiences but also the perceived experiences and behaviours observed in their cohabitants. As argued in Section 3.2.1, we did not ask them about privacy. Since we were more interested in learning about how participants would relate to the concept explicitly, we allowed them to talk about issues of privacy in their own terms. Instances of topics that came up during the interview include, for example, what they liked or disliked, the challenges they encountered, or how they or other household members used the devices.

4.2.1 Recruitment and Participants

Participants were recruited from our department, through community centres, and various online channels. As compensation, participants were offered a £10 voucher. Interviews were generally conducted in public spaces, and a few were conducted at participants' homes. Our first series of interviews focussed on general arrangements of and attitudes toward using any internet-connected technology in the home (n=18). The general public invited to participate in the first series of interviews were not pre-screened. We then started pre-screening participants when we moved our focus to newer internet-connected technology, excluding devices that would fit categories entertainment and communication (n=16). Lastly, invitations were extended to partners of previous participants as we started focusing on relationships (n=2) [1].

[1] Despite best efforts, we were not able to recruit more than these two partners.

Table 4.1: Participants by age, gender, and self-reported technology competence

		Skills		
Age	Gender	expert	competent	novice
18-34	female	0	7	2
	male	4	2	0
35-64	female	1	12	1
	male	5	2	0

Table 4.2: Internet-connected device ownership as reported by interviewees (n)

	n
Laptop	32
Smartphone	36
Tablet	20
TV	21
Voice Assistant	22
Kitchen Appliance	12
Smart Lights	7
Smart Energy Mgmt	22
Smart Security/Safety	13
Smart Fitness	16
Smart Healthcare	3

We interviewed 36 participants in the UK from November 2017 to March 2018 (Table 4.1). Each interview lasted between 30 and 45 minutes. The internet-connected devices owned by our interview participants are listed in Table 4.2.

4.2.2 Data Collection and Analysis

Arthur and Nazroo [291] highlight the importance of preparing a topic guide for interviews. Our guide included questions with regard to the different devices owned by participants, participants' general attitudes, their intention to purchase a device, experiences of using the device as part of their daily routine, changes in their own behaviours or those of their cohabitants, and how they thought and felt about these changes. We also asked participants about technology failures to elicit memorable events [292]. Participants were invited to comment on anything related to products they already owned and those they had learned about. The full interview guide can be found in the (Appendix Figure A.1).

All interviews were transcribed verbatim by the researcher. We used thematic analysis to code each interview [78]. The coding process started with a descriptive coding of each transcript (pen-and-paper method), followed by an in-case analysis. We then selectively coded across all transcripts, choosing the most distinctive and prominent codes (occurring most frequently) before transferring selective codes to the qualitative research software NViVo. Themes evolved in discussion with two other researchers at the department. We used codes and quotes to compare and contrast the emerging themes. The result of this process is presented in Figure 4.1.

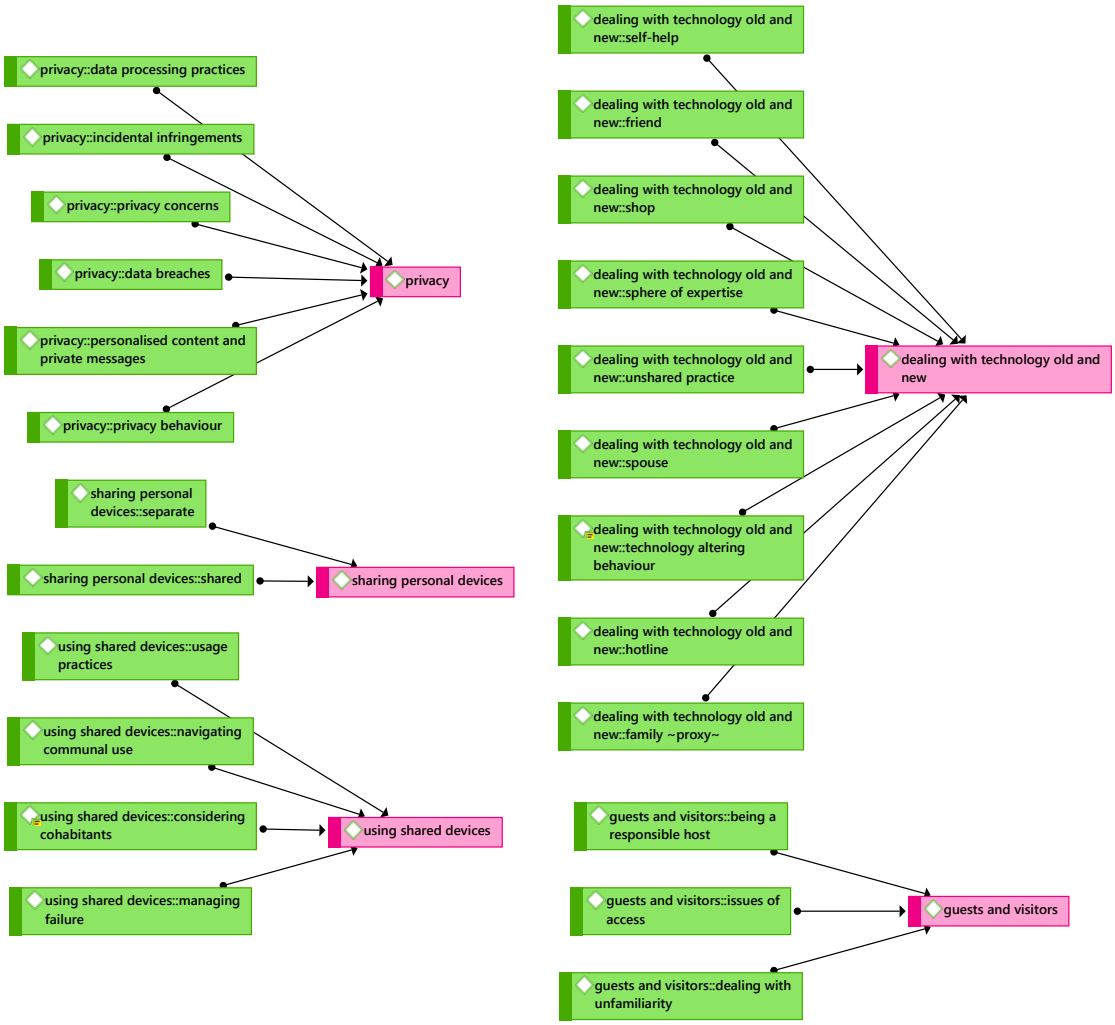


Figure 4.1: Codes and themes resulting from thematic analysis

We present five major themes to address our research questions: *privacy in the eyes of our participants*, *dealing with technology—old and new*, *sharing personal devices*, *using shared devices*, and *dealing with guests and visitors*.

4.3 Results

Closely related are studies by Garg and Moreno [34] focusing on "motivators, constraints, and practices of sharing internet of things" and Page et al. [197] investigating differences in attitudes of parents and their teenage children with regard to personal autonomy in the internet of things. These studies were conducted and published around the same time as our work[2]. Many of our findings corroborate with theirs as we highlight throughout this section.

4.3.1 Privacy in the Eyes of our Participants

While we did not prompt participants for issues related to privacy, the concept of privacy emerged in our conversations. A broad array of well-known privacy phenomena were reflected in their responses. For example, participants mentioned the concept of privacy in relation to the ideas of data protection/private messages (PI-001, PI-035), privacy as a complement to security (PI-011), or privacy as a desired quality for new products (PI-006). Privacy was also brought up when asked about concerns with regard to technology (PI-012, PI-016, PI-026), when discussing voice assistants with friends (PI-032), or when realising they could see co-users voice commands in log files (PI-018). Many of these issues are reported in prior research (e.g., [17, 193]).

Privacy concerns, attitudes, or preferences were mentioned and reflected in various ways. For example, PI-012 was not concerned about privacy at all while PI-026 was aware of some privacy and security risks but chose to accept them: "but I just enjoy technology and don't care as much". On the contrary, PI-001 was worried about someone seeing confidential messages because they were 'private' and that it was her by-principle stance on privacy. She also disapproved of companies monetising on their data and for the same reason did not use any cloud services. Without using the word privacy explicitly, PI-027 concurred with this general notion of caution, highlighting that one always needed to be careful what one said because it was potentially recorded and documented. While PI-016 was generally worried about data privacy in relation

[2] An earlier version of this chapter is published in [41].

to cloud services or the security and safety of products ("it kind of freaks me out"), he was comforted by other peoples' reviews and test reports. Particularly concerned about security cameras, both PI-016 and PI-024 said they would not buy such cameras because of privacy concerns.

The most prominent concerns related to privacy were issues of data collection and processing with different unwanted outcomes of data leaks/loss. PI-008 was concerned about 'the whole tracking thing', whereas PI-006 and PI-013 disliked the uncertainty of not knowing what a device was telling and to whom. PI-006 also blamed developers for their 'lazy programming,' where features were unnecessarily made dependent on the use of data. Other unwanted outcomes included the monetisation of one's data by social media (PI-001 and PI-011) and the risk of interference from foreign governments that would put one out of control (PI-034). Participants usually reasoned these issues by talking about acceptable risks. For example, data were thought to be "less critical" on energy consumption than on online searches (PI-011). Risks were usually acceptable because being singled out as victim by an attacker was unlikely (PI-032 and PI-035). However, PI-032 also remarked their assessment would change if they had children to protect.

Besides these general concerns and considerations of privacy and data protection, participants' reports of situated usage practices highlighted the interpersonal nature of privacy in the home. PI-018 mentioned that a friend had placed an Alexa in every room:

> so he can see like all the things is mum and his brother have been asking it. yeah.. and the other day he scrolled through and he was like, "it's a bit of an invasion of privacy" kind of (PI-018)

Noteworthy is the friend's self-assessment in which he described seeing his mother's and brother's interactions as an invasion of privacy.

While this reflexivity may or may not suggest future self-regulation, it is evidence of a situated understanding of what constitutes appropriate action, which seems to depend on partnership/household specific implicit agreements. This is illustrated in PI-009's remarks on using their partner's phone.

> but then the phone is more private because finally you have private messages and emails. I wouldn't really want to use his phone because it doesn't have the apps on it. the computer yes you can save your password and whatever you want in your browser and then you can just use it like it's yours. so it doesn't matter (PI-009)

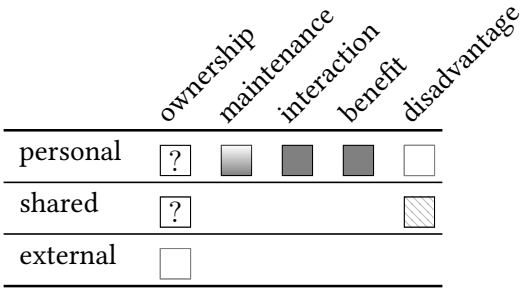
We do not intend to explain this quote by arguing that the participant respected the privacy of their partner and therefore refrained from using the phone. However, we want to highlight instead that privacy is grounded in an understanding of appropriate action that is established between cohabitants. Without closer investigation, it is thus difficult, or perhaps imprudent, to make interpretations of such a locally occasioned and inherent social phenomenon. Hence, further findings on the ways in which different people engage and interact with devices in the home will be presented in themes related to social interactions and device use, including *Dealing with Technology*, *Sharing Personal Devices*, *Using Shared Devices*, and *Guests and Visitors*. Each theme is supplemented with a diagram that summarises relevant dimensions of technology considerations and social groups (see Table 4.3).

4.3.2 Dealing with Technology–Old and New

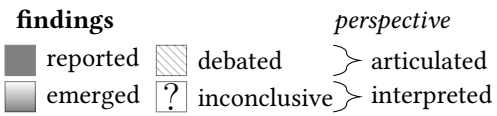
When obtaining, using, and solving problems with technology, our participants reported relying largely on existing social (spouses, parents, kids, and extended family) and work relationships [293, 294]. Many of our participants who provided advice to and sought help from others [295] considered the impact of their support, leading them to carefully consider their audience.

Support structures were based on participants' relationships and the expertise they saw both in themselves and in other people. Participants (PI-032) and (PI-034) observed how their parents were generally able to use handheld devices but relied on their children to find out about new features since they were "not very comfortable at all with fiddling around" (PI-034). This difference in competence and willingness to learn was also considered by participant (PI-011) who found her mother incapable of using Microsoft Windows and hence opted for a Google Chromebook. (PI-021) elaborated more broadly on his own expertise in providing technology support for family and

Table 4.3: Structured template for participants' experiences in light of social scope and technology orientation



Template for summaries of participants' experiences of technology orientation and social group membership. Technology orientation includes ownership, maintenance (taking care of the device), and interaction (use), possibly resulting in benefits and disadvantages. Experiences are qualified as personal, shared (interpersonal within the household), and external (outside the household). The filling encodes information on how these findings arose from our thematic analysis. Highlighted cells signal participants either *reported on* or *debated* a particular aspect. Findings marked as *emerged* imply a dimension was not explicitly articulated but arose from analysis of the underlying theme or situation. Cells with no annotations mean there is no apparent relevance, and cells marked *inconclusive* indicate that the dimension appears relevant but it is unclear exactly how.



friends. He found things like the internet or internet-connected kettles too immature for many who lacked knowledge for set-up and maintenance.

> Because if anything then it's *one more thing that they cannot manage by themselves*. So myself, I have regularly to get to my father to help him out. It's almost once every fortnight. [...] And he is still running office 2003. Even though it's not security updated and everything else. *Because I can not help him with the newest version* of Microsoft Office. (PI-021, emphasis added)

Based on the examples above, the direction of technology advice in parent-child relationships may depend on degree of expertise. While the adviser in the aforementioned cases was commonly younger than those receiving the advice, we also learned about cases where parents recommended the use of a particular smart home technology to their children. Two participants explained how they were motivated by their parents to install a home security system. It became apparent how benefits resulted in many aspects, from personal (feeling safe) to shared (looking after the dog)

to close family (peace of mind). Note that interactions with the system could be shared (looking after the dog) but were mainly personal.

Participant (PI-015) talked about how catering for many different interests meant equipping their new house with many smart home devices. She had recently moved into a new house with her partner. As she was interested in "smart things" and her partner was "quite keen with security", they installed a smart home security system. This was complemented by fire safety devices as insisted by her father, a retired firefighter who also used a similar system.

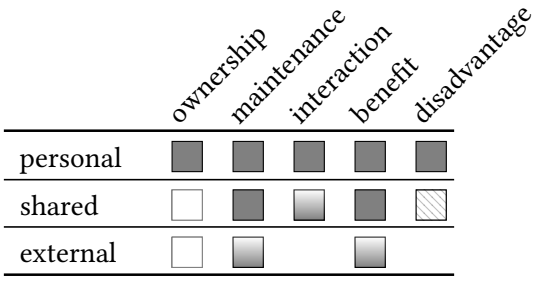
> And I wanted to easily manage the utilities and hence the smart things. And my partner is quite keen with security. And then I guess we went kind of from the security system to the cameras for the dog. To the smoke alarm. Because my dad wanted it. (PI-015)

The installation of new smart home technology could have unanticipated consequences for some household members. During the interview, the participant realised she now preferred doing online banking out of sight of the security cameras which covered the space in which she did online banking previously.

> I used to work in the sitting room downstairs at the dining table. I now only go to the desk. Especially to do online banking but also shopping or anything that has sensitive information. (PI-015)

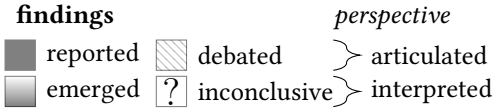
Uncertainty and unpredictability of potential effects of technology deployment were similarly reflected in participants' considerations of established support networks. A potential lack of support due to novelty and immaturity of such devices was mentioned as particularly challenging. A lack of support availability due to the novelty and immaturity of smart home devices were mentioned as particularly challenging, as seen in the excerpt below:

> With smart devices I probably *wouldn't have anyone to go to.* So I would look after them myself. [...] I would probably go to the local computer shop and ask somebody there, but *they don't tend to know an awful lot more* than I do. *I think there's so much to know.* (PI-027, emphasis added)



Summary of Theme – Dealing with Technology

Providing/seeking advice or support requires considerations of impact but also provides "peace of mind"; interactions with personal devices can become shared; and household members can be disadvantaged by unanticipated consequences



4.3.3 Sharing Personal Devices

Other studies [34, 194] reported on participants' attitudes and behaviours with regard to sharing, detailing different kinds of sharing and how they were arranged for. We report on the considerations made by our participants, including the degree to which a device was personalised (inconvenience to use someone else's device [194]), their partner's aptitude, and potential conflicts that could come with sharing. The key insight here is the ways in which participants oriented their accounts as sharers to their relationships with sharees, i.e., how the terms of sharing were explained and justified within the social context of their home.

While sharing personal devices could extend benefits of use to others, in some cases sharing was infeasible due to usage patterns or cohabitants' aptitudes. Desktop computers, laptops, or mobile phones were largely considered personal devices but could be shared under specific circumstances. Factors influencing the decision to share included the nature and goals of the social relationships (e.g., parent child, spouses, close friends), the qualities of the device, and the perceived ability of the user.

Several participants mentioned their partners were permitted to access their laptops (e.g., PI-009, PI-017). Participant (PI-032) explained how sharing laptop access was fundamentally rooted in their relationship ("for us it's always been we might as

well share anything"). They had taken the decision to simply share everything, not distinguishing what was his and hers.

> No not really. I mean we both have got logins to each others laptops. I mean.. I don't know if you are in a relationship or your friends are. But you know you sort of see couples that have been married for 50 years and still maintain separate bank accounts. And I went out with some friends of mine and they were... they have been married for a while now. And they were like, oh I will buy dinner for you tonight because you have done that for me... and I was like.. you have been married for a while now. You have got two kids. So... for us it's always been we might as well share anything. It's always been what I have is hers and what she has is mine. (PI-032)

However, being in an intimate relationship didn't mean access to devices would always be handled in the same way. Smart phones could be "too individual" (PI-017) or used "so often" (PI-029) that sharing was considered infeasible. Participant (PI-006) mentioned she would not be interested in using her partner's device as its qualities did not appeal to her:

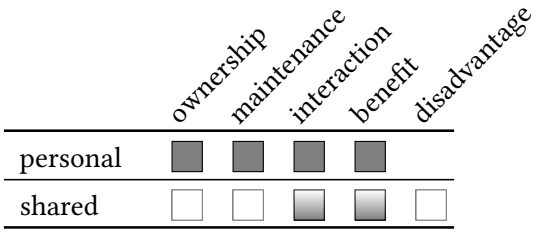
> No actually. In fact I don't even know his computer password; and that's how we like it; and I don't like it as he has BlackBerry phone. I've got a nice phone. I don't need that. (PI-006)

When asked to reflect on sharing personal devices, participants (PI-012) pointed towards their partner's aptitudes in handling devices. They preferred to keep their devices separate and to handle any arising issues on their own.

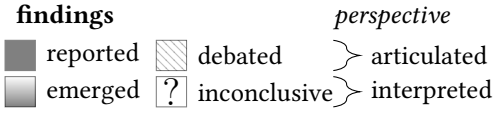
> No he would get annoyed, and then throw it on the floor. which he has done before. and then he will probably buy a new one if he had to. but he is very good in finding out how things not work.. like google and so. no, we keep our devices separate. I wouldn't ask him for advice either. (PI-012)

Participant (PI-001) emphasised that sharing their laptops would "beg for divorce" (PI-001), emphasising that the devices were "almost like a third family member" that needed attention and care-taking. However, participant (PI-001) realised there were exceptions to the rule:

> Absolutely not.. actually that would beg for divorce. [...]
> actually you are making me think. sometimes if he is out, I'm using his computer to print and that's alright, that's okay. (PI-001)



Summary of Theme – Sharing Personal Devices
Personal devices could be shared if considered sensible and desirable which could mean shared benefits



4.3.4 Using Shared Devices

We illustrate the ways in which our participants used shared devices by unpacking four sub-themes: Navigating Shared Use, Usage Practices, Managing Failure, and Considering Cohabitants.

4.3.4.1 Navigating Shared Use

The use of shared devices (entertainment or recreation) was commonly negotiated by considering each other's needs and preferences [197], and sometimes simplified through redundancy of devices. Our participants commonly mentioned spending time with their partners or family watching television. They would agree on which programme to watch if there was no strong preference by any of them. Those expressing a strong preference would usually be given priority, but there was also the possibility to evade conflicts by using a second device such as a tablet or a television in a different room.

> I thought it was the most horrible vibe ever at first. Because *I don't want to watch what he's watching but I want to be in the same room* as him. I tried reading books, but I can't read a book with the television on. (PI-006, emphasis added)

Similarly, access to and use of the smart voice assistant owned by one flatmate can be shared with his or her cohabitants. For instance, participant (PI-018) and her flatmate casually used the voice assistant while spending time together. The participant was also allowed to use the device without the owner (her flatmate) being present.

> We use [Alexa] for literally everything. Ask her what the weather is like, ask her if we ever have a conversation and we need to answer a question then we just ask her. (PI-018)

In other situations, shared access was technically not possible although socially permissible.

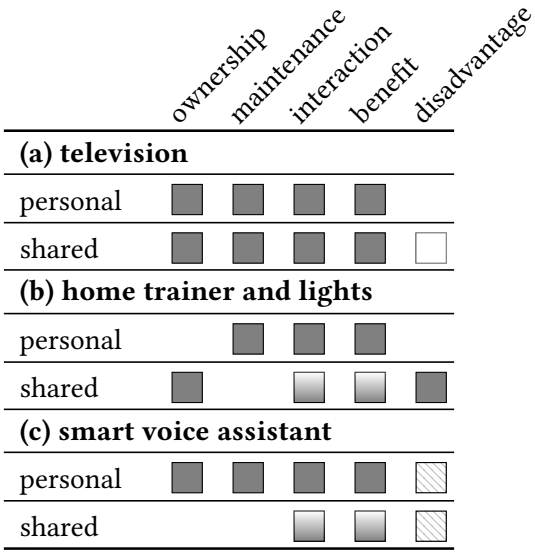
> My friend's Spotify and Amazon Prime is connected to it, so when he is driving and listens to Spotify and then I come home and start using it, it will cut his music out (PI-018)

In another example, access to a cross trainer and smart lights was shared and negotiated based on personal preferences and interest, leading to a stronger claim by those driving procurement and adoption in the first place. When both householders wanted to use the cross trainer at the same time, the two householders would trade the use of the TV as a reward (PI-035). The cross trainer of participant (PI-028) also supported different profiles for different users, so conflicts over personalisation were prevented. Similarly, participant (PI-009) would leave decisions on smart lights usage in the living room to her partner because he was "a little bit annoying" (PI-009).

4.3.4.2 Usage Practices

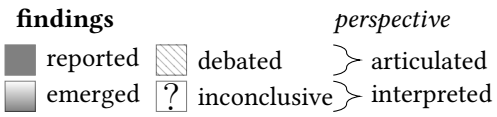
Our participants observed how they and their cohabitants developed different usage practices. For example, when it comes to device control, some people might choose to rely on others while some others might decide to use features, interfaces, or devices as interfaces in different ways from their cohabitants. This reflects the previously reported findings in that usage (adaption) of devices depends on understanding of configuration options [18, 34].

When existing devices were replaced, not everyone used them to the same extent. For instance, participant (PI-019) observed how her daughter linked her phone to a smart speaker while she listened to internet radio only and her husband did not want to use it, preferring his old stereo instead. Similarly, participant (PI-016) recalled how his mother used a smart thermostat while his father preferred manual control over the heating. Participant (PI-034)'s smart kettle was used as a "normal" kettle by his partner:



Summary of Sub-Theme – Navigating Shared Use

(a) Joint-use of mature technology (e.g., television) was common; (b) strong individual preferences influencing usage practices of newer devices (e.g., home trainer and lights; emerging shared benefits leaving individuals feeling disadvantaged); (c) benefits from sharing smart voice assistants and connected services (music streaming) and disadvantages caused by technical limitations



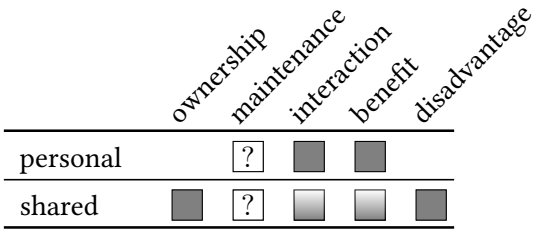
> If he is feeling cold, he is going to walk up and press the button on the thing. I mean he has an iPhone, but I can't even get him to pick up FaceTime because he doesn't understand it. (PI-016)

While participants in the aforementioned cases did not face any obvious drawbacks from their non-use of smart features, others reported disadvantages. For example, participant (PI-026) reported how he used his smart phone to control the lights while his wife preferred their Google Home. However, it was not possible to control the smart plugs that way. A similar situation led participant (PI-020) to an inconvenient workaround switching the lights on and off. While there were obvious solutions to both cases, the participants had not made use of them:

> No, she uses the Google Home. She tells the Google Home to turn the lights on. I haven't done an action for the smart plugs yet (PI-026)

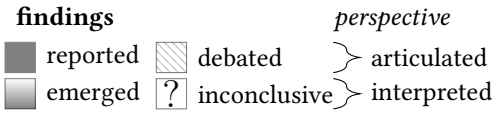
> I then have to text or send a message to my boyfriend and go like. Can you turn the lights on? And that really frustrates me. (PI-020)

Because participant (PI-020) had to use the lights as part of her daily routine, she eventually installed the smart phone app to control them. She "made do" with the system as relying on her partner to toggle the lights on her behalf was infeasible. However, such behaviour was possible in the case of participant (PI-023) who reported that her mum chose to rely on her father to control the smart TV and only ever use it in his presence.



Summary of Sub-Theme – Usage Practices

Different usage preferences (e.g., "unsmart" or manual use; emerging benefits for the household; and disadvantages to the community brought about by preferences



4.3.4.3 Managing Failure

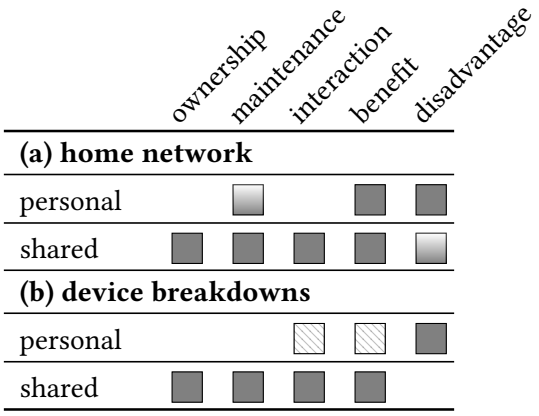
The task of taking care of the *home network* was exercised differently. That is, while the *home network* was commonly used and shared with those who rely more on it than others, participants often reported on joint efforts when taking care of it (see also [184, 293]).

Participant (PI-001) split the work with her partner. While he would be the one calling the provider, she would try switching the router off and on. Similarly, participant (PI-012) explained how her partner would attempt to fix the problem but she would call the provider if "it reached crisis". Slightly different was participant (PI-021)'s approach. In analysing any home network issue, his wife would give him a call and follow his guidance because the network set-up was "a little more complicated".

Personal preferences and expertise were important factors for participants (PI-010) and (PI-020). (PI-020) argued that while her partner was more likely to fix the television, she would be the one calling the provider and sorting out the issue since

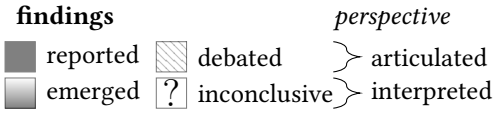
her partner did not like being on the phone and the internet was not a priority for him. For participants (PI-010), when a *personal device* broke down, the effort to recover from that break down was left to her. It was her "sphere of expertise" (PI-010). From device breakdown until recovery, the participant had to find other ways of controlling smart home devices.

Although the use of a smart home set-up as described by participant (PI-015) provided benefits to all inhabitants, it also increased her reliance on technology, explaining how she had to go "back to being more manual" (PI-015) when her phone broke. While reassured that the system was still workable, it made her realise how useful the smart system was and also how much she had gotten used to it.



Summary of Sub-Theme – Managing Failure

(a) The home network maintenance was shared with tasks distributed by expertise (emerging); (b) 'spheres of expertise' also extended to maintenance of personal devices, which not only enabled the use of shared systems but could also disadvantage individuals in case of breakdowns



4.3.4.4 Considering Cohabitants

When introducing internet-connected devices to the home, participants considered and involved their cohabitants to varying degrees. Maintenance tasks, interaction, and benefits could be shared among householders if more experienced or interested

individuals assumed responsibility of involving and educating others (see also [18]). For example, a smart home set-up (e.g., lights and security cameras) initially conceptualised and implemented by a single householder could affect all of its cohabitants. Without a single person taking the lead, this kind of negotiation is likely hampered by a lack of technological understanding [34].

Building on [18], our data is illustrative of a process more tech-savvy individuals might undergo until they recognise their need to answer to their cohabitants and assume leadership. This process, however, can take different forms.

Being aware Participant (PI-020) and (PI-024) were a couple and both were interviewed separately. Participant (PI-024) initially purchased smart sockets to control lights over the winter months and protect the house from burglaries. At the time of the interview, the sockets had been re-purposed by (PI-024) and become incorporated into a more permanent shared system. As suggested by the comments below, while both participants initially agreed on the purpose and use of the system, participant (PI-020) had been struggling with it. Two months after installation, she was still adjusting to its requirements:

> I then have to text or send a message to my boyfriend and go like. Can you turn the lights on? And that really frustrates me.[...]
> I have got the app now. But it's so. It's a little bit annoying. Because if you are already upstairs, and then you want to put the light on or off [without having the phone]. (PI-020)

The male householder (PI-024), who had been driving the technology adoption, appeared to have some knowledge of that situation:

> She likes [pauses briefly], she doesn't mind but she is not overly involved. She is quite happy with the lights and turning them on and off and how easy that is. (PI-024)

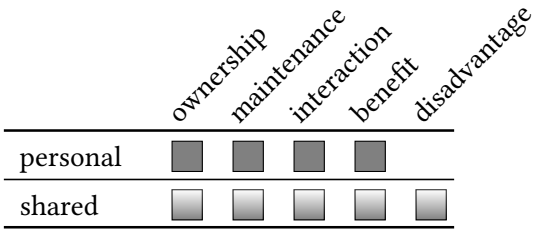
Ongoing consultation Considerations could become more easily articulated with growing expertise. Participant (PI-032) blogged about smart homes devices in his free time and semi-professionally reviewed new devices, bringing a high level of knowledge and expertise to the table. He highlighted how the use of new smart devices was

subject to ongoing consultation. Between the two spouses, it was his task to configure, investigate, and discuss the use of such devices with his partner (participant (PI-036). The partner also trusted him to act responsibly in protecting the household from any risks related to these devices.

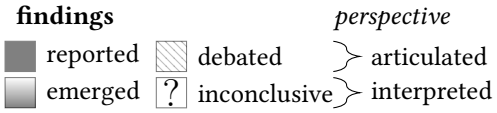
> Part of it is the family acceptance factor. Can I get on with it. *Can my wife get on with it. Can we get on with it when people come around. do they get one with it. And the other thing is how much effort it is.* (PI-032, emphasis added)

> You don't really understand how this works either, do you. And he was like no I don't. So let's not do that was a while ago and I can't really remember what it was. (PI-036)

Both examples, 'being aware' and 'ongoing consultation', demonstrate the importance of communication. Discussing implications of their co-design study with bystanders in smart homes, Yao et al. [208] suggest that communication can be part of the solution but might also be part of the problem.



Summary of Sub-Theme – Considering Cohabitants
Where the interest in smart technologies was not equal, participants considered their cohabitants' interest to varying degrees when introducing new technology to their household (emerging)



4.3.5 Guests and visitors

Considerations of other users, unfamiliarity with the system, and the need for access control were found to expand beyond the household to include guests and other visitors (e.g., contractors). Unfamiliarity with a system could inconvenience visitors, particularly when hosts spent little to no efforts introducing the system. This lack

of access control could potentially disadvantage the household and its individuals. Participants' considerations ranged from accommodating parents (PI-020, PI-036) to protecting systems from unwanted access (PI-015). These considerations were driven by a range of factors, including social norms of hospitality, intimacy, reliability, perceived ability, and personal preferences.

Issues of access

Two of our participants considered installing an Amazon Alexa in each bedroom. Participant (PI-015) raised issues of access control, not wanting potential guests to have the same level of access to the device:

> So we have talked about that. Having one in each bedroom. And so when we are up there. But *then we have guests as well* so they can access it. (PI-015)

Participant (PI-032) explained that managing access to devices could be done by informing visitors about the oddities of the home, enabling them to be respectful guests. However, he explained how he also opposed the idea of having a central, visible control unit for reasons of access control:

> You know you might just say take off your shoes before you come in. Or the bottom door doesn't lock. Don't touch the light switches. Everything else is. you know it was one of the reasons that when I looked at the home control panel that people send me here. It's just like a nice little tablet screen and you sort of meant to screw it somewhere in your house. I don't necessarily want people to come in and start fiddling with stuff. (PI-032)

Dealing with unfamiliarity

Because guests would not be expected to be familiar with the customs and intricacies of "using" the home, participants found different ways to deal with their guests' unfamiliarity. For a short stay, the household of participant (PI-020) deemed appropriate to explain to the participant's father how to use smart lights without providing him with means of control. Furthermore, the father was perceived as not being capable or interested in using new technology:

> And he was like your light doesn't work. And we were like, *no it does you just have to use the app.* [...]
> I think he just doesn't understand. My dad is not very good with technology. So, he was just like. What's the point in that. Stupid. (PI-020, emphasis added)

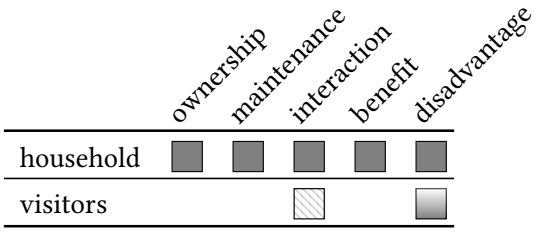
In another example, since their parents/in laws were going to stay with them for four weeks, participants (PI-032) and (PI-036) considered reconfiguring their system. Participant (PI-036) explained that after considering their guests' ability to control the smart home system using mobile phones, they reconfigured their smart home system to work independently of their mobile phones.

> We actually had my parents living with us for four weeks [...] And that required quite a major reshuffle of everything that we had.[...] both of us work [...] [The system] just went into a sort of lock-down situation [when they left the house]. So a lot of *stuff ended up getting disabled.*
> [...]
> We considered [connecting their phones] and I decided probably not because my dad is not very technical. I think my mum the same, and they certainly had other things to think about because they were moving to the other side of the world, and we thought let's try and make this experience as stress free as possible, and so we decided against that. (PI-036)

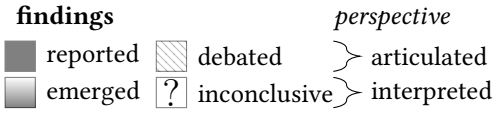
Being a responsible host

Responsibilities as hosts ranged from tackling unexpected issues with which guest would be immediately and obviously confronted to managing problems the host were already aware of. For instance, participant (PI-032) came to realisation when a lawyer friend who raised the point it was his own moral and possibly also legal obligation to mention indoor cameras (and other devices) to his guests:

> I mean the most important thing you have to tell people when they come around is "don't touch the light switches" which you know is fine. Because they are set to come on when they need to no one ever does. And the interesting thing is. I had a lawyer friend around and he said that I ought to warn people that there are cameras in the house and they might record people. [...] But also, that there is an amazon device which is always listening. But I think he has got a point. You know. You should tell people. (PI-032)



Summary of Theme – Guests and Visitors
Participants debated access for visitors and guests, and touched on disadvantages arising from smart technology in their home (emerging)



4.4 Discussion

In the previous section, the findings on the different facets of shared use of internet-connected technology in the home were presented. This section summarises and discusses the findings' relevance for research and design.

4.4.1 Communal Use

In *Privacy in the Eyes of our Participants*, we reported on unprompted discussions of privacy during the interviews, highlighting a broad array of well-known concerns expressed by our participants. While there was only one participant that explicitly mentioned privacy as an interpersonal challenge of appropriate conduct (PI-018), we found similar social considerations (e.g., relationship-appropriate behaviours) reflected in other instances (e.g., PI-009's considerations of accessing their partner's phone, or PI-015's online banking behaviours triggered by security cameras). We concurred with others before us in highlighting that notions of *appropriate behaviour locally occasioned* are situated and specific to both the physical environment and the people involved (e.g., [122, 230]). We also reported on the themes which highlighted situations in which people interact *because of* technology.

Our findings suggest in a number of ways that the use of technology in and around the home is in fact *communal*: The use is communal in the sense that individuals

manage use and sharing of technologies in relationship appropriate ways, taking into account not only each other's personal characteristics but also the potential impacts of technology on one another (e.g., how well someone gets along – Section 4.3.2). It is also communal in the sense of appropriate actions such as when individuals bring new technologies to the home and consider ways to make the technology work for the community of users (Section 4.3.4). We also found that decisions and arrangements for *Sharing Personal Devices* were rooted in social considerations, i.e., oriented to their social relationships within the community. The use of technology is also communal when taking into account guests and visitors. The group of users in the home, then, is a fluid concept. Intervention by technology owners at the prospect of someone being affected by smart technologies in one way or another might become necessary, or even a prerequisite for being considered a 'good citizen' (Section 4.3.5).

The use of technology is reflective of everyday concerns (e.g., sharing televisions, home trainers, or smart voice assistants), and these concerns then embody the moral order of the home (e.g., appropriateness of sharing personal devices or using secondary devices while allowing the partner to use the home trainer). In this regard, the use of technology in the home can be characterised as communal. This insight resonates well with our discussion of households as communities (see Section 2.4).

4.4.2 Facets of Communal Use

Users' engagement with technology is shaped by features within their situated contexts and their own sense-making. While differences in use and engagement occur between more mature internet-connected technologies and relatively 'new' smart devices, in all instances they are rooted in the social context of the household.

Households are communities and part of communities. Although the literature review in Section 2.4.2 discussed households as communities (i.e., as having their own moral order), the findings demand further discussions of the ways in which non-residents can become members of the household's moral economy [154]. Our findings suggest the need for community members to make available in talk and action

the moral order of the household for non-residents (just as much for residents). More research is needed to understand the ways in which moral and social order is established at household boundaries. For now, we can say that community members come into contact with smart devices and then learn something about the local moral order around the use of these devices in order to 're-create'/'re-affirm' their understanding of what is normal and appropriate.

Set-up, administration, and use are arranged for within a community. Our findings suggest that a dynamic division of roles and responsibilities (in the sense of who does what) in the home corresponds to the inherently 'messy' nature of the home [166] where different kinds of relationships overlap, all affecting and effected by co-present technologies. We corroborate with others [34, 194, 293] in emphasising the importance of considering the collective. However, it is difficult to delineate the group of people involved with the set-up, use, and maintenance of technology. For example, a non-cohabiting relative can become the administrator of the device despite not being its regular user (see also [295]). Domestic workers can either be affected by or required to use a device. Similarly, household members might not have the ownership or administrative access even though they are expected to use the device (e.g., adolescents helping their parents, parents managing their children, or adults supporting their elderly parents) (see also [5, 18]).

When managing access, individuals consider an array of personal characteristics. Participants clearly considered the nature of their relationships with, skills and expertise, character traits, and aptitude of the person they intended to share with. The decision to share smart phones, laptops, and other gadgets was deeply rooted in these aspects. In line with prior studies, our data similarly reported on situations in which sharing was permissible and that the purposes as well as the preparations for sharing were made available [34, 194, 216].

'Communal' devices require management often assumed by individuals. Similar to Garg and Moreno [34]'s work, we found that while some devices were not necessarily designed for collective use [5, 34], they had communal impact (e.g., smart

security systems or thermostat) [191, 214, 296]. We refer to such devices as *communal devices*. Our findings corroborate with others in suggesting that this form of 'digital housekeeping' is typically carried out by single individuals, which ultimately may become source for tension and conflict [5, 34]. In some case, these tensions and conflicts are product of the use of technology itself (e.g., discussions over configuration settings); in other cases, they might surface or fuel underlying and pre-existing conflicts. Most importantly, however, is the fact that these tensions and conflicts are situated within the moral economy of the household. Because members of the household frequently share resources and distribute labour, they also navigate such social situations just as frequently. As our findings suggest, there is much individuals can do to help others understand what a device does and how it works.

Owners can hold other users accountable, even for shared devices. Garg and Moreno [34] suggested that the notion of ownership remains relevant even in the context of inherently shared devices (cf. [194]). In our data, this was evident in established routines that involved devices owned by other people (e.g., using someone's fitness tracker or printer). Those borrowing the devices were not only expected to exercise care but also held accountable for any issues arising from their use. Tensions might arise from explicit or implicit disagreement over these notions of ownership, particularly when the device has communal implications. Therefore, it is important to understand what form these notions of ownership take and how they come about.

4.4.3 Researching Privacy and Communal Use

Communal implications of internet-connected devices are difficult to anticipate. The security camera and online banking anecdote illustrate such difficulty, highlighting that infringements of privacy may not be perceived or discussed but often dealt with in other ways (e.g., through behavioural change). Issues of privacy are closely linked to the products themselves and their presence. Unwanted effects of device use are not always unanticipated or benign and can bring tensions to interpersonal relationships [5].

Researching these issues requires careful consideration. Everyday concerns reflected in communal use are part of the home's moral order [154], and as such are

subject to change over time and contingent on the nature of technologies themselves. Devices use is also situated in the home. That is, household members attribute to and bring about meaning through their actions of using specific devices. This meaning is embedded within the relationships of household members and their personal characteristics. Understanding this situatedness is crucial to understanding communal implications, particularly those that are difficult to anticipate. The questions of who does what with which device under which circumstances and for what purpose become important.

We call for more interaction-focussed and situated research approaches (e.g., [145, 146]) to consider the phenomena of communal use and privacy as evolving over time and in relationship to new and old technologies.

4.5 Conclusion

This chapter explored participants' self-reported behaviours and their observations of other household members with regard to technology use in the home. We reported participants' practices and their implications, illustrating how technology use in the home is *inherently communal*. Our findings showed a complex relationship between communal use of internet-connected technology and various aspects of privacy (digital and physical) that took shape in practices of sharing and using shared devices, particularly where communal implications were difficult to anticipate. Drawing on our data and related literature, we outlined how communal devices were typically taken care of by a single individual anticipating or remaining ignorant of such implications. Individuals relied on past experiences and personal characteristics when approaching the use of a device, and because those past experiences and personal characteristics were inevitably not the same for every household member, devices were used to different extents. Moreover, individuals exercising authority and holding others accountable for their use of devices could cause tensions within the community.

As we have illustrated, all of these actions are not so much oriented towards conceptualisations of privacy but towards the social context in which they occur. While we have discussed considerations of relationships among household members as well as personal characteristics of sharer and sharee, what we have highlighted are everyday

concerns implicated in communal use of these devices. To better understand how issues of communal use (e.g., tensions and conflicts identified in the literature) are related to privacy in the eyes of participants *and* to the design of devices themselves, more longitudinal and observational research on communal use and privacy are called for. We answer this call with a study of households' experiences of communal use of smart home technologies in the next chapter.

5

Unpacking the Social Organisation of Communal Use and Privacy

Contents

5.1 Introduction

Households are communities in their own rights with shared space, resources, and a common history [154]. Household use of technology, as shown in the previous chapter, becomes part and parcel of relationships among community members. In other words, technology use in the home is *communal*. The thematic analysis of semi-structured interviews on the use of internet-connected devices has highlighted how not only members of the household community but also individuals external to the household took on tasks of set-up, configuration, and maintenance. In consideration of other household members' needs and desires, executing these tasks on behalf of the household brings about challenges of 'making technology work for the household'. These considerations include, for example, questions of device placement, appropriate use, and adequate configuration. However, the implications of these efforts regarding technology use are difficult to anticipate. Because the community of household members is in some way affected, using devices hence requires continuous renegotiations of moral and social order in the home.

Heeding the call for longitudinal, empirical research articulated at the end of the previous chapter, this chapter reports on an ethnomethodologically informed study. It unpacks the social organisation of communal use and its relationship to everyday concerns of privacy by investigating household members' interactions with one another, with their social relationships, and with smart devices in their home. An opportune site to research privacy, smart home devices that either invite communal use (e.g., smart lighting or smart thermostats [34]) or reportedly trigger strong privacy concerns in communal spaces (e.g., smart security cameras or voice assistants [200, 214]) are the

study's primary topic of investigation. We present a grounded analysis informed by sensitising concepts from EM (everyday activities, natural accountability, and dimensions of work – Section 3.2.2.2) to answer the following research questions:

> ***RQ-2*** *How does the nature of the relationship between internet-connected technology use in the home and privacy manifest in-situ?*
> ***RQ-2.1*** *How is communal use of smart devices in and around the home organised?*
> ***RQ-2.2*** *How is privacy oriented to as part of this organisation?*
> ***RQ-2.3*** *What are implications for product design and development?*

Prior work have focused on smart device adoption from perspectives of individuals (e.g., [193]), different user groups (e.g., [143, 208]), and households (e.g., [18, 25, 145, 205, 288]). More recently, researchers have focused on interpersonal relationships in households (e.g., [5, 213, 297]) and with a wider community (e.g., [298]). However, this study is the first to (1) allow households to choose a number of off-the-shelf smart devices; (2) observe their installation and use over an extended period of time (at least six months each); (3) focus on the communal nature of use[1]; (4) document the communal nature of smart device use; and (5) highlight the contingencies of this nature with the design of devices themselves.

In the following sections, we describe our study, introducing our approach to data collection and analysis. Next, we present our findings on four categories of interactions, roles, moral order, and rules before discussing the social organisation of communal technology use in the home. We draw on these findings to offer implications for design of communal use.

5.2 The Study

Our literature review has highlighted the importance of understanding life within the home as highly dynamic and recursively *interlinked with the ongoing establishment of moral order* (e.g., [16, 154]). We have positioned privacy within these household communities as intimately bound up with social considerations in the home (e.g., those concerned with the management of relationships) that dominate the very use of the

[1] In the sense of [154], they "possess a tradition, a moral order which frames and guides behaviour as well as the use of household facilities and technologies" (see also Chapter 4.3.4.2).

controls designed to manage interpersonal issues of privacy in the home (e.g., [22, 145]). Finally, we have highlighted how interpersonal considerations are also intimately linked with the adoption and use of technology in the home (e.g., [18, 288]). These insights suggest a strong orientation towards normative aspects, foregrounding the questions of *who does what, how, and why*.

As discussed in Section 3.2.2.2, we reside with [20, 145, 227] in choosing to be indifferent about existing theories and refrain from focusing on particular social phenomena from the outset. That is, we research privacy as a phenomenon with special focus on social interactions and their meaning for a community.

To answer our research questions, we recruited six families to join a six-month EM informed interview and diary study of household technology use (Figure 5.1). In keeping with the orientation outlined in the previous paragraph and motivated in Section 3.2.2.2, we provide an EM informed grounded analysis of the resulting data set.

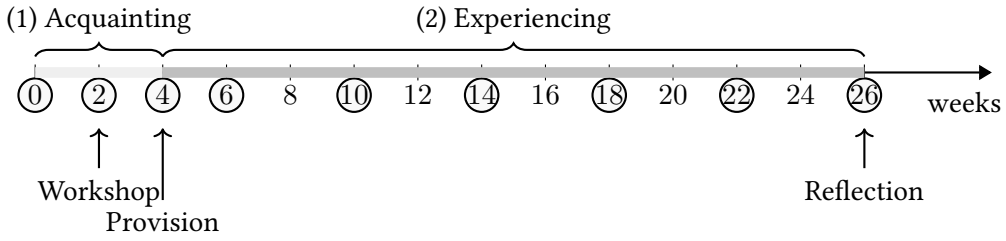


Figure 5.1: Planned progression of home visits (circled) vs actual time per household varied to accommodate for seasonal and family holidays. In (1), we got acquainted and conducted a smart home planning workshop. Phase (2) started with the provision of new devices followed by regular visits to learn about their experiences.

5.2.1 Recruitment and Participants

We recruited by reaching out to participants from our previous studies, and through social media and online platforms. Prior experience with smart home devices was not mandatory, but experience with instant messaging and/or email was required to participate and allow for ease of communication with the researcher. We further focused on families with children in response to previous studies which have suggested that business of everyday life increases desire to use internet-connected technology in families with two adults in full-time employment and their children [152].

A total of 10 families initially expressed interest. We offered a 'meet and greet' on Skype or in person to clarify details of the study. Thereafter, four families with children agreed to join the study. The fifth family with children joined the study following a second online recruitment drive, and the sixth family without children was accepted when our efforts to recruit families with children remained unsuccessful. Details on these families, the devices they owned, and devices they obtained as part of the study can be found in Table 5.1.

Participating families received a cash reward (£200) paid in four instalments over the course of the study and were allowed to keep the devices as incentive (£600-800). Families were allowed to drop out of the study at any point in time and without any explanation. When dropping out, they also had the opportunity to withdraw their consent for the use of diary and interview data. In any case, they were allowed to keep the devices and the financial rewards received up to the point. Out of the initial six families, Household 5 dropped out about four weeks into the study for health related reasons. They had not yet received any new devices, and they did not withdraw their consent. The first three interviews with this household are part of the analysis.

5.2.2 Data Collection

The first household visit started in August 2019 with our final visit in May 2020. Due to the first UK national lockdown caused by Covid-19, our in-person interviews scheduled between March 23rd and May 10th were moved online, and our conversations naturally gravitated toward health, safety, and the challenges of working and learning from home.

To facilitate communication with the families, we set up a web portal with household-specific participation pages (Figure 5.2) and the messaging service Threema was used[2]. We also asked participants to keep diaries throughout the study.

Home Visits

During each of the visits (30-60 minutes of unstructured interview), we encouraged all family members to share their experiences of using any of their internet-connected

[2]https://threema.ch/en – chosen for its WhatsApp-like UX but better data protection

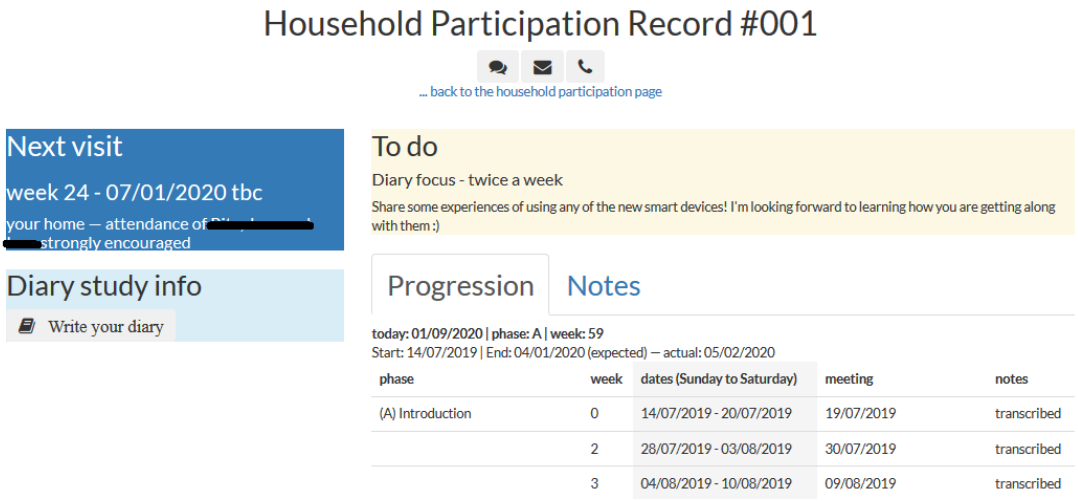


Figure 5.2: Screenshot of household participation page—each household received a login detail to their individual page where they could find information on progression and summaries of researcher notes from past meetings (Dashboard in Appendix Figure B.4)

technology. For example, in households one and four, the researcher would arrive after the family had finished dinner and join them for a cup of tea at their dining table. We engaged with participants in conversation for as long as they preferred, but we were equally happy to just listen to what they had to discuss between one another. Naturally, the conversation for the first few minutes evolved around what happened at school or work but eventually turned towards experiences with smart devices; for example, through recalling conversations with friends/colleagues about these devices. We generally made sure that every household member was given time to share their experiences, actively involving children in the conversation in so far as parents were not doing so already. We used a simple dictation machine to record these meetings.

Researcher Diary

Field notes of each visit were kept in the researcher's diary after the meetings. The researcher employed a three-step note-taking approach: (1) a short summary of issues and topics discussed during each visit to be posted on the household participation page; (2) descriptive observation notes on interactions with devices and between participants; and (3) interpretative notes and reflective comments on the researcher experiences.

Table 5.1: Participating households and their networked devices.

Households and Participants (household income)	**Networked Devices**
H1 (£70-80k): Rosa (mother, 40s) and Jaco (father, 40s), living with three children Iria (daughter, 16-18), Peter (son, 6-8), and Tom (son, 1-3)[1]. Up to two student lodgers (16-18)[1,2] regularly stay with them. Rosa (postgraduate degree) works as a health practice manager, and Jaco (undergraduate degree) works for an international automotive company.	*pre study*: smart tv, smart phones, iPads, and laptops *new devices*: smart speakers, smart display, smart cameras
H2 (£70-80k): Monique (mother, 40s) and Adam (father, 40s), living with their son Eric (1-3)[1]. Monique (undergraduate degree) works in communication management, and Adam (undergraduate degree) works as an IT manager at a local University.	*pre study*: laptops, smart phones, streaming devices, smart meters *new devices*: smart speakers, smart display, smart camera with doorbell and chime
H3 (£40-50k): Carrie (mother, 40s) and Felicity (daughter, 10-12) live together. Paul (father, 40s undergraduate degree)[1,2] pays a regular visit to his daughter. Carrie holds a postgraduate degree and works as a support teacher in special needs education.	*pre-study*: Computer, Smart Phone, e-reader (Kindle) *new devices*: smart phone, smart speaker, smart display, streaming device, smart thermostat
H4 (£60-70k): Carla (mother, 40s) and Aaron (father, 40s), living with their children Malte (son, 10-13) and Ester (daughter, 8-10). Carla (postgraduate degree) works as a UX Designer and Aaron (undergraduate degree) as a design teacher. Both work regularly from home.	*pre study*: smart phones, smart speakers *new devices*: smart speaker, smart display, smart camera and doorbell, smart lighting
H5 (£70-80k)[3]: Frank (father, 40s) and Cassie (mother, 40s), living with their sons Donald (9-10) and Fabian (6-8). Frank (postgraduate degree) works in innovation management for a local university, and Cassie (postgraduate degree) works in furniture restoration.	*pre study*: smart phones, tablets, laptops, streaming devices, smart speakers, smart lighting, smart thermostat, smart turbo trainer *new devices*: –
H6 (£100-150k): Tobias (husband, 30s) lives with Sylvie (wife, 30s). Tobias (postgraduate degree) works as an innovation director developing start-ups. Sylvie (undergraduate degree) works as a midwife at a local university hospital.	*pre study*: laptops, streaming devices, smart thermostat, smart phones, do-it-yourself Raspberry Pi system *new devices*: smart display, streaming device, smart bridge for Apple Homekit, smart switch, smart lighting, smart doorbell

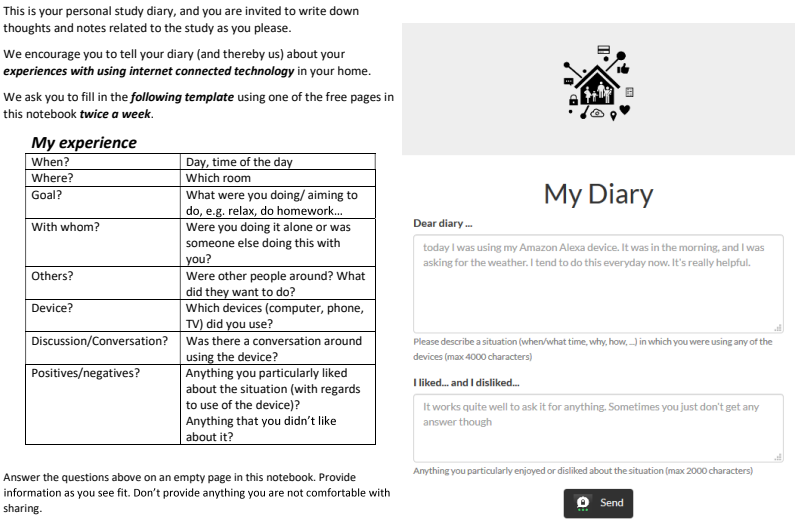
[1] Not actively participating.
[2] Not permanent household members.
[3] Household left the study after smart home planning session due to illness.

Participant Diaries

Participants were invited to choose either paper-based or digital diaries; most participants preferred the digital version which we run using Threema messenger. We

encouraged participants to log instances of shared use of any internet-connected devices they owned. Having realised early on that an initial template was too structured (e.g., requiring information on which device, with whom, where, for what purpose, pros/cons—Figure 5.3a), we simplified the template by asking for their overall experiences (Figure 5.3b). During part (1) of the research, we asked about their experience using a device they owned already. From part (2) onward, we encouraged participants to comment on their experiences with the devices with which they were provided. Diary entries also served as starting points for conversations during our home visits.

Figure 5.3: Initial and revised online diary templates and notebook versions of participant diaries



This is your personal study diary, and you are invited to write down thoughts and notes related to the study as you please.

We encourage you to tell your diary (and thereby us) about your ***experiences with using internet connected technology*** in your home.

We ask you to fill in the ***following template*** using one of the free pages in this notebook ***twice a week***.

My experience

When?	Day, time of the day
Where?	Which room
Goal?	What were you doing/ aiming to do, e.g. relax, do homework...
With whom?	Were you doing it alone or was someone else doing this with you?
Others?	Were other people around? What did they want to do?
Device?	Which devices (computer, phone, TV) did you use?
Discussion/Conversation?	Was there a conversation around using the device?
Positives/negatives?	Anything you particularly liked about the situation (with regards to use of the device)? Anything that you didn't like about it?

Answer the questions above on an empty page in this notebook. Provide information as you see fit. Don't provide anything you are not comfortable with sharing.

(a) Initial paper-based diary template

(b) Revised diary template (online)

Smart Home Workshop

To prepare participants for the planning session, we shared consumer insight reports with the participants on smart home planning[3] and test reports on particular devices[4]. All of these reports were created by Which?, a popular UK product testing and consumer information organisation.

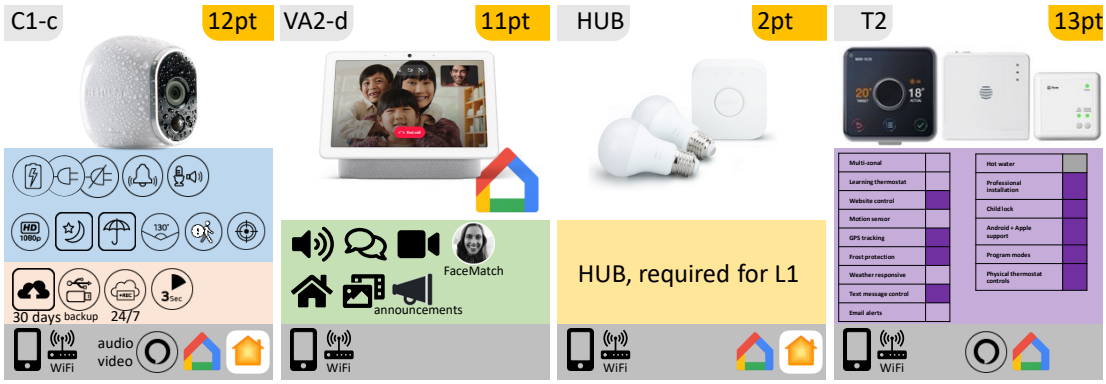
[3] e.g. https://www.which.co.uk/reviews/wireless-and-bluetooth-speakers/article/how-to-set-up-a-smart-home

[4] e.g., https://www.which.co.uk/reviews/smart-thermostats/article/are-smart-thermostats-worth-it-aEmy52Z0vdnr

We conducted a workshop during the third visit to identify devices of interest. To this end, we created a card deck (Figure 5.4) with details on device features. Using a points system to represent the costs of our devices, we asked participants to build two sets of cards worth £800 and £600 respectively. Our motivation for this approach was two-fold: (1) we were interested to see whether workshops would bring forth notions of ownership with regard to set-up and ongoing use (see also [34]); and (2) the workshop required participating families to arrive at a consensus through discussion, thereby revealing something of their social and moral order.

We ordered and delivered the devices to our participants' homes during our next visit (Appendix B.1).

Figure 5.4: Examples of cards from our smart home planning session. The card deck represents the four main categories of devices we included (not exclusively): smart security systems, smart speakers/displays (voice assistants), smart lighting systems, and smart thermostats



5.2.3 Data Analysis

The final data set included 47 interviews (∼45 minutes per interview), 47 field notes (∼200 words per note), 13 participant diaries (∼1,485 words per diary) and 22 photographs. The data set was imported into the qualitative data analysis software "Atlas.TI 8", which supported our coding and diagramming process throughout.

The research approach for this chapter is motivated and discussed in Section 3.2.2.2 where we outline a synergistic relationship between an EM informed study and a GT inspired analysis. The approach suggested empirically generated [264] representations demonstrating the social organisation of the setting under investigation

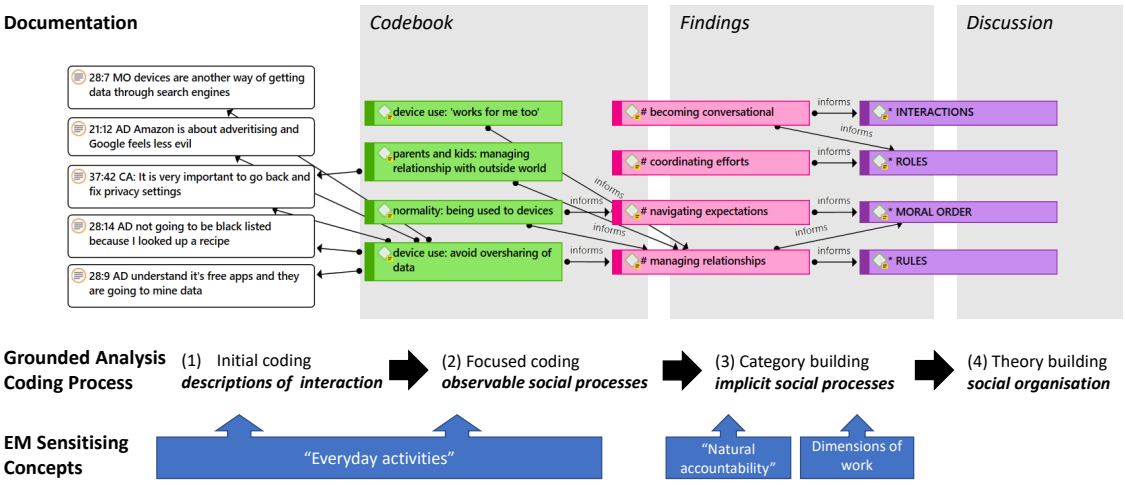


Figure 5.5: Overview of the analytic process including quotations with initial codes (white), focused codes as observable social processes (green), implicit social processes as candidate categories (pink), and theoretical codes (purple). The figure also illustrates the use of sensitising concepts (blue).

be derived by providing 'general' implication for design [228]. In this study, we used GT process to guide and focus our efforts in organising and navigating our data set. We refrained from analytic construction of traditional social science theories. However, we recognised their utility for areas of design, product development, and policy. The structure and organisation of our findings should allow designers to independently navigate our record.

As detailed in Figure 5.5 and further described below, our analytic approach allowed us to produce a structured account of phenomena related to communal use and privacy that emerged from our data. Such account then served the need for actionable, reusable, and abstract insights [242]. Note that the use of standard GT terms and their role in our grounded analysis is illustrated in Figure 5.5. Theoretical codes (purple) in our analysis are inspired by Crabtree, Rouncefield, and Tolmie's [228] generic implications for design. They are informed by categories (pink) which are best understood as implicit social processes that relate to observable social processes (green).

Discussing the benefits of importing GT for empirical studies, Charmaz and Mitchell [242] suggests adapting its methods for "specific objectives of a study and for the style of the researcher". To do this, the procedure, which was repeated for each transcript, field note, and participant diary of every household, was as follows.

First, the researcher and a colleague individually read the document. They then met to code the artefact jointly, incident by incident as description of interactions (e.g., [242]). The artefact was coded with a focus on preserving actions and comparing data with data *initially*. Codes were captured as names of quotations (white in Figure 5.5). During this step, *focused* codes describing *observable social processes* (coded in green in Figure 5.5) began to emerge. These social processes manifested over time through constant comparisons with each other and with quotations/data.

Once all the artefacts pertaining to one household were coded, the researcher created networks that linked quotations with codes and emerging categories. Investigating these networks, the researcher began to write memos which served to manifest categories (pink in Figure 5.5) while drawing on sensitising concepts presented in Section 3.2.2.2. Once these memos were integrated with the household coding networks, they served as reference points for comparing codes and categories between incidents and households[5].

The coding process was not focused on modelling behaviours related to privacy. However, the coding process on social processes that contributed to the organisation of communal use was inevitably tied up with everyday concerns of privacy [145, 227].

Core concepts (coded in purple in Figure 5.5) emerged through iterative comparisons of implicit social processes (categories, pink) with observable social processes (focussed codes, green) and descriptions of interactions (quotations, white). The social organisation (theoretical concepts, purple) represents links between categories and outcomes of the meaning brought about by their social processes. Their meaning is created and reflected by social processes, contributing to the establishment of social organisation. It is important to note that our intention was not to analytically construct a generative or prescriptive theory but rather to empirically generate a descriptive/sensitising framework.

Once we were confident that we have arrived at an insightful and stable representation of the social organisation of communal use, we iteratively queried existing EM related literature to verify codes, categories, and emerging concepts. At this point

[5]Note that we did *not explicitly* apply *axial* coding in Strauss's sense but refined our candidate categories throughout the analysis, i.e., in promoting focused codes to candidate categories or in merging two categories.

our analysis was complete, i.e., 'theoretical saturation' [245, 270] was achieved. The final product of this coding process is depicted in Figure 5.6.

5.3 Findings

An important insight corroborates with the previous chapter and confirms our methodological orientation: participants rarely referred to privacy explicitly, and the concept did not appear to be an immediate concern in their practical actions—at least not in the ways referred to in the literature on informational privacy that concerned with control over information. Instead, participants' perspectives on privacy were bound up with other situational considerations and reflected in interactions of everyday use. To answer the research questions for this study, it is necessary to take as a starting point an exploration of these activities before turning towards the ways in which privacy is embedded in everyday interactions.

In so doing, the novelty of these findings is two-fold: first, a framework of the social organisation of communal use that builds on social processes presented across concepts of *interactions, roles, moral order, and rules*; and second, anecdotal evidence on the relationship between the reported challenges of communal use (e.g., power imbalances) and the framework.

5.3.1 Interactions

The relevance of devices to the social and moral order in the home becomes visible in interactions. Interactions refer to when individuals (household or members of the wider community) communicate with one another face-to-face or mediated by devices (generally by making sense of a system's state and recent changes, but also by facilitating asynchronous communication between individuals). Prerequisites for interactions are, at the very least, opportunities and 'being conversational' (familiar) with the ways a device can be used. The concepts of roles, rules, and moral order discussed later manifest in interactions.

Participants draw on various resources to make visible and constitute the relevance of smart technologies in their home. The findings describe a household's collective

Figure 5.6: Final Grounded-Theory coding structure

ability to talk about a device in terms of its purpose and how that purpose is established. Contributing to this ability are a number of factors: experiences with similar kinds of devices (e.g., smartphone-based voice assistants being similar to stand-alone voice assistants), exposure to reports on these devices or advertisement for these devices in the media, and time spent using devices. Collectively, experiences and insights are shared in conversation through purposeful demonstrations, teaching, and observation. In these ways, household members learn about others' usage practices, usage preferences, and possibilities of use. Interactions also hinge upon familiarity with one another as part of a decision-making process such as choosing devices for study purposes.

The starting points for households' considerations of smart devices varied though all of them had some prior knowledge of the subject. Our interviews offered a platform to share insights and ask questions about the devices, thereby establishing a common understanding of what the features of a device were and how these features could be used as shown in the following vignette. In this conversation between Cassie and Frank during the smart home planning workshop, the couple is exploring the use of a smart door lock.

Vignette 5.1 *Household 5—visit 3*

Frank: As in a smart door lock.

Cassie: A smart lock.

Frank: Yes. Because …

Cassie: So we just have to carry a key as well as a backup?

Frank: Well, they usually have …

Cassie: In case the phone dies.

Frank: They have fobs, but it is also proximity with your phone or whatever as well.

Cassie: Yes.

Frank: And I think it is the Ring one that has also got the video in it, so that if someone is there and you are not, like say your folks turned up early and we were not back …

Cassie: Oh, yes.

Frank: …you can let them in.

Cassie: Oh, that is cool. What if the postman knocks and you are not there? You could say where to leave it?

Frank: Yes, yes. So I mean that would be, I mean that will be interesting to find out …

Researcher: Yes.

Frank: …about either what the options are or what you would suggest in that context.

After learning from Frank about the core functionality of a smart doorbell, Cassie imagines usage scenarios while seeking confirmation to her assumptions from Frank. Together, they assess the utility of the solution. Cassie's considerations thus contribute to an evaluation of practical contingencies under which the system needs to be able to operate. The combined experience of both household members provides a holistic picture. Noteworthy is also how the practical everyday use serves as the starting point for considerations ("we just have to carry a key as well as a backup?" and "in case the phone days"), only after which does Cassie consider possible futures of a postman delivering a parcel or the parents being early for a visit.

By drawing on considering everyday practices, household members can benefit from jointly anticipating usage scenarios before purchase. While single household members are likely familiar with "whatever else is going on in the home" [16], they will not be able to fully anticipate practices, needs, and desires of others. Usage practices vary between people (see also Chapter 4) and therefore need to be reflected upon. Although the discussions above take place before the participants obtain a particular device, the sense-making process of *becoming conversational* we described is useful in highlighting a sequence from understanding what a product does and how it fits with everyday practices to envisioning possible futures with the devices; all of which happen in conversations between household members.

However, a household's ability to become conversational depends on opportunity and access to knowledge. While opportunity can be created by design, and knowledge is available through members of the household and resources we shared prior to the meeting, there are limitations to this approach: first, the features considered for appropriation by household members are those advertised by manufacturers only (thereby unlikely to include considerations of privacy [204, 300]); second, additional knowledge through household members may not always be available [301]; and finally, not all household members are involved in the processes outlined above (e.g., children frequently were involved only later).

When relatable experience and knowledge are not readily available, participants may involve the researcher more closely in their exploration of smart devices. In

Household 3, Carrie's approach to smart home planning revolves around replacing old devices, much as she had done before the study. Felicity and herself chose a new smart phone and a smart thermostat as essential devices. After having learnt that a smart voice assistant could replace their old stereo, Carrie chose a Google Home Hub Max. The vignette below shows some considerations involved in making sense of the configuration, most of which are trivial for Carrie and Felicity but later become apparent in their engagement with the researcher when they begin to learn about the 'inner workings' of the device. They experience that the impact of configuration settings on device functionality is not always articulated by manufacturers as part of the configuration process.

Vignette 5.2 *Household 3—visit 4*

Felicity: Okay. 'When you use your assistant to talk to a service, Google shows information.' Well, we are not going to talk to a service, are we?

Carrie: I think you will otherwise you will not be using it, Felicity.

Felicity: Oh, so, "Shares the information about what you are asking." So, if I said, "Karate videos" ...

Carrie: Yeah.

Felicity: ... it would say "YouTube karate videos, please"? Probably do not want 'please'. It is actually surprisingly quickly.

Researcher: Did you decline that one?

Carrie: It did not give me an option to decline, I do not think. It has just given me information.

Researcher: Okay. If you go back.

Carrie is left here to presume that "otherwise you will not be using" the product, that is, the device might not work. In fact, later on this was proven true when their decision to not collect "web and activity data" excluded them from free access to YouTube without being offered a conclusive explanation. While this kind of knowledge is shared between mother and daughter through the process of jointly setting up the system, the situation is different for the smart thermostat which was installed by the energy provider under supervision of Felicity's father[6]. It was Felicity who explained the use of the thermostat's wall-mounted control panel to her mother.

[6]Note that although not a resident, the father was a regular visitor to their home.

Summary Interactions refer to individuals using devices or communicating with each other. For household members to effectively negotiate the use of devices in interactions, conversational familiarity is required. As this section has shown, familiarity progresses on different levels starting from a priori considerations grounded in prior experiences and anticipation of possible futures of devices uses to practical and concrete decision-making during set-up and configuration of devices. Crucially, interactions provide both access to knowledge and opportunity for a household community to jointly establish conversational familiarity with their products.

As we illustrate further in the next sections, interactions do not only contribute to familiarity with devices in the ways described here, but also become an essential part of the ways in which the use of devices is socially organised at home.

5.3.2 Roles

Roles describe who *normally* does what with which devices in the home. While roles are usually not formally defined or articulated, they are sometimes brought up to highlight expectations [302]. Adults coordinate their efforts with regard to device configuration, ongoing use, and maintenance. While coordination largely happens between adult household members, it also extends to neighbours and friends, and in that sense encompasses the wider community. Household members coordinate their actions across emerging divisions of labour following, in part, divisions of knowledge and experience.

5.3.2.1 Divisions of Labour

Divisions of labour frequently emerge as the set-up of devices is carried out by adults on behalf of the household. The set-up is not carried out communally: while some households divide tasks among themselves (across Households 1–4, the set-up of voice assistants was led by women while men focused on security, light systems, and thermostat systems), in other households the set-up of all systems is conducted by one person; in Household 6, for example, the voice assistant is configured only by the husband. These divisions of labour are planned for by our participants. For instance, in Household 4 Carla left the set-up of cameras to Aaron because she knew he enjoyed

using cameras. Rosa also relied on her husband, Jaco, to set up their smart security system as it requires fixing camera mounts outside the house for which he had to borrow the required tools from a friend.

The vignette below shows two parents, Adam and Monique, from Household 3 describe their experiences with setting up their smart doorbell.

Vignette 5.3 *Household 2—visit 5*

Monique: I still kind of haven't installed the doorbell. Literally on, like …

Researcher: Oh, haven't you?

Monique: …it, I'll show you.

Researcher: Yeah.

Monique: It will not. I've done the app, I've followed the instructions.

Adam: I think it's because my account's connected, I think we need to share an account.

Researcher: Yeah.

Monique: No, because it says that it's …

Adam: But I haven't been able to dedicate as much time to those devices, but I think it's also a testament that they're, in terms of at least set-up it's user-friendly …

As Monique struggles to complete the set-up on her smart phone by herself ('I still kind of haven't installed the doorbell'), it becomes the task of Adam who had set up the system using his smart phone in the first place to support Monique. However, Adam makes a statement about his lack of time available to dedicate to the devices, implying that with more time available he might have been able to do more to ensure Monique's set-up was successful. The vignette suggests that (1) divisions of labour are not always planned for but sometimes arise from the nature of devices themselves, and that (2) when it is not planned for additional coordinative efforts are required along with time and opportunity to ensure the technology works for everyone.

In Household 4, the mother, Carla, and her daughter, Ester, configure a Google Home Mini to recognise only Ester's voice to prevent Ester's brother, Malte, from using the device. While Aaron, the father, was not present during the set-up, he considers adding Spotify to the Google Home device to improve Ester's experience of it at a later point (Vignette 5.4).

Vignette 5.4 *Household 4—visit 5*

Ester: Yeah. Sometimes it says, "This can only be used on Spotify users."
Aaron: Have you got Spotify on there? Because Google does not respond to me. Ever since …
Carla: No, it does not respond to me.

Household members' ability to support each other in solving problems with devices can be limited by the nature of devices, particularly where a division of labour during the set-up is consequential for a division of labour in subsequent configurations ("Because Google does not respond to me"). In Household 4, the two parents fail to use family accounts for Google and Amazon on their devices, leading to a situation in which most of the services they pay for are linked to only Aaron's accounts (e.g., Spotify as becoming relevant in Vignette 5.4). Such a division is limited by the nature of devices or the features linked to accounts, requiring coordination between spouses to make devices work for their family (e.g., for their children).

5.3.2.2 Differences in Use

The two households mentioned above were relatively unfamiliar with smart home products at the start of our study. Households 5 and 6, however, have already owned several smart home products. In these households, an additional division of use emerges which, at least in part, could be attributed to an earlier division of labour in the set-up and configuration where devices have already been put in place by inhabitants with strong interests in exploring this kind of technology.

In Household 5, Cassie and Frank live with their children, Donald and Fabian. Vignette 5.5 takes place several months after Frank has configured the smart lighting system (including wall light switches) which was linked to the voice interfaces and already used by all family members.

Vignette 5.5 *Household 5—visit 2*

Cassie: But can I say, "Can you set that scene in the kitchen?"
Frank: Yes, it is configurable on a room-by-room, bulb-by-bulb setting.
Cassie: Okay, well, then we should do that, set one up for cooking and eating.
Frank: Yeah, I have but you have not found them and it is easy enough to change

them, right? [...]
Researcher: How do you usually find out about new things?
Cassie: When I see Frank doing it.

The vignette further illustrates the importance of "being conversational" (see Section 5.3.1) for successful coordination between adults. In this case, Cassie checks her understanding of the lighting system with Frank ('Can I say ...') before applying that information to propose a new configuration. One new insight that arises from Vignette 5.5 is the different kinds of coordination required and fuelled by different interests in technology[7]. Noteworthy in this context is Frank's remark that the settings he made are "easy enough to be changed", suggesting that he could resolve the situation should any disagreement arise between both of them. However, the first part of the same sentence also suggests a lack of communication and coordination between the two ("I have but you have not found them"). Participants' frequent remarks on 'finding time to deal with technology' also sheds light on the similar complexity faced by many of the other households in setting up, configuring, and maintaining devices. We can assume that configuring and maintaining devices become another thing to fit around the demands of everyday life. The challenges and complexities as well as different levels of interest also contribute to a lack of coordinate work in communication between household members.

The vignette also shows that a person's familiarity can be reinforced through the ongoing use of those devices and additional ones. In Cassie's response "we should do that" (Vignette 5.5), it is important to note that 'we should' is used rather than 'I can' or 'I should' or similar. The 'we' signals that Cassie alone is not the person who configures the devices, implying that it is a shared effort or someone else's task. Frank aligns with this position in his response ('yeah I have'), indicating that he has done the set-up while displaying his knowledge about the device compared to Cassie's. Later, in response to the researcher's question, Cassie orients to a clear division of labour and expertise between her and Frank: when Frank configures the device, Cassie learns about what new things it does. In this sense, the division of labour is also consequential for the

[7]In fact, Frank described his motivation for signing up the household to the study as related to differences in attitude and aptitude between himself and his wife.

experience of other users, particularly where adults assume configuration responsibilities on behalf of their household.

These insights are particularly interesting because their potential causes might predate the study. They show a slightly different outcome that might evolve over longer periods of time (more than six months) and without additional motivation through participation in a research study: single individuals assume the task of taking care of all smart home products on behalf of other household members. However, as we have suggested above and will further unpack below, this division of labour is not just contingent on individual interest and is not always planned for.

5.3.2.3 Fluidity of who does what

While there is a division of labour in the cases mentioned above, this division is not always clearly and consistently delineated. Instead, there is a fluidity of who does what where spouses change or exchange the tasks they typically do. For example, in Household 1 Jaco has set up the smart security cameras and taken on the task to regularly review their recordings. When his phone broke, Rosa took over this task of checking the video feed for incidents daily. As opposed to Household 2 and 4, Jaco has configured the corresponding application on Rosa's smart phone, not mentioning any particular challenge.

Vignette 5.6 *Household 1—visit 6*

Rosa: yeah so he did the set-up and then it transferred it to my phone. And that's when I change the name of the cameras because it was something with long numbers but if you see something like back of garden then you know exactly what you are looking into

Researcher: and are you getting all of the notifications too?

Rosa: yes, but I mute them during the day

Researcher: so you mute them but do you also look at the cameras at the recordings?

Rosa: sometimes, not, I guess, I guess I have other things in my head when I come home. It's interesting to see. I guess because I know he will do it. I will take a secondary role but perhaps If he didn't then I would build that into my day.

In the vignette above, we can see how Rosa makes the system 'work for herself' by setting camera names that signal the camera's location. Note that because she

knows that her husband regularly reviews the recordings, she does not take on that task. Instead, Rosa assumes a "secondary role", expecting her husband to look after the home security system. This role of looking after the security system is co-established and shared between the adults. Furthermore, efforts to coordinate tasks between adults also extend beyond the immediate household. Rosa and Jaco involve one of their friends next door to help recharge the cameras when Jaco goes on a business trip. This duty has previously been taken by Jaco.

Household 4's experiences with the same smart security system illustrate that the design of the technology itself affected the construction of roles. Such influence is not always welcome, and requires additional coordination between adults. The parents, Carla and Aaron, have set up the Arlo camera to not only guard their front door, but also to allow their son, Malte, to record short messages as he comes and goes independently. (Malte has only recently started to walk to school by himself and frequently wished to meet friends in a nearby park). Carla and Aaron are discussing issues regarding coordinating their efforts to make the systems work for the family. The precursor to the vignette below is Carla's attempt, after the front door camera was remounted following a recharge, to adjust the activity zone settings in the security system which determine areas for which notifications are sent out after.

Vignette 5.7 *Household 4—visit 7*

Carla: Aaron can do much more on his app than I can.

Aaron: Because mine's Android. And it seems to be easier somehow anyway to get hold of all the options and do things.

Researcher: Well, so what is it what you can do on Android?

Aaron: All the things like changing the video quality and all that …

Researcher: That makes sense (? 16:43).

Aaron: … and (inaudible 16:46) one way of doing that on the iOS but I can't find out how to.

Carla: Yeah, we couldn't find, we sat with our like apps side-by-side and they're just really different.

Researcher: Okay, okay, so yeah, well, I guess they have quite a different access then?

Carla: Yeah, Aaron has to do all the admin.

Aaron: Again it's me ruling all of the apps, isn't it?

Carla: I know. Yeah, it's weird and …

Aaron: I dominate Alexa, yeah.

> Carla: … it doesn't seem to be that Aaron's got an admin access and I don't, it's just that the apps are different.
>
> Aaron: Yeah, it's not always deliberate, with Alexa Show it was, with Alexa Show I did say you have to link it to my account and I'm, you know, but with this that was just accidental. With the lights I think you've got a bit more …
>
> Carla: Oh, yeah, so …
>
> Aaron: …yours seems to work better than mine.
>
> Carla: …yeah, yeah, that's true. The Hue app I think is a bit easier on iOS than Android. So I do all the lights.

Coordinating their efforts to make the system work for both of them ("we sat with our apps side-by-side"), the two adults work out functional differences between their applications. The different levels of access to features such as "changing the video quality" result in Aaron "having to do all the admin". While this division of labour is welcome in other households, Aaron remarks that he "ruled all the apps" before the two go on to explain how their access across different devices is rarely equal. Both display an awareness of the kind of control which results from using either person's account to access any of the devices, as evidenced in Aaron's mention of Alexa Echo Show which was initially configured by Carla and linked to her account ('with Alexa Show I did say you have to link it to my account'). The parents in Household 4 wish to share access to devices following their idea of a spousal relationship in which either of them has the ability to manage everything on any of the devices, technology design permitting. Sometimes they deliberately refrain from this approach, and diverge in other times.

Summary Adults coordinate their interactions to make the technology work for their home. Roles in the home are co-established between adults. When they are called into account, they highlight an expectation of the person assuming the role and doing the work ascribed to it. This is in line with Hilbert who defines roles as "something actors occasionally require to achieve mundane, non theoretical ends" [302, p. 218]). However, devices sometimes fail to accommodate for the fluid nature of who does what in the home. Roles are not always assumed by single individuals. Rather, it is the individuals who move in and out of roles. Roles are sometimes shared between adults; at other times tasks that serve the fulfilment of a role can be delegated. When the nature of devices (features

they offer/lack) is consequential for a division of labour (who can do what with devices), the division of labour is considered problematic and requires additional coordination.

5.3.3 Moral Order

In this section, we show how households' interactions inside and outside the home reflect and contribute to a moral order—"shared goals, values, norms, and beliefs, about words, deeds, and actions considered 'normal,' 'right,' and those considered 'wrong'" [161, p. 5052]. We do so by arguing that expectations with regard to appropriate use are not only held by members of the household community but also extend beyond the immediate household. We further show that these expectations are implicated in everyday interactions and communication between community members, and that they are usually not articulated among household members but surface when expectations are not met.

5.3.3.1 Inside the home

As we will *also* show in Section 5.3.4.1, notions of appropriateness can be seen in interactions between household members both with spouses and with children. This appropriateness shows that household members reflect on the use of devices, and particularly on the ability to make appropriate use of devices when the design of devices is perceived as limiting.

Preceding Aaron's explanations in Vignette 5.7 are insights he gained first-hand from online media and experiences with smart devices. Having previously learned about a "protective dad" who has placed cameras in every child's bedroom, he finds it challenging to adopt this kind of behaviour and perspective. In the following vignette, he positions himself as 'not this kind of father figure'.

Vignette 5.8 *Household 4—visit 5, edited for clarity*

Researcher: Yeah because you mentioned it is mostly your accounts, so you are in control of these things.

Aaron: Yeah, that is an interesting (inaudible 36:24) because I can monitor everything that is quite interesting. It is meant to connect(?) devices, but it can close off even more. You have to have a family (inaudible 36:43) in every room, for instance. Dad is watching all the time. And so that is, over time, it is potentially quite difficult.

Aaron elaborates on potential issues and dangers of him, or other father figures, having too much control over devices ("Dad is watching all the time"). In his view, these devices cannot contribute to the kind of family life Carla and himself prefer ("close off even more"). The potential usage of these devices does not align with the kind of concerns of parenting he would like to attend to. He wishes that his children grow up in an environment without being overly controlled by him or anything.

While Aaron's reasoning in the vignette above is reflective of his first-hand experiences, expectations of normalcy become visible during continued use when others' actions are called to account (background expectancies [255]), and this demanding account reveals what appears to be the home's moral order. In Vignette 5.6, Rosa assumes a "secondary role" as she only reviews recordings when she knows that Jaco would not be able to. Note that Rosa is not excluded from reviewing the recordings. However, as the vignette below illustrates, *how* the task (reviewing the recordings) is accomplished has not been discussed or mutually agreed on but was somehow left to Jaco.

Vignette 5.9 *Household 1—visit 7*

Rosa: The last two weeks we, after the kids went to sleep he wasn't sleeping, I could hear his phone buzzing (makes noise). Then I couldn't sleep. And then I said, "Do you have second wife or what? Your phone is buzzing all the time." And he said, "It's Arlo," I said, "Oh, okay."

To Rosa, Jaco's behaviours (being on the phone before bedtime) do not present itself as 'normal', but she readily accepts the explanation Jaco offers. Jaco's response ("It's Arlo") indicates that he is fulfilling his role, a role that Rosa knows he has taken on and which is important in their shared and established goal of protecting the home (the family has wanted to reduce vandalism on their property and contributed to the neighbourhood watch).

The two household members establish the relative needs and purposes of reviewing the camera feed in light of existing goals and values, i.e., looking at the phone in this situation (before bedtime) is unusual but permissible given their shared goal of protecting the home. Another example of household members orienting to the home's moral order in making a device work for all household members is presented in the vignette below. Aaron in Household 4 explains how he has moved the Alexa Show 5 to the bathroom.

Diary 5.1 *Aaron, Household 4—after visit 4*

We set up the Alexa show in the bathroom. The kids can enjoy music and videos while washing. I covered up the camera just to make sure people can't spy on us, esp the kids

While his emphasis here is on their children enjoying the music and videos, during the interviews it becomes clear that the parents, particularly himself, also enjoy having access to entertainment in the bathroom. Note that the camera covering is motivated out of concern for his children as he reconfirms in the vignette below.

Vignette 5.10 *Household 4—visit 6*

Aaron: But for us I think that is, to me it is mainly just as long as the kids are not being filmed in a private way, there is not much else about my own privacy setting I actually care that much about. It becomes more of an abstract idea, that privacy rather than something I particularly want to keep, secrets.

These excerpts provide insights into his reasoning which is to protect the children from being spied on and that privacy is an abstract idea that is not relevant in practice. His goal has been to protect the children from "being filmed in a private way" in the bathroom. In his consideration, this is not entirely in line with his overall parenting values, which involve protecting the children from such outside influences.

Over time, these interactions with their encapsulated goals, values, and sense of normalcy (as visible or discussed with other household members) become part of a moral order. While household members could derive a sense of normalcy by observing others' interactions, the opportunity of non-household members to partake in this local process is naturally limited. Consequently, a sense of appropriateness of action is difficult to uphold when others come in contact. Just because one household has had experience with smart devices does not necessarily mean that other households should, too. The resulting local organisation of use is not appreciated by people outside the home in similar ways.

Some of our data suggest that when people are not able to appropriately orient their actions to the moral order (due to lack of familiarity with that order), they refrain from interacting with devices where possible. For example, the student lodgers in Household 1 generally do not interact with any of the devices (Rosa: "She will not

use something that is not hers"). The notable exception is a returning student lodger who has stayed with the family repeatedly during the last seven years (Jaco: "We are like his family."). He happily interacts with the devices and even plays pranks on the other household members by muting the microphone.

The difficulty of establishing what constitutes appropriate behaviours (orientation to moral order) for occasional interactions is also visible in participants' diary entries. In the diary entry below, Sylvie expresses her discomfort with interactions mediated by doorbells cameras and doorway intercommunication systems.

Diary 5.2 *Sylvie, Household 6—week 9*

Over Christmas I used my phone to answer the door bell while I was out using my 'Ring' app. It was very convenient to be able to accept a delivery despite not being at home. I didn't like the awkwardness of the situation- the delivery man wasn't expecting to speak through a device and I felt it was interrupting the meeting I was in.

Sylvie finds herself in a 'situation' that is signified by a lack of normalcy. Communicating with a delivery person who also seems unfamiliar with the smart doorbell feels awkward to her. As this diary entry suggests, several challenges are involved in dealing with people outside the home.

5.3.3.2 Outside the home

One particular challenge is the need to manage neighbours' expectations with regard to devices in relationship-appropriate ways. The parents in Household 1 find it necessary to inform their neighbours about their new smart security system which also overlooks parts of the neighbours' property. It is worth noting that the community here includes their direct neighbours on both sides, a 'lady' and a young family they are friends with. Household 1 is also part of a neighbourhood watch.

Vignette 5.11.1 *Household 1 – visit 6*

Jaco: it's our neighbours are happy as well, [...]
Researcher: so you mentioned the cameras to them
Jaco: yes of course
Researcher: what did they say?
Jaco: they say it was brilliant where did you get from and how

Rosa: yeah we had to do it from a privacy point of view. Because they need to be aware of them being filmed

Researcher: so you just let them know

Jaco: no they were happy

Rosa: yes they were happy because if something happens to the front of their house then you have the video

Jaco mentions that he has been talking to the neighbours about the cameras ("our neighbours are happy as well"). Rosa supports him by emphasising they "had to do it from a privacy point of view" since they are also being recorded by the cameras. She further highlights the way the cameras are positioned can help protect the neighbours' properties and therefore is beneficial for them ("if something happens [...] then you have the video").

The vignette illustrates two things: (1) it shows how Rosa and Jaco have coordinated their efforts to make the newly installed cameras accountable to their neighbours since both consider this behaviour as appropriate for neighbours (reflecting the moral order); (2) it shows a division of labour between the two adults (Jaco taking care of the more practical issues related to the system while Rosa helping with managing the work required to make the system work well in the community). Rosa uses phrases like 'had to' and 'need to be aware', signalling that she is oriented to mundane concerns of being a good neighbour and fully aware of what needs to be done in restoring accountability with their neighbours. The two adults share and contribute to the task in different ways.

The second part of the vignette shows how the neighbours started taking interest in Jaco's and Rosa's use of the security cameras by seeking confirmation of the ways in which the system is used. In demanding accounts from Jaco, they are able to gain a better understanding of what normally is to happen with the system and its recordings.

Vignette 5.11.2 *Household 1 – visit 6*

Jaco: they keep asking 'did you see anything happening in the house' and I said 'I check everyday don't worry. If something is happening to your house, someone will knock your door or so' then it's recorded'.

Researcher: okay

Jaco: so I'll tell them. They are asking and then I think the wife asked me once and the husband asked my twice.. and they said it's good because when you go on holiday then you don't have to worry about. It's good it's fine. I check everyday when I come from work

The neighbour family has asked Jaco whether he will 'see anything happening' around their house. What Jaco offers is a description of the ways in which he uses the system. He has told the neighbour that he regularly reviews the camera feed ('I check every day when I come from work'), and that he will keep them informed should something happen ('someone [would] knock [on their] door').

The interactions provide a sense of normalcy for the neighbours. Their acceptance of the accounts also indicates Jaco's perceived competence of orienting to the purposes he has described (to moral order). Part of this moral order has become how the system is used by Jaco, for what purpose, and what the conditions for engagement are ("I'll tell them [if something should happen]").

However, coordination with people outside the home similar to Household 1 (Jaco and Rosa) is not always possible, particularly where situations are unanticipated (see also Diary Entry 5.2). In fact, without the ability to communicate and gauge others' interest, household members have no means to manage familiarity and normalcy when coming into contact with other people. However, this may result in situations in which the 'moral order reasserts itself', as evidenced by participants' reflections:

Vignette 5.12 *Household 2—visit 6*

Adam: And a neighbour over a way there had, she said, "Oh, I kept ringing your doorbell." Because she did not leave the message function, because you can leave a voice message to say who you were, when you called. Because she said, "Oh, I did not know how it worked." And so that is something that I kind of, it suddenly struck me that beyond our sales, obviously the people … because I will not ring my doorbell that often. Because I have keys. But for the people who have not used these devices before, it might be quite intimidating or just the fear of the unknown. It is something I did not kind of figure, I just thought people would press it and be happy to leave a message or … Because there is no visual instruction, so …

Researcher: So what happens if you press it?

Adam: So it rings and we will get a message, but it says, "If you would like to leave a voice message,"

Researcher: What, it speaks to you, does it?

Adam: Yes.

Researcher: Okay.

Adam: And I think people get a bit freaked out. So then I did not kind of anticipate, I suppose, I did not even think about it.

Adam acknowledges that while his families are familiar with the technology, his neighbours cannot be expected to possess the same sense of familiarity ("I did not kind of anticipate"). In light of everyday concerns of maintaining good neighbourly relations (e.g., the neighbour wanted to leave a parcel), he has identified a lack of instruction, either designed into the device or provided by himself. Later, he goes on to reason that while the postman might be familiar with this novel technology, this could not be expected of the general population.

The use of these devices, hence, is closely linked with relationship considerations outside the home where the management of relationships is possible through communication. In other cases, participants consider how expectations could proactively be dealt with by considering effects of these devices on people outside the home. For example, Frank in Household 5 has anticipated that pointing a camera at their neighbour's property is not advisable. They have not maintained a neighbourly relationship that would accommodate for the kind of relationship management Household 1 is able to.

Vignette 5.13 *Household 5 – visit 3, edited for clarity*

Frank: …and therefore it is very much facing perpendicular to the house, which here would mean we are looking at, you know, the road and the neighbours across the street which is probably not quite what we want, and we certainly do not want them to feel there is a camera pointing at them you know. So we would have to think about where we …I suppose we could, yes, just have to have a think about where we put it. …

What is remarkable in the vignette above is that this assessment is articulated by Frank (using 'we') but shared by Cassie (her supporting 'Yes'). It becomes clear that Frank speaks on behalf of them both. The couple demonstrates familiarity with the moral order outside the home. While this moral order would also be reflexive of their interactions with the neighbours, it is also reflective of the societal context of this study. While surveillance is ubiquitous in UK public life, expectations of an undisturbed private sphere are equally strong. For example, Monique of Household 3 is confronted by a neighbour who suggests they ought to check whether a CCTV license is needed.

Summary Household members orient towards the moral order inside the home in varying capabilities, facilitated by the shared nature of resources and space in the home itself. A sense of normalcy is negotiated through household members interactions (e.g., when using devices but also articulated in managing expectations). Inside the home, household members actions, then, represent the moral order. There is an understanding between adults in the home how things ought to be, and at times this understanding can be extended to others outside the home. This is achieved by presenting the household's moral order to people outside the home.

Where there is no relationship with others outside the home or the relevance of a relationship is not apparent to household members, expectations can be left unmet. Household members can devise other strategies to share their experiences and support with others in gaining familiarity with devices, or they can refrain from doing so by containing the use of smart devices to their homely perimeters. Notably, household members' efforts towards the wider community are driven by a sense of 'we versus them,' which can lead to a sense of shared tasks and responsibilities (a shared role of being a good neighbour). Interactions with the wider community typically are occasional and thereby do not lend themselves to establishment of normalcy in the same ways interactions between household members do.

5.3.4 Rules

Rules do not exist to prescribe behaviours through role expectations because "morality is not simply a phenomenon attached to society that makes it run smoothly" [303]. Instead, rules are employed by actors to achieve mundane ends [302]. They are not devices to create order but "devices invoked to *account* for order" [188]. In this section, we illustrate how the local moral order can shape the management of interpersonal relationships in the home and with the 'outside world'. We also show how this management can become more visible through *rules*.

5.3.4.1 For Children

Household members articulate rules to help each other interact 'appropriately' with respect to established goals and values or the moral order of the home. This is particularly visible among parents introducing rules to help their children.

Parents articulate parenting concerns, a role typically shared between two adults. For example, in Household 1, Rosa and Jaco have established that her daughter is not going to get access to the smart security camera feed despite her interest in watching her friends walking by and making funny faces to the camera.

Vignette 5.14 *Household 1 – visit 8, edited*

Iria: No, they have not given me it yet.

Rosa: Daddy knows ((inaudible 11:23)?

Jaco: I also was busy with it. But I would leave it. But it is for …I do not want to give it to her, I want to keep it for me,(inaudible 11:32). […]

Iria: Yeah, but you said you would.

Rosa: You might delete videos.

Jaco: Yeah, that is why I would worry about it.

Jaco: That is the kind of like when she is, like, she is not here we are talking to you, like, we talk to you but …

Iria: But what is there to talk about?

Jaco: Because when she is, one of her, if all three of ask, one of us delete the video, that is how we …

Iria: No, they are just worried because everyone in our year, in my year literally knows where we live. And all the boys love to cycle past our house. And they will always knock and come and say, "Hello," to me, so they are just worried. I think it …

Jaco: Well, as a father I'm always worried but it is even though you are a boy or you are a girl or it does not matter, they still are children.

The rule the parents have discussed beforehand ("daddy knows") establishes that Iria will not be given access because she "might delete videos". However, Iria reveals what this rule might actually be about, that her parents are worried "because everyone in [her] year [...] knows where [the family] lives". Jaco confirms this motivation ("as a father I'm always worried").

The rule of 'not giving Iria access' then serves to further the parenting goals, part of which is to assist the daughter with being able to independently manage personal relationships. By similar token, she is also considered not sufficiently competent to

contribute to the management of hers and others' relationships in the digital world. The parents consider the smart security system to be an essential part of their parenting role, which is not reconcilable with the daughter's interest in using the system. In this way, the rule of not giving access to the system shows the moral order of the home.

Jaco and Rosa in Household 1 also manage their children's access to the Echo Show 5 in the kitchen. At the beginning of one of our visits and before her two boys made their way into the kitchen, Rosa asked the researcher not to mention any keywords that can be used in interactions with the Echo Show 5 since the two boys had repeatedly played the same YouTube channel[8]. Clearly, the children are not expected to understand what constitutes appropriate use of the system. In the present study, their use is at times guided by rules and at other times regulated by limiting access.

Other rules have been established to manage the exposure of children to the digital world. In Household 2, wanting to protect their son from the world of brands and targeted advertising, Monique and Adam introduce their son to the Google Home with the keyword "Doogle" instead of "Google". Established between the adults for the benefit of their son, this rule for use shows the household's moral order, i.e., that they would like their son to grow up unaffected by targeted advertising and other influences from the online world (Adam, visit 2).

These mundane concerns related to the role of parenting. Parents' efforts are oriented to the local moral order of the household. Another example of rule invocation that reveals the moral order in relation to parenting is provided in the next vignette. Mother Carrie and daughter Felicity in Household 3 jointly set up the Google Home device. They attempt to connect the Google Home app to their Google Home Hub Max, and subsequently want to set up music streaming. Prior to this excerpt, they have provided a nearby street when prompted for an address of their new device. The device is now asking for location permissions to be able to connect to other devices.

Vignette 5.15 *Household 3 – visit 4*

Carrie: Okay. So, if I allow it, will it just do it now and then not later?
Felicity: I guess so.
Carrie: Because I do not really want somebody following me around where I am

[8]Note that we had not told them about any possible uses before.

going all the time. Okay.
Felicity: 'Settings', 'location'. What do we do?
Carrie: So, I need to see how to get back to this thing with the settings to change the privacy. I need the internet for that. Oh, I guess I can do it without, can not I?
Felicity: Yeah. See if you can get the music on.
Carrie: Yeah. Let me do the privacy thing first.
Felicity: The privacy is more important.
[...]
Felicity: Features and services?
Carrie: It was more services, I think, if you had to choose.
Felicity: Yeah. I thought I saw it. Go down. Music.
Carrie: No. We are doing privacy at the moment, Felicity.
Felicity: Oh. I thought you were talking about the music. Sorry.

As Felicity and Carrie continue configuring the device, Carrie signals that she wants 'to do the privacy thing first' to which Felicity readily agrees before establishing the rule that "the privacy thing is more important". However, when her mother's search for the location setting takes Felicity back to the configuration page of the music streaming services, she wants to 'go down' to look into the music configuration. This prompts Carrie ('no') to re-establish that they "are doing privacy at the moment". In establishing and following through on this rule, Carrie displays an awareness of the local moral order (i.e., that "the privacy thing" is more important than entertainment). Rules are invoked by parents to establish moral order in the set-up and configuration of devices, providing meaning to their actions which might not be noticed by their children otherwise. In the vignettes above and other examples, we see that this encompasses the management of relationships not only between household members but also with the online world (see also [145]).

Rules, however, do not always suffice in helping children learn about the moral order and orient their actions. Sometimes rules are implemented to actually restrict access, as implicated in the parents' reactions to Felicity's interest in setting up entertainment (Vignette 5.15) and Iria's plans to watch security camera recordings for fun (precursor to Vignette 5.14). Parents also limit their children's ability to use a device. For example, in Household 4, Malte struggles to manage his screen time:

Diary 5.3 *Aaron, Household 4—week 12*

We need to find a better location for the Echo Show so that Malte doesn't use it to play games on and watch videos all the time as he can't regulate his screen time and finds it very hard to get off any screen.

While rules are articulated to teach the moral order to children, at time they have to be complemented by restrictions to be effective.

5.3.4.2 Between Adults

Rules between adults are rarely as clearly articulated, but they exist nonetheless. As Garfinkel shows us, the orderliness of everyday life is mostly unremarkable but becomes visible to us when it is breached, when background expectancies surface [255]. In Household 6, Tobias and Sylvie are exploring which devices to acquire as part of the study. While discussing smart security cameras, they recall a past incident in which Tobias has set up the webcam to watch their kitten in the kitchen while at work. In this extract, Tobias' subsequent action of providing the web link to his mother so that she could also watch the kitten is described by Sylvie as inappropriate. Sylvie 'did not like' this and explicitly finds fault with Tobias.

Vignette 5.16 *Household 6 – visit 2*

Researcher: How about cameras outside or inside?

Tobias: You will not find cameras inside?

Sylvie: Oh, yes, that is because you used it inappropriately, though. Tobias rigged up a camera so that we could observe what the kitten was doing when we were not in, and we could access it using a web link, and Tobias gave the link to his mum. So his mum could then observe the cat plus us, whatever we were doing in the kitchen, and I did not like that but that was your fault.

Tobias: Yeah, I shared the link.

Sylvie: Yeah, but it was nice to be able to see the kitten.

Researcher: And then the camera went away?

Sylvie: Yeah, and then the kitten started going outside and it was redundant.

Tobias relates to the past incident by implying a rule of 'no cameras insight' ("you will not find cameras inside?"). Sylvie recounts the past incident where her mother in law has gained access without her knowledge. The vignette shows how the moral

order is established in shared experiences (past mistake of sharing) and articulated in rules. These rules are then applied to new situations.

Outside the home, household members in our study have not established clear rules but provided information and insight as discussed in the previous section (Section 5.3.3.2). This sharing allows other community members to position themselves and their own needs against the circumstances of device use (e.g., the shared purpose of using a device to catch burglars and protect the neighbourhood).

However, community members could allude to or highlight the applicability of 'rules' (as in laws and regulations) to challenge these circumstances as documented in the vignette below. In Household 2, Monique narrates a situation where she found herself confronted by a neighbour, and her husband Adam comments on the issue.

Vignette 5.17 *Household 2 – visit 7*

Monique: So I was just with Eric and the neighbours were just going and he was saying, "Oh, it is interesting …" because I was telling him about how it is good for security as well as answering if you are not here …

Monique: …say, "Hi, just leave it round the corner, I am going to be here in two minutes." And he said that we need to have a licence because he said, "You should check that it is not classed as CCTV …"

Adam: Okay.

Monique: "…and if it is then you need to have some kind of licence."And also, if you remember when we were burgled…

[…]

Adam: I do not think it needs a licence.

Monique: I do not know either, he said just …

Adam: No.

Monique: …to check, I do not …

Monique speaks positively about the security benefits of the camera. The neighbour does not appear to fully agree, offering her instead the (unsolicited) advice to check for CCTV license requirements. The neighbour suggests a rule (here a law) might regulate which use of home security cameras is appropriate and permissible. Here, rules are invoked by adults to highlight expectations of appropriateness that reflect the moral order.

Summary Our findings show how rules are used to highlight the meaning of interactions in relation to moral order, e.g., to limit children's use of devices or establish appropriate use between adults. The meaning of interactions is in turn challenged by articulating rules. Parents use rules to support their children in managing their relationships in the physical and digital world. Note that these rules are essentially articulated not only to manage access to devices but also to attend to "*higher-level* matters" [188] related to concerns of parenting such as protecting children from the online world, or helping them to regulate their screen time. This kind of moral and social order is pre-established between adults in the home and finds its application in the articulation of rules pertaining the use of smart devices.

To highlight the importance of the moral order, adults likewise use rules which are linked to households' past experiences or to societal agreements such as laws and regulations. However, it is equally important to acknowledge that rules are not established in prescriptive or generative ways. As adult members of the household are able to—and are expected to—orient their actions appropriately, restrictive use of rules between adults (as opposed to children) is often not evident.

5.4 The Organisation of Communal Use

This section draws on our findings to construct a framework representing 'the organisation of communal use'.

5.4.1 Overview

By summarising our efforts in documenting interactions, roles, rules, and their relationship with the moral order, we draw connections between these concepts in Figure 5.7. In the sense of expectations, roles *provide for* interactions while interactions *manifest in* roles. Interactions *inform* rules in at least two ways: they might make the articulation of a rule necessary (parents for their children), and/or rules can be proposed by adults to call moral order into account. In turn, rules *provide meaning to* actions such that community members are enabled to act competently. Rules *articulate expectations for* roles but do not define them in these expectations. Rules are not just role expectations but also

account for moral order. Assuming and acting as part of a role requires *considering the meaning* of rules and how this meaning encapsulates social goals and moral order. Social values and goals are reflected in the moral order of the home. An important concern among household members is to maintain and nurture relationships across digital and physical worlds by managing the 'attack surface' with the digital world [145].

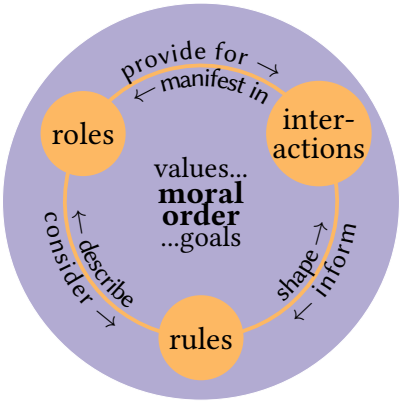


Figure 5.7: The Social Organisation of Communal Use

5.4.2 Roles and Competent Behaviour

Roles are not constructed by articulating expectations as is the common understanding in the functionist role theory (actors conform to expectations to gain approval). Neither are they prescriptive in an interactionist sense (role-taking to see the world with other's eyes) [302, 304]. In their discussion of a receptionist's role in a social work agency, Zimmerman [305] argue that no set of constructed role expectations (job profiles) can sufficiently cover members' behaviour which encompasses a large array of contingencies. As Hilbert [302] emphasises, individuals always place their own interpretations on the enactment of role expectations (rules), such that they work around limitations while upholding the intended meaning of a role [302] (see also Jaco's reviewing the recordings at night in Vignette 5.9).

Competent 'role' behaviour manifests in interactions where their meaning in relation to social goals becomes visible, i.e., the reflexive orientation of actions to the moral order, the social goals, or the purposes to which members ascribe. In Vignette 5.16, Tobias fails to meet Sylvie's expectations of the social goal implicated in the original

intended use of a cat camera, i.e., to look after their pet. Sylvie's expectation is unmet when Tobias orients the social goal of nurturing the relationship with his mother instead. Part of being competent is also the ability to balance personal goals with those of the community. In Vignette 5.14, Iria is not given access to the security camera feed as she might delete videos which her parents preferred to keep in order to look out for her. Finally, where social goals are not coordinately established with the community, community members might orient to 'normative notions' of what they consider right and wrong within the wider community. For example, Frank demonstrates this competence in considering the effects of security camera usage on their neighbourhood (Vignette 5.13).

5.4.3 Rules and Moral Order

Our insights on rules and moral order expand on existing literature. The differences in rules application and invocation observed between adults and children corroborate with Crabtree et al.'s [188] findings on home network policy use. The authors highlight that any articulation of rules makes explicit what is "deemed to be permissible" which itself may *only* be welcome in the management of specific activities and behaviours. Our insights on the use of smart security cameras and smart voice assistants support the notion that a clear articulation of rules is used to attend to 'higher level' parenting concerns (e.g., turning rules into parenting devices) [188]. The hesitation we observed with regard to articulating rules outside the home is also reflected in Crabtree et al.'s [188] findings on the use of domestic network policy. The conversation Household 1 had with their neighbours (Vignette 5.11.1) supports Crabtree et al.'s [188] suggestion that creating awareness of "activities that are relevant to rule use" (letting the neighbours know what is happening in their environment) provides opportunity for appropriate action and can be an appropriate substitute where the articulation of rules is not permissible [188]. However, we also highlight that the means by which household members could let members of the community 'know what is happening' are poorly supported by the current design of devices. Crabtree et al. [188] suggests making the home network

accountable to users, which remains an active research area (e.g., [46, 205]). These efforts need to take into consideration the social organisation of communal use.

Roles and rules in the home are oriented to and employed in similar but different ways. When roles are articulated, expectations with regard to their fulfilment become visible. What is done by a person assuming a particular role needs to be oriented towards the everyday concerns and social goals ascribed to the role. However, these are neither defined a priori nor fully articulated. Rather, rules are articulated to account for the moral order, for an orientation towards the same social goal. In this sense, intended meaning (social goals) and expectations are bound up in roles and rules, but 'using' (e.g. articulating) roles and rules are not sufficient to cultivate the competence of orienting towards an underlying social goal in others (e.g., children). Furthermore, particularly limiting conceptualisations of roles and rules in implementation can undermine efforts to build and exercise competences (e.g., Aaron "dominating Alexa" in Vignette 5.7).

5.4.4 Social Goals and Privacy

The findings document how participants' perspectives on privacy are bound up with other situational considerations, among which privacy is rarely an explicit reference. As Aaron (Household 4) puts it:

> it becomes more of an abstract idea, that privacy rather than something I particularly want to keep, secrets. (Vignette 5.10)

When explicitly mentioned, the somewhat abstract concept of privacy requires further practical consideration and explanation:

> we had to [inform the neighbours] from a privacy point of view. Because they need to be aware of them being filmed. (Vignette 5.11.1)

The word itself is used to express aspects of a locally agreeable moral order, as this vignette of household 3 illustrates:

> Carrie: Because I do not really want somebody following me around where I am going all the time. Okay.
> Felicity: 'Settings', 'location'. What do we do? [...]
> Carrie: Yeah. Let me do the privacy thing first.
> Felicity: The privacy is more important. (Vignette 5.15)

In this sense, the word privacy becomes a vehicle to explicate a part of the local moral order which in turn manifests in the practical actions reported above. These practical actions (e.g., talking to the neighbour about the cameras) reflect everyday concerns. Privacy becomes wrapped up in these concerns but is rarely made explicit.

These insights presuppose our EM informed methodological orientation. Of course, the aforementioned quotes can be interpreted as 'privacy as secrecy' or 'control over information'. Further vignettes in this chapter can be interpreted as occurrences of privacy conceptualisations such as the 'right to be let alone' or 'control over information' (Diary Entry 5.1, Vignette 5.13, or Vignette 5.16) or 'limited access to the self' (Vignette 5.15). Similarly, one could draw on privacy theories. For example, Vignette 5.15 can be discussed as 'privacy as boundary work' and Diary Entry 5.1 illustrates 'privacy as contextual integrity'. These references reflect the multifaceted nature of a phenomenon that others have called a 'concept in disarray' [49] and researching it may invoke many different interpretations of the word [20]. Methodologically, these interpretations lead us astray from our goal to document how privacy manifests on the ground and to provide insights into observable and reportable practical action to inform design[9]. Such interpretations may encourage us to label and gloss over a social phenomenon that is not often explicitly accounted for and hardly relatable or actionable.

Staying close to relatable and actionable considerations, we need to explore the everyday, social considerations that are reflected in household members' practical work. When the term privacy is used, it is appropriate in the context of everyday concerns related to parenting (Diary Entry 5.1), being a good neighbour (Vignette 5.11.1), or not being followed around by someone (Vignette 5.15). We have also reported several other occasions in which privacy is not articulated as concern but could be analytically categorised as privacy behaviours, e.g., not pointing security cameras at neighbours (Vignette 5.13), calling a device 'Doogle' to protect children from effects of brands (Household 2), or not tolerating cameras inside the home (Vignette 5.16). Taking the perspective of our participants, it becomes clear that they are not concerned with analytic or theoretical matters of privacy as much as with everyday concerns.

[9] See also, the discussion of EM informed approaches and design in Section 3.2.2.2.

Prior research has documented household members' concerns with everyday matters rather than the concept of privacy in other contexts [20, 22, 145, 205]. Our findings in the context of off-the-shelf products for the smart home corroborate with these insights. In attending to social goals, values, past experiences, a sense of normalcy, and societal norms, household members are rather concerned with the mundane matters described in the previous paragraph. They orient their actions to the moral order. Crabtree, Tolmie, and Knight [145] find that people are rather concerned with managing the "attack surface" of the digital world on the social when they made use of passwords for their personal computers or shared content on the online social networks. This preoccupation with 'managing relationships' [145]—one's own relationships and those of others—is also evident in our households.

Household members employ a range of practical methods to "manage risks of particular cohorts"; and because of the qualities of smart home devices in our study these can be seen as another variant of methods reported in [145]. What we have observed is a range of methods that are partly established in the literature (e.g., camera covering) and others that emerge in reaction to relatively new interfaces (e.g., parents encouraging their child to call their Google Home devices "Doogle" instead of "Google"). As we have pointed out, rules are frequently invoked by adults to articulate and account for the moral order to others (e.g., their children).

Our findings suggest a difference between household members' orientation inside the home and outside the home. Inside the home, the guidance provided by roles and rules is available to individuals in the ways described above but does not translate to relationship management outside the household. Participating families jointly contribute to efforts of relationship management, e.g., in their considerations of creating awareness among their neighbours (signified in the use of 'we' Vignette 5.5). This perspective can surface based on the assumption that household members become conversational with regard to their smart products.

We have described the work of our household members in terms of managing relationships as well as expectations. Expectations can be best described as anticipation of a sense of normalcy given a situation. Where household members anticipate that

expectations might be unmet, they are concerned with managing them proactively. Hence, expectations are essentially about managing accountability of devices and interactions across the fluidity of who typically does what and to what end. Currently neither perspective is well supported by design, and we suggest both be taken into consideration.

5.5 Discussion

Our framework provides concepts and details for privacy research and product development concerned with communal use. This section draws on existing research to highlight opportunities for empowering households' privacy. Here, we understand empowerment as enabling household members to "gain mastery over issues of concern to them" [32] in the sense of enabling 'equality of opportunity to access resources' [31] (see also Section 1.2 Research Politics).

5.5.1 Dynamic Nature of Roles

Where devices limit the ways in which communal use can evolve, they are perceived as problematic. Roles are abstract but not in a generative sense [239, 272], and rules are prescriptive but not definitive for roles [303]. If design is suggestive of generative and restrictive ways of technology use, the resulting models are unlikely to be adopted. One such example is the access control models proposed in [213] but largely unused. Designers can draw on the framework presented above to take into account the dynamic and evolving nature of communal use.

Generally, access control models should not be built in ways that restrict future changes. For example, they should not be strictly limited to a single administration account. They also should not be restrictive in ways that curtail interactions contributing to the shared roles (e.g., maintenance of a system). While actions around the use of smart technology in the home might be "differentially organised" [16], technology features should not restrict role actions but facilitate role establishment.

Everyday concerns and practical work documented in this chapter—particularly when shared by household members—offer an alternative orientation for design efforts. A possible first step is to enable 'moving in and out of roles'. We are not proposing to

simply assign the same role to more users. Rather, we are suggesting that roles (and inherently permissions) be oriented to social purposes or goals. The next two chapters further elaborate and demonstrate this point.

5.5.2 Designing for Coordinate Work

There is a need to design for coordinate work ('articulation work' [306]) in order to support privacy in communal use (via [307])—i.e., the various concerns with relationships and the management of expectations that guide practical action. In addition to designing for the management of relationships with and mediated by the online world [145], we suggest designing for coordinate work that contributes to the negotiation of social goals. Social negotiation and coordination between users contribute to the accountability of devices with all household members, answering questions such as what a devices is designed to do, how it could be used, and how it is used by the community [205]. We suggest this perspective can contribute to the rethinking of the approach to informational privacy and novel design patterns [308].

Our suggestion is to allow for members' interactions with a device, particularly when exercising privilege, to become socially accountable through technical mechanisms such as creating awareness of activities that contribute to role use (i.e., showing what is happening in an environment). This accountability is essential for other members to gauge whether interactions are naturally accountable to the moral order (i.e., if they are part of an activity coordinated between household members) and what purpose the activity serves. For example, windows stickers which disclose the operation of CCTV not only potentially deter burglars but also create awareness among community members. To integrate this kind of visibility into products, researchers have developed concepts and methods, among which is the concept of social translucence [280, 309]. The concept and a related framework are centred around the idea of translucence in interactions with the system—i.e., helping users to coordinate their use of the system by creating accountability with limited visibility. Our findings suggest that—for 'healthy' relationships at least—such insights might be conducive to reducing privacy issues and coordinating related management efforts.

5.5.3 Enabling Users

Following the observation that the set-up and configuration of devices are mostly performed by single individuals (digital housekeepers), researchers have proposed the need to involve others in the process [213]. Our methodological approach underlines that involving the household is a promising venue for future research: throughout our study we are not aware of any noteworthy disagreement over the use of devices that leads to relationship issues or devices being abandoned. We believe our sessions with the household have provided the stage for every household members to share expectations and experiences, as well as to learn from one another. The key lesson here is that it is essential that we design in ways that facilitate *conversational familiarity*.

Digital housekeeping is widely discussed in the literature as an important yet contentious task (e.g., [25, 195]). We therefore suggest designing for 'digital housekeeping' [184] and other privileged users in ways that can contribute to conversational familiarity, to highlight opportunities for shared experiences that might facilitate processes of adoption. Prior research has suggested to design devices that are *accountable and transparent* to household members to allow for smooth integration into domestic routines [184]. The call for accountability and transparency in device design aligns with the social translucence approach we suggested above.

Another perspective akin to creating shared experiences and enabling other household members can be linked to the competence required on part of the community members when taking part in communal use. Since the community members orient their actions to not only expectations but also everyday concerns and social goals, we can characterise this competence in relation to roles as the ability to manage expectations in light of established social goals. With regard to rules, we postulate that they might be used to highlight competence-relevant aspects of the moral order to articulate their existence and importance to other community members, especially children. Important questions as to which opportunities and challenges are involved in this competence, how it could be fostered, and what its limits are require further research.

5.5.4 Purpose and Privacy

Manufacturers are obliged to seek users' consent by transparently documenting their data collection and processing practices in light of specific purposes [63]. This transparency requirement is usually satisfied in privacy policies and through the use of notice and consent frameworks. However, both face a lot of criticism in the single user context [134–137, 308, 310–312]. The criticism includes: (1) the set-up of devices requires a degree of practical reasoning that is largely unwelcome and even infeasible (e.g., reading privacy policies); (2) permission request models/patterns (pre-installation and/or during ongoing use) fail to take into account the situational (contextual, temporal, and occasioned) nature of preferences; and (3) the framework suggests the management of privacy could be an individual's exercise whilst the literature highlights the importance of the social (e.g., networked privacy in online social networks).

When it comes to smart technologies in communal use, these issues are amplified. We have found that: (1) individual challenges are fuelled by individuals aiming to manage others' accountability to the digital world; (2) 'privacy preferences' are rarely oriented to by individuals or the community, and only requested prior to or during installation as opposed to at the time of use; and (3) the configurations are to be performed by a single individual, providing little to no (technical or social) accountability to other users. Furthermore, based on a secondary analysis of the here reported data set, consent is dynamic in that people desire to grant, amend, and revoke consent at different points in time [48]. Relatedly, Speed and Luger [313] raise questions on consent given by those not actively or implicitly involved in the set-up and configuration of devices. As for devices without graphical user interfaces, other means are necessary to inform their users. It has also been pointed out that interactions with devices are not always deliberate and voluntary [313].

These 'notice and consent' challenges in the realms of the internet of things/smart home have long been anticipated [312]. Researchers have called on the community to fundamentally rethink the underlying approach to informational privacy and for novel design patterns [308]. Our insights into privacy in communal use highlight a misalignment of the technical interpretation of purpose by manufacturers and that by

their customers. Off-the-shelf smart home devices typically embody an orientation of purpose to the regulatory requirements of data collection and processing. As our study shows and our framework of communal use illustrates, households tend to orient toward everyday concerns of being good parents, a good neighbour, a good spouse, or a good child. Household members' orientation toward the purpose of device use becomes part of this social and moral order. The technical purposes found in smart devices are not naturally linked to household members' mundane concerns with managing relationships or expectations (see also [145]). Instead, they become "more of an abstract idea, that privacy rather than something I particularly want to keep, secrets" (Aaron, Household 4).

This misalignment between household goals and product designers' efforts to seek privacy as compliance must also be noted. To comply with data protection legislation, a lawful basis for data collection and processing practices must be established. This is most commonly achieved through the practice of obtaining consent, which needs to be meaningful and informed to benefit the users. However, given the observations summarised in this section, this goal might not be attainable with currently available tools and methods. We suggest aligning technical purpose and everyday concern can help address these power imbalances between users and manufacturers. As we will discuss further in Section 7.3.2, users can be empowered in their data protection rights (e.g., exercising more meaningful consent), and a better understanding of users' needs and demands can benefit manufacturers.

5.6 Conclusion

The goal of this chapter is to investigate the on-the-ground relationship between communal use and privacy. To this end, we have presented an ethnomethodologically informed study of six households' experiences with smart devices, offering an account of the organisation of communal use in terms of interaction, roles, moral order, and rules. With regard to privacy, we have expanded on prior work [14] by highlighting members' orientation toward relationships and the management of expectations rather than their preoccupation with privacy or 'control over information'. We have illustrated how our participants' concern of managing their relationships with and within the digital

world is a coordinated and sometimes distributed effort in the organisation of communal use. The coordination of these efforts requires adults to become conversational when device-related issues arise. We have discussed how roles and rules are constructed in this context, suggesting that the relationship of these concepts be reconsidered in light of relevant system design. Finally, we have discussed implications for design to better accommodate the 'sociality of work' for devices to be more 'transparent and accountable' in order to become an essential part of the moral order. We believe this orientation can help us address, not avoid, a broad array of privacy issues.

Drawing out these implications for design, we have limited ourselves to a perspective that allows us to sensitise designers to the ways in which social and moral order in the home are accomplished. However, we have not focused on intra-subjective issues such as discussing why individuals exhibit certain behaviours or what has motivated their actions. As we suggested in 'Enabling Users', within the organisation of communal use the actions of individuals can have far reaching consequences for other community members. Hence, design must better understand and support these kinds of perspectives. Taking individual influences on the communal organisation into account, the next chapter broadens the perspective to propose a conceptual framework that empowers privacy through innovation in research and design.

6

Informing Privacy Innovation for Communal Use

Contents

6.1 Introduction

Product designers and researchers ought to move beyond a "solutionism perspective that dominates legal and engineering discussions" [126] on privacy in smart homes. The Information Commissioner of the United Kingdom has called for efforts in "supporting trust in innovative data use" by engaging with designers and developers to consider privacy from "the earliest stage of development" [314]. Our stance is that data use can only be truly innovative in the eyes of the public if a holistic everyday perspective on purpose, collection, and use has been taken [140, 315].

Based on our empirical work on communal use of smart technologies in the previous chapters, we are uniquely positioned to offer a holistic perspective of everyday use that sets centre stage privacy as reflexively established in social values and human relationships. A perspective that, we hope, can facilitate innovation in product design and privacy research to rethink the use and value of smart technology for people.

To this end, our empirical work highlighted a need to sensitise designers to the ways in which local and moral order are accomplished in interaction. The implications in the previous chapter also highlight the need for a critical and reflective engagement with the ways in which communal use of technologies is enabled, thereby highlighting issues that system design cannot solve while motivating the need for user experience design to rethink communal use (see Section 2.3).

Broadly, user experience design teams are concerned with creating meaningful and relevant experiences for users. To achieve that, user experience designers ought to consider the *'why, what and how' of product use.* The insights in Chapter 5 were obtained from analysing members' 'meaning making' in interactions where the 'what and how' of product use is investigated. While sensitising concepts from EM provide for focus on actors, they do not consider cognitive processes which offer further insights into the 'why' of product use. We therefore complement the previously practice-oriented perspective with a cognitive perspective to gain further insight.

To facilitate the process of design for privacy and communal use, this chapter bridges the hitherto perspective focused on everyday interactions and agentic perspectives (i.e., conceptualisations of privacy as control over information) common in product design and data protection regulation. By juxtaposing the understanding of privacy as inherently social and embedded in context to common perspectives of informational privacy and data-driven innovation, the chapter provides the foundation for innovation in research and design beyond the principled implications given in the previous chapter.

Drawing on prior research and expanding on the previous chapter's framework of everyday interactions, this chapter provides a conceptual framework for innovation in research and design for communal use and privacy. It aims to answer the following research questions:

> ***RQ-3*** *How can the resulting findings inform innovation in research and design for privacy in the home?*
>
> ***RQ-3.1*** *What is the context for innovation in design and research for privacy in communal use?*
>
> ***RQ-3.2*** *What are opportunities for empowerment within that context?*
>
> ***RQ-3.3*** *How can design seize these opportunities to empower households?*

The conceptual framework *CoPriSm* situates our and others' findings within the HCI literature on privacy in the home (Section 6.4). The *audiences* for our framework are product designers, user experience designers and researchers, and privacy researchers in HCC. The framework can facilitate innovation through design thinking, help designers and researchers to understand requirements, and serve as a boundary object to discuss communal use and privacy in the home. The rest of this chapter provides insights for these different audiences. The next chapter includes two case studies that apply

CoPriSm in evaluating existing and creating new artefacts, thereby demonstrating its value for research and design. Depending on their interest in this work, readers might want to continue reading at different points in this chapter:

- Researchers interested in the **process of constructing the framework** may find related work in the next section (Section 6.2) and a description of methods in Section 6.3.
- Researchers and designers interested in **applying the framework** may want to continue by reading Section 6.4. The section presents the framework with its key considerations (Section 6.4.1) and provides instructions on how to use the framework as part of a design thinking process (Section 6.4.3).
- Researchers and designers interested in the **empirical and theoretical grounding** of concepts and their related considerations may find further details in Section 6.5.
- Researchers and designers interested in a **discussion of the framework's contributions** to the scholarship on communal privacy in HCC may wish to consult Section 6.6.

6.2 Background and Related Work

This section positions the framework in relation to existing interaction design frameworks and introduces an agentic perspective by reviewing literature from social psychology. Reflecting on this perspective, the section also discusses the need for responsible research and innovation with regard to empowerment.

6.2.1 Related Design Frameworks

Existing conceptual frameworks in HCI and CSCW articulate goals of awareness and intelligibility [222]. Notably, Bellotti and Edwards [316] have provided four principles to support intelligibility and accountability of interactions: inform the user of capabilities and understandings; provide feedback; enforce identity and action disclosure; and provide control "over the system and other user actions that impact him or her" [316, p. 202]. The authors emphasise the importance of considering relevant information

from outside the system and the effects of the system on the outside world as opposed to only within a system (previously proposed by [317]).

Awareness is an important feature of multi-user interaction design. Yuill and Rogers [318] have highlighted the need to consider "multiple concerns and dependencies when designing shared technologies" [222, p. 83] and discussed the implementation of social nudging—appropriate cues that suggest how one should behave. Designers and researchers have also been provided with a principled way for understanding how systems will be used in real-world contexts [222].

Erickson and Kellogg [279] have proposed social translucence to support multi-user interaction. Socially translucent systems provide appropriate accountability, visibility, and awareness akin to real-world properties of social interaction. By applying this approach to smart home environments in designing socially translucent smart lighting systems [309], Niemantsverdriet et al. [280] have subsequently developed their own "Designing for Awareness in Shared Systems" framework. They guide designers through a process of considering how to design for awareness, asking (1) what information is needed for awareness?; (2) how can awareness information be embodied?; and (3) how can awareness be used effectively in interaction?

While awareness, intelligibility, accountability, and visibility are important features for the coordination of communal use, these frameworks are focussed on interaction design. They provide little guidance on the relationship between everyday user interactions with the practical matters of privacy and the organisation of labour in the home. However, as our Chapter 5 has illustrated, privacy needs to be considered as a pervasive feature of system use—a value and social goal implicated in interactions (see also [146]). There is then a need for a framework that links the organisation of everyday use with practical matters of privacy, bridging abstract values and facets of communal use to particular design features.

6.2.2 Modes of Agency and Action

The interaction design frameworks discussed above are grounded in an agentic/socio-cognitive perspective on action. In the most basic sense, agency describes an actor's

faculty for actions. Although the concepts of agency, actor, and action are widely accepted, "agency is a fundamental and foundational category and puzzle in virtually all social sciences and humanities" [162]. Across the meta-theoretical split of micro (reductionist approach, only actors are real) and macro (large scale social entities are irreducible) perspectives, there is disagreement over definition, range, and explanatory power of agency.

Albert Bandura's Social Cognitive Theory (SCT) [319] and his work "Toward a Psychology of Human Agency" [320] are the foundations for the ongoing debates. We briefly summarise these foundations below while acknowledging that researchers have since expanded on and refined its elements.

Individuals have some means of control over their own behaviour, which in turn contributes to an expected outcome. Cognitive regulation of motivation and action takes place through exercising forethought, self-reactiveness, and self-reflectiveness. To exercise control (self-regulation) appropriately, agents require awareness of the environment (social and physical), awareness of potential impacts of actions on the environment, and clarity on the expected outcomes and feedback on their progress of achieving a particular goal. Individuals struggle with self-regulation if there are no indicators that a considered behaviour would be morally right or wrong. Under such circumstances, individuals rely on others' feedback to assess how well they are doing.

Part of self-regulation is self-reactiveness. Self-reactiveness describes an individual's ability to construct appropriate courses of action. To give meaning and purpose to their actions, individuals compare goals based on a value system, a sense of personal identity, standards for environmental and biological conditions (e.g., appropriate to age), and limitations. Goals then motivate actions through self-evaluation of expected outcomes. However, goals do not trigger actions directly and can be of different challenge and temporal proximity. Distant goals are best broken down as part of a goal hierarchy to combine distal aspirations and proximal self-guidance.

Self-regulation of actions also relies on moral agency, linking moral reasoning and knowledge to conduct. As part of their cognitive processes, individuals evaluate moral judgements against personal standards and situational circumstances. Over

time, they develop a competence to comply with the moral order while their own standards for appropriate behaviour increase. Considerations of moral behaviour are culturally situated. Note that moral agency needs to be activated by an actor, and can indeed be disengaged on many occasions—people have the ability to act against their moral judgements [321].

An important aspect of self-reflectiveness is self-efficacy, which is defined as an individual's belief of their ability to influence the outcome of their actions [322]. Self-efficacy is affected by four main factors: experience ("enactive attainment"), modelling/observing others' success ("vicarious experience"), social persuasion (e.g., encouragement), and physiological factors (e.g., central nervous system arousal to distress and top-down regulation). Self-efficacy beliefs influence whether people think and feel positively or negatively about themselves in relation to their environment. They decide which environments people are willing to enter and which activities they engage with.

Individuals use *proxy-agency* by enlisting others to act on their behalf. To exercise proxy-agency, individuals rely on perceived social efficacy [319]. Motivations to delegate through proxy-agency include beliefs that others can do things better, desires to not bother oneself, and the fact that skill and knowledge require practice and dedication. Individuals might desire to exercise less self-agency which requires management of responsibility (here, being accountable for ones actions), stress, and risks. Therefore, Bandura describes proxy-agency as 'vulnerable security' that draws on competence, power, and favour from others. Exercising proxy-agency reduces opportunities to practice self-agency which could increase self-efficacy. Relinquishing control through proxy-agency may not always be perceived as hindering future competence at the moment of delegating. For example, while the presence of someone with high competence can undermine one's skills, people can find ways to effectively foster self-efficacy in each other.

To summarise, individuals are "not simply onlookers" or products of their behaviour [320]. According to Bandura's [320] theory, people are "self-organising, proactive, self-regulating, and self-reflecting" agents, and thus the main contributors to their behaviour. Agency, however, requires the involvement of other agents. Different modes

of agency require "commitment to a shared intention and coordination of interdependent plans of action" [320]. The next section discusses these insights on the self, proxy, and collective agency in light of communal use.

6.2.3 Agency and Action in Communal Use

In the context of smart home related research, agency is probably best defined as the capacity to act for ourselves. Such capacity hinges upon power, skills, means, and opportunities. Agency can be fostered or curtailed, e.g., by revoking access to assert one's own preferences [34]. However, as a 2012 paper suggests, striking a balance between user-centric and technology-centric agency is a difficult task [323]. Page et al. [197] discuss a disagreement over the level of control among their participants, suggesting that perceived proxy-agency [320] brought about by automation in 'smart' devices has been the object of disagreement among users. Geeng and Roesner [5] argue that those in charge of installing devices often have "outsized agency around, control over, and access to smart device data and functionality" [5]. Based on these perspectives, providing (a feeling of) appropriate agency is articulated as design goal [213], e.g., to enable by-standers' agency in other peoples' homes [208]. Others have described different situations for proxy use, e.g., as part of a household organisation or on behalf of children [324].

Aspects of Bandura's work also feature in other research on technology use and privacy/security. Perhaps most prominently is his theory of self-efficacy [325], which has been used to understand effects of stewardship (e.g. [298, 326, 327]) and explain individuals' (e.g. [203, 328]) and collectives' ability to protect their privacy online (e.g. [297, 329]). While these contributions have taken into account some aspects of Bandura's work, we believe a more holistic consideration of agency and action is warranted. In Table 6.1, we document how discussion of human agency and actions fits with community members' behaviour in the home (Chapter 5). Although we could observe and document only household members' actions and accounts of their actions, at times participants also articulate their goals and expected outcomes. Hence, our insights resemble the three different modes of agency. Bringing together prior research,

our interaction perspective along with insights from human agency, we discuss this more holistic consideration below.

Table 6.1: Bandura's modes of agency illustrated

Modes of agency	Example
self individuals that act according to their own goals	[...] Felicity: Yeah. See if you can get the music on. Carrie: Yeah. Let me do the privacy thing first. Felicity: The privacy is more important. [...] Felicity: Yeah. I thought I saw it. Go down. Music. Carrie: No. We are doing privacy at the moment, Felicity. – Vignette 5.15
proxy individuals ask others to act on their behalf	Cassie: But can I say, "Can you set that scene in the kitchen?" Frank: Yes, it is configurable on a room-by-room, bulb-by-bulb setting. Cassie: Okay, well, then we should do that, set one up for cooking and eating. Frank: Yeah, I have but you have not found them and it is easy enough to change them, right? [...] Researcher: How do you usually find out about new things? Cassie: When I see Frank doing it. – Vignette 5.5
collective groups of people collectively working toward a shared goal	Rosa: yeah so he did the set-up and then it transferred it to my phone. And that's when I change the name of the cameras because it was something with long numbers but if you see something like back of garden then you know exactly what you are looking into Researcher: and are you getting all of the notifications too? Rosa: yes, but I mute them during the day Researcher: so you mute them but do you also look at the cameras at the recordings? Rosa: sometimes, not, I guess, I guess I have other things in my head when I come home. It's interesting to see. I guess because I know he will o it. I will take a secondary role but perhaps If he didn't then I would build that into my day. – Vignette 5.6

Here, moral agency links human agency to the interpreted values and social goals bound up in the moral order through a process of self-regulation, situating any action within the triadic reciprocal causation of environment, behaviour, and self. Bandura also holds that "people are producers as well as products of social systems" [319, p.

15]. Similarly, the moral order is reflexively established in coordinate work between household members. It is "not a determination or a causal nexus" but rather "the reflexive nexus of social praxis" [165, p. 237]. While conceptualisations of morality between these two perspectives might be different, the ways in which individuals orient their actions to different understandings of 'right' (normally expected) and 'wrong' are similar. Hence, we draw on the field of social psychology to consider cognitive processes involved in the organisation of work in the home.

6.2.4 Power, Empowerment, and Responsible Innovation

In Section 1.2, we subscribed to a "reconceptualization of power as a capacity or ability, specifically, the capacity to empower or transform oneself and others" [27] which aligns with the notion of empowerment as "a process by which people, organizations, and communities gain mastery over issues of concern to them" [32]. We also described our goal of increasing *power-to* such that there exists an *equality of opportunity to access resources* [31].

We also used Wartenberg's [33] response to feminist conceptualisations of power (*transformative power*) to illustrate the fine line between supporting and controlling behaviour. This challenge is reflected in the introduction and discussion of SCT, particularly in the nature of proxy agency as 'vulnerable security'. Bandura describes proxy agency as relying on competence, favour, and crucially power [319]. Where proxy agency is at work, people have to rely on their proxies goodwill to be supporting rather than controlling. This is problematic as proxy agency might decrease *power-to* and increase dependency on others in a way that is disempowering.

The relationship between empowerment and proxy agency requires careful consideration as we illustrate with a discussion of power in intimate relationships of which gender is a particular feature. Power balances ingrained in intimate interpersonal relationships are delicate (e.g., [7]). For example, power balances surface as gendered performances of technology use where exercising proxy agency may be desired to nurture the relationship [199]. A resulting shift in skill and ability between individuals is not necessarily a remarkable problem for household members (e.g., it was only

remarkable for household 4 in Chapter 5). Proxy agency, however, can also be unwelcome and even reinforced unwittingly where the design of devices unequally caters for gendered performances [198] such that the "landscape of responsibilities" in the home changes [25]. Devices can fuel existing imbalances that are not always visible and facilitate coercive or controlling behaviour through their affordances [195, 196].

It would be imprudent to assume one could anticipate these issues. We cannot readily anticipate technology use (recall Venkatesh's [176] comment on the unpredictability of what households will actually do with technology [176]). Second, preventing malicious usage while enabling legitimate use by design is a challenge that requires new considerations of usability and security [330]. Finally, uptake of more complex technical configurations for dynamic social contexts is limited (e.g. [213]). As much as it is desirable to consider upfront the impacts of design decisions discussed in the previous paragraphs and offer flawless designs, such anticipation hardly seems possible.

Evidence-based evaluation of ethical issues such as power and empowerment is a common dilemma in research and innovation. It is usually unclear what outcomes an innovation might bring about, i.e., how new designs might be used. Certainly, not all outcomes are always desired. Researchers in RRI ask, "how should we proceed under conditions of ignorance, uncertainty and ambiguity?" [331, p. 114]. The RRI approach aims to "anticipate and assess potential impact and societal expectations with regard to research and innovation" [1]. Responsibility is typically understood as care and responsiveness (non-reciprocal and future-oriented) as opposed to interpretations as liability, accountability, or blame [332]. The notion of responsiveness (as corrigibility [333]) encourages innovators to continuously act to correct decisions made in error, to adapt to changing environments, and to consider views and changing perceptions.

Innovators are encouraged to be *anticipatory* of possible outcomes/effects, *reflective* of opportunities and motivations, *deliberative* in making decisions, and *responsive* to possible alternatives. These commitments allow innovators not only to reflect on their own intentions and motivations but also explore perspectives of other people. Given the goal of the process is to reduce the likelihood of unintended negative outcomes,

[1] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/responsible-research-innovation

RRI facilitates constructive democratic stewardship and fosters a collective duty of care among researchers and innovators [331].

> Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society). [334, p. 9]

Different approaches of RRI are broadly discussed, drawing on combination of existing tools and methods such as technology assessment, "upstream" engagement, and anticipatory governance [332]. Among these approaches is the AREA framework adopted by UK research councils. The framework encourages researchers to implement RRI principles in four phases[2]: *anticipate* possible impacts, *reflect* on purposes and intentions, *engage* with other perspectives in inclusive ways, and *act* to influence direction and trajectory of the research process itself.

These processes, tools, and methods of RRI will inform our efforts to empower communal use and privacy in the home. Exercising foresight and anticipation, we further discuss potential misuse of the framework as well as the value and application of RRI practices in Section 6.4.2.

6.3 Methods

Our method for creating the conceptual framework is based on 'conceptual framework analysis' [281] to provide a deeper understanding of a phenomenon by interlinking a set of concepts [281]. Following Jabareen [281], we only include concepts (not factors or specific behaviours) in our framework. In establishing relationships between concepts, the framework provides the foundation on which a range of phenomena related to communal use and privacy can be further explored.

By placing "soft interpretations" on empirical data from Chapters 4 and 5 and prior research insights [281], we identify the concepts presented in Table 6.2. We then draw connections between analytic and sensitising concepts (from Chapter 5) to make

[2]https://epsrc.ukri.org/research/framework/area/

Table 6.2: Salient concepts in multi-user and privacy-related research on smart homes

Reference	awareness and intelligibility	ownership, and power	relationships	contextualising	socio-technical affordances	agency and action
Chalhoub et al. [48]	X	X			X	X
Crabtree, Tolmie, and Knight [145]			X	X		
Garg and Moreno [34]	X	X	X		X	X
Geeng and Roesner [5]		X		X	X	X
Jakobi et al. [205]	X	X		X		
Jakobi et al. [335]	X		X	X	X	
Levy and Schneier [7]	X	X	X			
Murthy et al. [298]	X	X	X		X	X
Naeini et al. [202]	X					X
Richardson [151]		X	X			
Tabassum et al. [217]			X		X	X
Watson et al. [327]		X	X		X	X
Yao et al. [208]	X	X	X	X	X	X
Yao et al. [143]	X	X	X	X	X	X
Zeng, Mare, and Roesner [193]	X	X			X	X
Zeng and Roesner [213]	X	X	X	X	X	X
Zheng, Chetty, and Feamster [336]	X	X	X	X		
Chapter 4		X	X	X		
Chapter 5 (e.g., Vignette)	5.2.1	5.7	5.11	5.2.1	5.7	5.5

warranted assertions. This approach is discussed in relation to Jabareen's [281] eight steps of conceptual framework creation below.

Unlike systematic literature reviews/surveys which aim for an exhaustive search completion, conceptual framework analysis strives for theoretical saturation. The goal of conceptual framework analysis is to identify salient concepts from a range of different data sources. The researcher 'stops' when theoretical saturation is reached, i.e., querying an existing data set and/or collecting additional data does not yield further insights on

the topic. Data sets can include any kind of empirical data, including but not limited to research data, newspaper articles, or research papers.

Phases 1–5 We iteratively query our data set and expand our literature search until saturation of concepts is reached. At the end of this process, our data set includes soft interpretations of our empirical data in Chapters 4 and 5, and 69 articles spanning the fields of HCI, CSCW, and Human-Data-Interaction, and other studies at the intersection of anthropology and media/information studies. The articles are collected as follows. Drawing on literature from our review of privacy in the connected home, we complement this literature with a cursory Google Scholar search using key words that reflect our research focus on multi-user challenges, social relationships, and privacy in smart homes. "Privacy AND 'smart home' AND 'social relationships' OR multi-user" were the search terms we used. Based on our screening criteria, we include studies with a focus on multi-user or social relationship issues while those with no empirical contributions are excluded. Following references from [145] to find other EM informed work, we search the ACM Digital Library using the terms 'ethnomethod*' and one of the following terms: 'home computing', 'home network', 'ubicomp', or 'smart home'. The screening criterion is to include empirical and ethnomethodologically-informed studies on the use of internet-connected technology in the home. As we reach theoretical saturation, we stop including additional materials from these queries and arrive at 69 articles.

Through iterative reading and coding, we arrive at a set of candidate themes. We deconstruct these candidate themes to identify "main attributes, characteristics, [and] assumptions" [281]. Lastly, we synthesise these themes to form our set of concepts. Final concepts and their empirical grounding across *key* papers are presented in Table 6.2.

Phase 6 We situate the identified concepts in relation to smart home core components identified throughout our literature review in Chapter 2 (smart technology, community members, and information).

New We add an agentic perspective to our framework that allows us to put concepts into action.

Phases 7–8 We discuss our framework with other researchers at the department to refine concepts and their connections.

6.4 The Framework: Communal Privacy in Smart Homes

The resulting conceptual framework, CoPriSm, is depicted in Figure 6.1. The framework draws connections between community members, smart technology, information, and moral order to highlight the relationships between the organisation of communal use (roles, rules, and different modes of interaction) and relevant research perspectives (socio-technical affordances, contextualising, and awareness/intelligibility). It suggests design perspectives (manage, enable, embodied) as ways to facilitate communal use through innovation.

The organisation of communal use derived from an EM-informed study and grounded analysis in the previous chapter is at the core of CoPriSm as seen in how the purple circle in the upper right corner is placed at the centre of the framework. CoPriSm situates communal use in relation to research and design perspectives by complementing the interaction-focused perspective of the previous chapter with an agentic perspective (semi-transparent, white overlay in the centre).

In summary, communal use in the home evolves around information generated by community members interacting with smart technologies, some of which in turn becomes available to the community members. However, community members participate in the use of smart technologies, generation of information, and consumption of information to different extents. Interactions between household members and with devices reflexively establish moral order as values, goals, and everyday concerns.

Moral order is established in coordinated action by community members [166]. Part of these negotiations are everyday concerns or social goals, e.g., 'being a good neighbour' or 'being a great parent'. The analytic concept of privacy (e.g., as control over information) dissolves into these everyday concerns ([145] and Chapter 5).

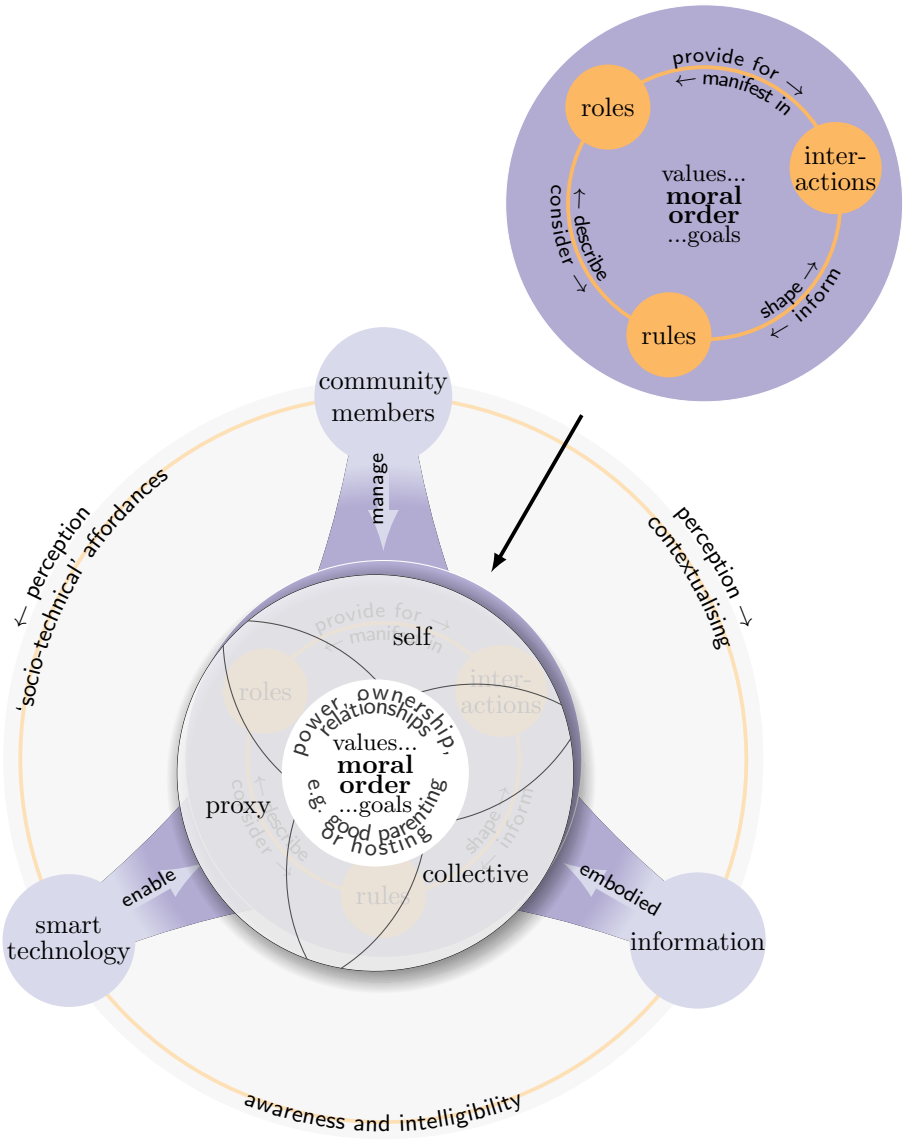


Figure 6.1: 'Communal Privacy' in Smart Homes (CoPriSm) – Conceptual framework to inform research and design

The concepts of power, ownership, and relationships are considered as perspectives on *values* implicated in the moral order. That is, communities and their members reflexively establish moral order while orienting to locally appropriate interpretations of distributions of power, rights and obligations of ownership, and qualities of relationships.

It is important the nature of this relationship be acknowledged as it links our empirical, conceptual, and descriptive work to the politics of empowerment and further ethical considerations involved. Hence, the construction and application of

Table 6.3: Framework overview of themes and concepts

Section	Concept	Considerations
6.5.1 How is communal use organised?		
6.5.1.1	Interactions	What are important interactions with devices and between householders?
6.5.1.2	Roles and Rules	How does the smart technology contribute to the establishment of roles and rules?
6.5.1.3	Modes of Action	How does the smart technology support different modes of actions?
6.5.2 How can communal use be facilitated?		
6.5.2.1	*Managing* communal use	How can community members *manage* smart technologies in communal use?
6.5.2.2	*Enabling* communal use	How can smart technologies *enable* interactions of communal use?
6.5.2.3	Information is *Embodied*	How can information be *embodied* for communal use?
6.5.3 How can research perspectives contribute to communal use?		
6.5.3.1	Contextualising	How can information be contextualised within communal use to be meaningful?
6.5.3.2	Awareness and Intelligibility	How do smart technologies support awareness and intelligibility for communal use?
6.5.3.3	Socio-Technical Affordances	How do technologies afford interactions of communal use?

this framework cannot disregard the design politics involved. We provide important considerations and guidance on *empowering households* (Section 6.4.2) after introducing the framework with its concepts.

6.4.1 Key Considerations

This section summarises the three main framework themes: communal use, related research areas, and design perspectives. Key considerations of these themes are also listed in Table 6.3 alongside references to their grounding in Section 6.5.

6.4.1.1 How is communal use organised?

Important considerations for the organisation of communal use include:

- *What are important interactions with devices and between householders?*
- *How does the smart technology contribute to the establishment of roles and rules?*

– *How does the smart technology support different modes of actions?*

Communal use refers to when members of a community, such as a household, use and share access to smart technologies. Note that individuals do not necessarily use or share the same levels of access to smart technologies in the same way. Instead, the use of technologies is arranged within a fluid division of labour that is continuously negotiated between community members.

The interactions of household members with smart technologies contribute to the establishment of social and moral order in similar ways to interpersonal communication/interaction. Smart technologies thus become an essential part of social and moral order in the home through the ways in which interactions contribute to the construction of roles and the use of rules within the organisation of communal use.

Roles and rules are dynamic constructs that only exist in interaction. When community members articulate roles, they highlight expectations related to everyday concerns. Roles are not a set of rules, and rules do not prescribe roles. By articulating rules, community members highlight expectations of moral order. Importantly, rules do not prescribe actions but provide intended meaning for interactions by articulating goals and values implicated in moral order. In this sense, they are fundamentally different from their counterparts used in system design [188].

In fact, there is a fluidity in terms of who does what with community members moving in and out of roles. The performance of interactions by different community members can also be examined from a socio-cognitive perspective. This perspective suggests that we must distinguish between self, proxy, and collective agency and action: community members at times act only in their own interest; they sometimes act on behalf of others; and they collectively work together in other cases. Where their own goals conflict with those of the group, community members rely on moral agency to orient these actions to moral order.

6.4.1.2 How can communal use be facilitated?

Community members, smart technologies, and information offer pathways to facilitating communal use. These pathways can be considered in terms of the following questions:

- *How can community members manage smart technologies in communal use?*
- *How can smart technologies enable interactions of communal use?*
- *How can information be embodied for communal use?*

Taking an agentic perspective, community members interact with each other and with devices. Their 'self'—personal characteristics, experiences, and preferences in regard to levels of agency and independence—and their ability to exercise moral agency and foresight contribute to the ways in which community members take part in communal use. Community members contribute to the co-creation of roles, gender identities, and practices of use. Community members manage their relationships with and in the physical/digital world through the use of technologies.

Smart technologies can also enable management through appropriate affordances that fit with the (dynamic) needs of the community (e.g., affordances for different modes of action and use as described above). Considering different modes of actions also allows designers to consider non-use of devices in light of proxy actions (members acting on behalf of/ in consideration of each other). Crucially, affordances enabled by the interactions influence the ways in which moral and social order is established.

For community members to make meaningful choices, appropriate information needs to be embodied in smart technologies and presented alongside these affordances. Smart technologies can become part of accountable practices of communal use through supporting transparency, visibility, and intelligibility to achieve context-appropriate accountability of device use. This accountability lies in part in understanding the social appropriation of devices, that is, making device use more purposeful and meaningful for the community. Embodiment of information can also help close evaluation gaps between community members' expectation of data collection and processing practices and manufacturers' actual practices.

6.4.1.3 How can research perspectives contribute to communal use?

To facilitate the establishment of communal use, researchers and designers draw on research areas at the intersections of community members, smart technologies, and information. Relevant considerations include:

- *How do smart technologies support awareness and intelligibility for communal use?*
- *How can information be contextualised within communal use to be meaningful?*
- *How do technologies afford interactions of communal use?*

Topics of awareness and intelligibility are frequent in research that seeks to make smart technologies more accountable to community members by creating transparency. Both concepts are important for data protection legislation that defines the need to make individuals aware of data collection and processing practices in intelligible ways. Smart technologies often lack in that regard. These concerns also extend beyond matters of data protection (e.g., notice and consent). Where appropriate awareness and intelligibility of a device functionality is broadly lacking, community members' efforts to make smart technologies work for the community are hampered. These perspectives of more and deeper insights into how smart technologies work does not necessarily lead to expected actions and outcomes.

Transparency of data flows does not necessarily motivate action. Community members are not concerned with the flow of data but with the meaning that others can attribute to the data, the information others gain. Appropriate controls for information management, rather than data management, are lacking. For example, data cannot be turned into information by adding an array of contextual factors. Instead, systems should enable articulation work that makes digitally collected data meaningful in light of social and moral order.

'Articulation work' [306] and communal use more broadly require socio-technical affordances. These affordances account for the social embeddedness of interactions by pairing control with meaning-making to enable coordination of activities and thereby facilitate social negotiations of device use. Socio-technical affordances rely on contextualisation of relevant information. Such information is required for individuals to orient to the community appropriately, and it needs to be provided in awareness raising and intelligible ways.

6.4.2 Empowering Responsibly

Our discussion of power, empowerment and responsible innovation in Section 6.2.4 encourages our commitment to *anticipate*, *reflect*, *engage*, and *act*. Here, we *anticipate*

possible impacts of creating the framework and *reflect* on our purposes and intentions. Insights from these activities motivate not only a call to action but also a call for engagement with other perspectives.

The framework's purpose is to foster innovation in research and design for communal use that empowers privacy in smart homes. We constructed the framework to serve this goal by highlighting how communal use was organised, how it can be facilitated, and how research and design perspectives can contribute to its establishment. The construction of the framework was carried out based on a particular definition of empowerment. However, we highlighted in Section 6.2.4 that people with other conceptualisations of empowerment or other intentions could exploit proxy agency to serve their goals. This ambiguity requires us to extend our critical reflection beyond our own perspective to include different viewpoints.

In what way can the framework be used to amplify and exploit power imbalances by design? Proxy agency as 'vulnerable security' can contribute to imbalances as we discussed in Section 6.2.4. For example, to increase 'vulnerable security,' designers could trick or force people into using proxy agency through lack of multi-user support. They could also encourage the use of proxy agency by design but in ways that do not contribute to an establishment of communal use. The actions of proxy agents would not serve to empower through role modelling. Instead, the outcomes and effects of proxy actions would be hidden. Relevant information would not be contextualised such that an interaction became accountable to the community of users. The design would not provide the necessary affordances (e.g., using frameworks such as social translucence to provide a degree of awareness and intelligibility of the system state). Proxy agents could be dissuaded or prevented from engaging moral agency particularly when effects on others are not apparent, leading them to embrace false beliefs over the acceptability of their actions.

When relationships break down, individuals might initially limit their ex partner's access to devices. The 'optics' of these configuration changes matter [7, 330]. While our framework does not suggest particular access control configurations, designers could

present to the community of users information on configuration changes in context-appropriate ways. They could also decide to make such information only visible to a single administrator user. This could prompt a situation in which configuration changes by administrators become 'decontextualised' due to lack of signalling character for users.

Coercive control depends on close, often domestic, relationships and includes practices of isolating victims, controlling aspects of every day life, monitoring and surveillance, and threats and intimidation [9]. Our framework could be used to facilitate coercive control. For example, through inappropriate levels of awareness and intelligibility of the system status and related information, 'data leakage' could serve to isolate, shame or humiliate individuals [9]. Knowledge about inappropriate levels of awareness and intelligibility of other users could similarly be exploited to isolate individuals. Finally, different household members favour different kinds of affordances. Disparity in the level of control offered by different affordances (e.g., analogue versus digital, or on device versus remote control), could contribute to unremarkable data leakage, covert monitoring, and a lack of control for some users.

As illustrated by these examples, it is not obvious how to enable legitimate use while preventing illegitimate use with good usability [213, 330]. Research and design efforts using the framework ought to consider this challenge and the issues discussed above. **Acting** on the reflection and anticipation done in this section, we recommend the following two measures:

1. Reflect on design politics. Transparency helps one reflect on purposes and intentions during design and research processes. Heeding the call of Schneider et al., we strongly encourage designers to articulate their own politics and conceptualisations of empowerment [24]. Schneider et al.'s [24] conceptual framework of empowerment in HCI requires engagement with four different dimensions of empowerment: (1) the concept of *power* such as power-to or power-from; (2) *psychological components* (feeling, knowing, and/or doing) as intended outcomes of empowerment; (3) the *persistence of empowerment* as either transient or persistent; and (4) the *design mindset* as either expert or participatory [24].

Table 6.4: Engaging with CoPriSm to unpack design and research challenges

Type and starting point	Example
Observed phenomenon: value orientation	power imbalances (e.g., outsized agency of one community member [5]) or perceptions of 'privacy violations' (e.g., devices sharing data with third parties [336])
Usability issue: technology failure	customer reports on failure to support 'household roles' appropriately (e.g., single administrator only)
Social needs: goal driven	use case oriented design or considering multi-purpose use of existing devices (e.g., security cameras for entertainment [48])

2. Employ an RRI approach. We also encourage researchers and designers to apply RRI methods and techniques when using the framework. Our discussions and reports of technology use throughout this thesis resonate with those who develop and practice RRI for HCC [337]: "the future cannot be predicted, but there is room for exploring different possible pathways" [338]. The next section details a design thinking approach that can be used to explore different possible pathways with an RRI mindset. While researchers and innovators in HCC often show some elements of RRI practices, it is important that these practices are cultivated further [338]. To this end, we also **engage** with different perspectives through case studies in the next chapter.

6.4.3 Practising Design Thinking with CoPrism

The conceptual framework CoPriSm presented earlier in this chapter is tailored towards designers and researchers. We have suggested that both can draw on the framework to foster innovation for privacy and data protection by design. This section describes the way in which CoPriSm informs the work of design thinking. However, the steps discussed below are also useful for any empirically informed innovation process concerned with communal use of smart technology in the home.

Don Norman described that the work of design involves how one "take the original problem as a suggestion, not as a final statement, then think broadly about

what the real issues underlying this problem statement might really be"[3]. It is the designers' task to resist the temptations to jump to conclusion before fully understanding a problem space. To avoid searching for a solution before the actual problem is well understood, designers have to consider a broad range of possible solutions before they finally converge on one [139]. The process of design thinking is typically described in five steps that are not considered sequential but interlinked and repetitive. These include empathising with the user, defining the problem, ideating candidate solutions, prototyping candidate solutions, and testing with users.

The framework considers privacy as socially embedded and reflected in moral order. Furthermore, the framework is applicable to different kinds of research and design challenges as listed in Table 6.4. To successfully address these challenges, the design thinking process needs to emphasise the importance of social goals and values reflected in everyday use. The framework itself then can facilitate design work during different phases of *empathise* (overview in Figure 6.2) as well as *define* and *ideate* (overview in Figure 6.4).

Design Thinking Instructions for CoPriSm

The following paragraphs are written as instructions for design thinking with CoPriSm.

Empathising Draw on individual lived experience (better: include stakeholders in some form, e.g., interviews or co-design for brainstorming; best: collect empirical, observational data) to *empathise* with users and unpack the phenomenon within the social organisation of the home, i.e., investigate its accomplishment in everyday interaction by considering Section 6.4.1.1 (*How is communal use organised?*). Trace your path throughout the framework (inside out or outside in – starting points see Table 6.4) to make sure you have established a holistic picture of the problem at hand, and keep considering social goals and values. These can act as your checks and balances to understand how people might appropriate technologies and for which goal/value negotiation and coordination design needs to provide. These social goals

[3] https://jnd.org/rehtinking_design_thnking/

and values will also allow you, as designer or researcher, to become more aware of your own 'design politics' (*Empowering Responsibly*).

Figure 6.2: Empathising – Understanding the problem

- Identify the nature of your problem according to 🔍 Table 6.4. What is your starting point?
- Start out by considering sequences of actions that constitute or contribute to the establishment of communal use (How is communal use organised?). Trace path from outside in or inside out in 🔍 Figure 6.1 to begin unpacking the social context of use. How does the use of smart technology contribute to establishment of moral order? What is the local moral order, its values, and social goals? What are the politics involved in the problem at hand, and can these politics be expressed in terms of values such as power balances, ownership challenges, or relationship issues?
- Take another look at the interactions involved in your candidate descriptions of the design problems and your ideas for solutions. What are the local/user politics involved? Who should be doing what, on whose behalf, and to the benefit of whom? Who might be disadvantaged?

Methods such as storytelling can facilitate this process. Make sure to take note of social goals for sequences of actions.

📖 Read Section 6.6 for ideas and deepen your understanding

Designing and Ideating As you start moving from *empathise* to *design and ideate* phases, you will explore ways to address the challenge at hand. At this point, shifting towards an agentic perspective is beneficial. Start organising actions that will become part of an intervention according to their agentic mode (self, proxy, and collective), not just as you already considered them but also as how they could be (e.g., most actions could be done by individuals themselves or by others on their behalf, and these two options come with their own implications). Then start to consider how these interactions can be augmented to make them work for the community, e.g., by using socio-technical affordances, contextualising information, or fostering awareness and intelligibility (Section 6.4.1.3 – *How can research perspectives contribute to communal use?*). This consideration maps onto the design design dimensions (enable, manage, embody) that are worth reconsidering at this point (Section 6.4.1.2 – *How can communal use be facilitated?*).

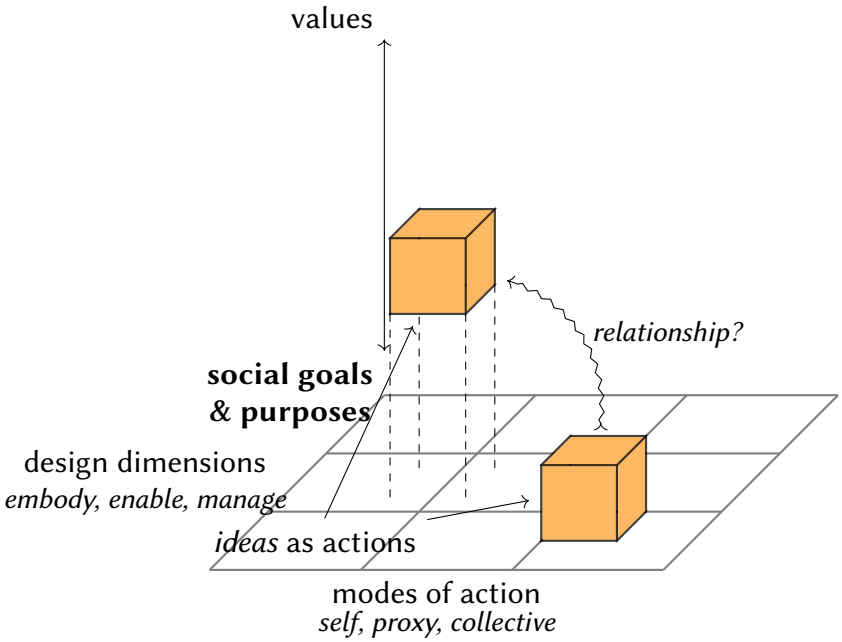


Figure 6.3: Thought model of shift towards agentic perspective

Note that this process can be complemented by any number of UX tools and methods. For example, it might be useful to break down actions that any design intends to enable into a schema as depicted in Figure 6.3. While considering which social goals (e.g., being a good parent) and values (e.g., independence) they serve and which purposes (e.g., protecting children) might be attributed to them, the schematic organisation of ideas (actions) across design dimensions and modes of actions can provide useful grounds for discussion. Note that ideas (orange boxes) can relate to one another, and that exploring this relationship is important. Do they serve the same values and goals but draw on different modes of actions or design dimensions? This and variations of the question along the three dimensions of Figure 6.3 are worth exploring. For example, community members might work from different angles of related goals to make technology work for the community. However, technology is unlikely to work for the community if members pursue different social goals. Researchers and designers might support this process by applying strategies such as value sensitive design [339].

Finally, designers will converge on one solution and start testing it with users. In design thinking, the testing phase also informs the empathise and ideate phases.

Figure 6.4: Defining and Ideating – Shaping solutions
In considering the questions below, work out principled ways for your intervention ideas, e.g., which mode of action, which kind of intervention (enable action through technology, manage social relationships to influence others, or embody information in technologies to facilitate accountability), and to what end (How can communal use be facilitated? and How can research perspectives contribute to communal use?).

- Identifying – What are useful design goals to capture insights from the empathise stage?
- Realising – How can these design goals be realised?
  - What 'sociality of work' is needed? Also consider: what actions are involved in the interventions you are considering? What is the mode of these actions (🔍 6.5.1.3 Modes of Action)?
  - How can these interactions be augmented to make them work for the community? How can they contribute to establishment of social goals and avoid conflicts with values? Have you considered transparency, intelligibility, and visibility?
- Mapping – How do these augmented interaction modes map on design intervention perspectives (enable, manage, embody)?
- Cross-checking – Cross-check your findings with insights from the empathising phase, especially how social goals are implicated. Is there a chance to make interaction less ambiguous to the community? Are they accountably linked to social goals? Are they in line with values and design politics?

Be aware of design politics: challenge your understanding by acknowledging that what we perceive as power, ownership, qualities of relationships, and laudable social goals just is part of a locally occasioned and negotiated social and moral order (e.g., use value sensitive design [339]).

📖 Read Section 6.6 for ideas and to deepen your understanding

Designers will compare user testing insights with previously made assumptions and the goals they have set. The structure we outlined above will support that process.

6.5 Further Considerations for Research and Design

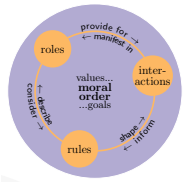
The detailed descriptions of concepts presented here overlap with the summaries presented in Section 6.4. The reader might choose to apply the design thinking approach without reading this section and instead use this section as reference.

6.5.1 How is communal use organised?

Communal use is dynamic and continuously evolving through interactions. Roles and rules have particular social meanings for the organisation of communal use. We

complement the everyday perspective by considering interactions as self, proxy, and collective in nature.

6.5.1.1 Interactions

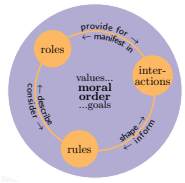


The existence of smart technologies and their relevance to the household community are constituted in interactions among household members. These interactions provide the foundation to explore roles, rules, and moral order (social goals, values, and everyday concerns) as these concepts are also constituted in interactions. Interactions constitute issues of setting up and maintaining devices but are also relevant during ongoing use.

To make visible the relevance of smart technologies to the community, members draw on resources like pre-existing knowledge, exposure to reading materials, and past interactions with similar technologies. These different resources are equally important for ongoing social negotiation of devices use that constitutes in interactions.

Design of smart technologies needs to carefully consider which interactions contribute in which ways to the establishment of communal use.

6.5.1.2 Roles and Rules



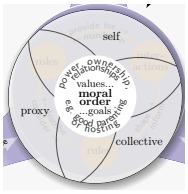
Roles and rules are part of the reflexive establishment of moral order (Chapter 5). In summary, roles are used by community members to articulate expectations related to an intended social goal that provides meaning for their actions. Rules (role expectations) do not prescribe roles, and neither roles nor rules are sufficient for predicting behaviours. Situated in articulations of moral order, role expectations are invoked to highlight intended meanings and readjust actions to moral order. A specific competence to orient actions in this way is required to contribute to the coordinate work that establishes moral order, one which is frequently not attributed to children.

Consequently, roles and rules have specific, situated meanings that serve purposes within the social organisation of the home. Here, the meanings and purposes are not necessarily akin to the use of roles and rules in system design. This has several

important implications for design: 1) using roles and rules as prescriptive system design elements is problematic; 2) design for coordinate work is needed; and 3) proposals to accommodate for different competencies must be made.

Where smart technologies prevent communal use from evolving dynamically, they are perceived as problematic. Designers need to take into account the social nature of roles and rules as different from their counterparts in system design.

6.5.1.3 Modes of Action



Section 6.2.2 considered agency and action as means to self, proxy, and/or collective ends. These different modes of action inevitably lead to consideration of goal conflicts and their resolution which is the nexus of self-regulation.

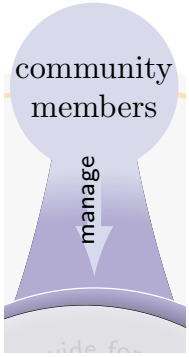
The framework highlights implications for research based on a foundational understanding of social psychology discussed above. We postulate that most actions as part of communal use pertain to proxy and/or collective goals. Through ongoing social negotiations, members work to align their understanding of collective goals with that of others. After all, acting in the interest of the community contributes to a stronger feeling of belonging and a sense of 'ontological security' [148].

This coordination of goals benefits the work of proxies. However, there is little support in technology design for the needs of proxy actions. More research is needed to support proxies in orienting their efforts to social and moral order.

6.5.2 How can communal use be facilitated?

Within this conceptual context, we have identified three ways in which intervention and innovation can facilitate communal use: (1) communal use must be managed by community members; (2) communal use must be enabled by smart technology; and (3) information must be embodied in smart technology.

6.5.2.1 *Managing* communal use

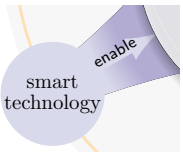


Community members need to be supported in their management of communal use. 'Managing' refers to a broad array of possible actions and interactions between community members. In managing their everyday life, they reflexively establish social organisation and moral order (see above and Section 5) by acting according to the different modes within the social organisation of the home.

When acting, community members bring their self and personal characteristics (e.g., Chapter 4 and [45]) to the table. By considering how analytic categories pertaining to the 'self' influence actions within the social organisation of the home, we open up a space where a range of phenomena can be explored such as the co-creation and role dynamics of gender identities around technology use in the home [168, 199] or general preferences with regard to agency and independence [197].

Smart technology is appropriated within a web of interpersonal relationships. To manage communal use, community members employ different means and methods (e.g., cohort dependent risk management and gate-keeping in using passwords). Community members manage communal use by concerning themselves with the use of technology and dealing with 'attack surface' on relationships in the digital and social world. They also manage "the accountability of their own and others' actions in the sharing of personal data, and with managing intrusions into everyday life from the online world at large." [145].

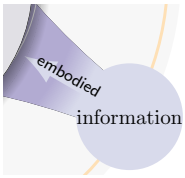
6.5.2.2 *Enabling* communal use



Smart technologies need to enable communal use (see also Section 6.5.3.3). *Enable* captures how smart technologies interplay with the social organisation of the home. Devices need to be appropriated to fit with the needs of a household. In Chapter 5, we have documented ways in which smart technologies match, conflict with, and alter the moral order in the home. For example, features of devices that favour a division of labour are not always welcome (Vignette 5.7). Key components to 'enablement' are perceived use of devices or affordances, which may be individual or co-established within the community.

Designers have long been struggling with providing affordances not only for 'use' but also for 'non-use'. Our framework illustrates how smart technology affects social order. It thereby suggests different ways in which that order is established in and around the use of smart technology (no personal interaction with devices necessary).

6.5.2.3 Information is *Embodied*



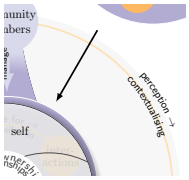
Information needs to be embodied by smart technologies. For devices to become accountable to the social order of a home, they need to provide for appropriate transparency, visibility, intelligibility, and accountability of information. In other words, there is a 'gulf of evaluation' [139] with regard to what community members expect their devices to do with their data and what devices actually do (e.g. [191, 340]). To address this gap, information that is produced and used by smart technologies needs to become embodied. In other words, *information practices* of devices need to become more intelligible and visible through visualisation and articulation (e.g., [46, 341]).

Researchers have recently established Human Data Interaction as a research area that deals with these kind of challenges faced by data-driven societies [342]. They put forward legibility, agency, and negotiability as design goals. To fully realise these goals, new architectures and tools have been proposed, e.g., DataBox or Solid. While these are important research efforts, they will not materialise in time to address societal challenges originating from technology design we are facing today. Appropriate embodiment of information is important for all kinds of products that are being designed.

6.5.3 How can research perspectives contribute to communal use?

There are ongoing research efforts that can contribute towards the establishment of communal use. This section discusses three core concepts that connect community members, smart technologies, and information.

6.5.3.1 Contextualising



A widely observed phenomenon is the context-dependency of 'privacy preferences' regarding data flows (e.g. [5, 103, 213]). However, regardless of whether or not the data source is a physical artefact, an oral account of a conversation, or a digital record, what community members mainly concern about is not data per se but the process of extracting meaning from data and turning it into information (e.g. Jakobi et al. [205]).

Community members orient to "regimes of observability and accountability". They do not only manage how information is understood by others, but also whether this information is meant to be made visible and shared in the first place [166]. What is appropriate to share is governed by a 'calculus of accountability' through which members manage what information is available to whom and when, what is shared, and how it is understood. Crucially, they manage others' orientation to the shared information. Online, community members often lack the appropriate means to guide "what is intended to be achieved by the parties of sharing in situated instances of sharing" [343].

Digitally collected data therefore requires *articulation* "in terms of the social and moral organisation of domestic life" [344]. Given a risk of misinterpretation, it is not possible to "read off" [344] understanding of interactions from data. It is problematic to assume that through collecting more data, the systems will be 'contextually-aware' and able to discriminate meaning of human device interactions. To make data meaningful, systems should support articulation work by users [345].

6.5.3.2 Awareness and Intelligibility

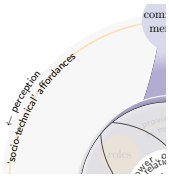
Awareness and intelligibility are concepts frequently debated in HCC. Additionally, researchers draw on the concept 'articulation work' [306] to understand how technology can support members of a setting to coordinate their actions (e.g., [307, 346]). To facilitate communal use, efforts to create awareness and intelligibility of articulation work by design are required.

Information on how exactly 'smart' devices function is not accessible for a vast majority of users. This lack of access has often been attributed to a lack of appropriate affordances [34]. Because control over data is a prevalent concern in

privacy legislation and system design, concepts such as awareness [48, 143, 208] and intelligibility [205] are popular angles of investigation. Relatedly, transparency of data flows [191], user interactions [213, 280], and accountability are often proposed as design goals. A key question is: how exactly can these notions be achieved through flow of appropriate information without creating cognitive overload or 'privacy' issues in multi-user environments?

Given that awareness implies neither understanding nor action, recent research approaches have therefore begun to combine awareness with understanding of and appropriate affordances for action to truly support users [46]. Others have employed End-User-Development approaches to understand information demands [205].

6.5.3.3 Socio-Technical Affordances



Designing socially appropriate controls despite technically limited opportunities is the remit of CSCW [347]. For phenomena such as security and privacy which are deeply social in nature, this brings about the need to reorient design away from analytic concepts to everyday concerns (e.g., Dourish's [227] information practices).

The concept of socio-technical affordances captures the social-embeddedness of interaction with devices. As opposed to 'normal' affordances, socio-technical affordances are possibilities for action and meaning-making. For example, considerations include who acts on behalf of whom and pursuing which goals [348].

Another aspect of these affordances is to provide for coordination and negotiation opportunities so as to facilitate the establishment of moral order in the home. To this end, socio-technical affordances need to enable awareness and intelligibility of smart technology while aiming to contextualise information.

6.6 Discussion

The framework itself constitutes a contribution to privacy research on communal use in HCC. This section therefore discusses the value of the framework in light of existing research and design challenges.

6.6.1 Combining Research Perspectives

In combining an analytic view on human agency with an interactions perspective on the accomplishment of social order in the home, we have joined perspectives from two different sociological research traditions. While they can be conflicting, we have positioned them as complementary as the human agency perspective offers an additional way to instrumentalise our understanding of the social organisation of technology. In constructing analytic concepts and establishing connections between them, we have also placed warranted assumptions with regard to their relationship. We suggest these links can be evaluated in at least two different ways: 1) through empirical investigations; and 2) through their value in informing design exploration and their potential to bring about fruitful discussions in the academic community.

The analytic view of human agency also has its own baggage. As we have pointed out, it is contested across disciplines. While Bandura's theory is widely recognised and well established, more research is needed to deeply explore the relationship between technology use in communities and Social Cognitive Theory. Future research needs to consider limitations of the theory as recent developments in social psychology show. For example, forethought [320] relies on executive functions. Research shows that these are often impaired or delayed based on genetics, biology, and life experiences which can cause irregular development or even brain lesions. Similarly, self-reflection relies on a higher level of thinking that does not develop until around seven to nine years old and also varies with the development of executive functioning, e.g. [349].

6.6.2 Social Goals and Coordination

Divisions in or disagreement over use can be attributed to differences in goals, attitudes, preferences, and other facets of personal identity (e.g., [5, 208, 215, 350]). Our framework illustrates how social negotiation is routinely engaged by community members to address the disagreement. According to Bandura's theory, self-reactive influence involves evaluating intended performances against personal goals and values. When community members adopt self-reflectiveness, they are equipped with the means to negotiate communal goals and coordinate the use of technology at home.

Insights into 'privacy' in communal use—i.e., the various ways in which concerns with relationship management that guide practical action can be coordinated (Chapter 5)—can contribute to the rethinking of the approach to informational privacy and novel design patterns [308]. Researchers have documented how creating awareness of data flows (through embodiment) from the home network to specific companies can provide opportunities for learning and goal alignment in discussion [46]. Such efforts to reorient design toward relationship management with the online world need to be complemented by more local concerns on relationship management mediated by devices in the home.

In the previous chapter, we have already suggested that visibility and awareness can support the establishment of social goals. Here, we add that this establishment needs to take into account different goals and modes of actions. Important questions become how negotiation of social goals can be supported by devices that are mainly used through proxy agency. Exercising proxy agency in this way calls for complementary social action that establishes goals and reports back on perceived success and failures in communication. To address this, designers can implement nudges in their systems.

6.6.3 Roles and Access Control

Roles and rules are not of predictive or generative nature in the home (Chapter 5), but are invoked to articulate expectations. Previous research has shown that access control models are too prescriptive, and thus receive limited uptake in managing access within the home (e.g. [213]).

First, it is important to acknowledge the design politics involved in creating access control models, which are often considered the panacea of security and privacy. Despite research efforts to understand 'user requirements' in the context of smart home (e.g., [216]), decisions to implement specific roles with a specific set of permissions and corresponding rules are made by designers on behalf of users. This way, then, designers' values and goals also become part of their product (e.g., when features of devices can potentially bring up unanticipated and potentially unwelcome divisions of labour between adults (Chapter 5)). Focusing on capabilities (who can do what) during

system design can obfuscate what a role (who does what) in the home is really about, i.e., accomplishing a social order that is local to the home.

One way everyday concerns might inform the design of access control mechanisms is through their goal orientation. We have discussed how goal types and hierarchies influence the impact on intentions. Massacci and Nguyen [351] propose goal-oriented access control for the home. Efforts like these might be better suited for the home, not only in situating needs for exceptional access (e.g., emergencies for ageing populations [351]) but throughout the ongoing use of devices to constantly remind users that their actions should create meaning that aligns with social goals.

6.6.4 Characterising Communities

Proxy-agency and its implications account for a large proportion of community members' interactions with technology in and around the home. Divisions of labour in and across roles indicate that members enact proxy-agency by acting on behalf of a group while aiming to take into account implications of their actions on others. Members acting as proxy-agents need to rely more heavily on their moral agency, foresight, and self-reflectiveness.

It is also important to note that interactions with technology are but one part of all interactions in everyday life in our homes. How this influences the ways in which proxy agency for the management of technology is appropriated has been discussed in the literature: While the influence of individuals on the collective is well known (e.g., as technology support givers [94], privacy or security advisers [295, 301], or 'digital housekeepers' [184]) and researchers frequently advocate for higher degrees of community collective efficacy (e.g., [41, 217, 297, 327, 329]), the implications of proxy-agency (opportunities and challenges) are under researched [121, 298, 324].

We suggest considering communities as constituted in proxy relationships. This network of proxy relationships is established where members exhibit levels of social efficacy that allow them to enlist others for the purpose of achieving their own goals. Communities are also characterised by collective agency and efficacy beliefs. Either through proxy agency, social efficacy, or coordination of goals, members pool knowledge,

resources, and skills to act in concert to shape future events. Bandura holds that interactive, coordinative, and synergistic dynamics cause group-level properties to emerge, and which are not reducible to individuals [320]. The higher the interdependence, the stronger the collective efficacy beliefs.

6.6.5 Proxy Agents and Teachable Moments

As illustrated in the many divisions of labour in Chapter 5, 'resources and responsibilities' in the home are shared, and community members do not just frequently but also inadvertently relinquish control [320]. Consequently, demands for the support of proxy relationships by design are manifold, e.g., parents caring for kids, adults caring for the elderly, or trusted advisers assisting with configuration and set-up of devices. Perhaps with the exception of parental controls, proxy relationships are not well supported [298, 324, 352]. There is little support for specific tasks, and no support for the coordination and management of activities and goals in communities [217, 327]. As a consequence, proxy action currently requires impersonation of others where establishing the right amount of advice (e.g., good stewardship vs too much paternalism [298]) becomes problematic.

One opportunity that can also be facilitated by technology itself lies in the co-location of actors and activities. In overcoming individual hurdles for technology use, those who enact practices are those who exert efforts to make technology work for the household. If visible to others, these practices can enhance self-efficacy of others. Individuals wishing to learn about a particular device can rely on these strategies. Designers can similarly think of ways to facilitate efficacy building, either for individuals or the collective. Collective-efficacy relies on knowledge of others' abilities. Devices can facilitate and foster these beliefs by providing information or creating visibility of 'differential rights' and related interactions with devices. These efforts can contribute to higher degrees of confidence to cope with devices.

We point to principled ways in which design might create teachable moments. Technology education more broadly (e.g., for children but also adults and elderly) is another area where moral agency and goal alignment is required. To illustrate, one might look at ongoing debates around children and their technology use where different

parenting styles and goals are at play (e.g., parenting styles and their relationship to parental mediation theory [353]).

In principle, design can facilitate proxy action in supporting foresight and self-reflectiveness in a number of ways. Devices can be designed to embody social contextual information (e.g., social goals for use) or to provide talking points for proxy users to elicit such information. Design can further support proxies who act on behalf of the household community by (1) highlighting the need to align their personal goals with community goals; (2) enabling the engineering of solutions for particular problems on behalf of others who then execute them; or (3) allowing proxy users to solve problems on behalf of others. Crucially, each of these steps offers a chance for upskilling and reducing 'vulnerable security' should that be desired.

Lastly, similar considerations hold where *devices* are designed to act as *proxy agents*. Whether and how devices themselves can act with moral agency and become oriented to moral order are important considerations. The insights on teachable moments, goal hierarchies, and alignment are valuable for both, those performing configurations and for the design of appropriate automation in proxy agency.

6.7 Conclusion

This chapter has motivated and documented the creation of a framework for innovation in design and research called 'Communal Privacy in Smart Homes' or CoPriSm. The framework provides structure for the research concepts that contribute to the understanding of communal use, combining interaction-focussed with agentic perspectives. It uniquely positions designers in HCI, particularly user experience designers, to deconstruct design challenges before repacking them for the context of communal use in the home while considering modus operandi for design interventions. Throughout this process, the framework advocates integrating an orientation towards social goals and values of everyday life in human-device-interactions.

The framework is useful in a number of ways: (1) it can facilitate innovation through design thinking, e.g., drawing on 'sensitising concepts' and agentic perspectives to understand modes of operation; (2) it can help designers and researchers in HCI

to understand requirements of new artefacts; and (3) it can also serve as a boundary object [39] that can be used jointly by the disciplines of HCI, system engineering, policy, and law to understand and discuss the intervention space for privacy in the home.

The construction of the framework has also highlighted important ethical considerations of empowerment and design challenges for communal use. For instance, power differentials are inherent features of relationships which will be affected by any intervention. Hence, we recommend articulating design politics while carefully considering future impacts by following an RRI approach.

Following this approach, the next chapter demonstrates the applicability of the framework to empower privacy through innovation in research and design. Drawing on CoPriSm, two case studies demonstrate how new interventions are created to empower households.

7

Case Studies of Empowering Privacy in Communal Use

Contents

7.1 Introduction

The previous chapter has introduced CoPriSm as a conceptual framework and proposed a design thinking approach to empower households' privacy through innovation in research and design. We have anticipated possible outcomes of creating the framework in Section 6.4.2, particularly reflecting on the ways in which CoPriSm might be misused to disempower people. We also have encouraged innovators to practice RRI as means of directing their efforts towards desirable goals.

Returning to the overarching research question, this chapter continues our RRI inspired process to explore how CoPriSm can empower privacy in the connected home in light of the considerations discussed in Section 6.4.2. We present two case studies where the framework is applied. The use of RRI in this chapter is two-fold. First, as researchers and creators of CoPriSm, we *engage* with possible futures the framework might bring about. Second, as designers in HCC, we follow the process of responsible innovation to put forward design proposals for empowering privacy in communal use. We reflect on purposes and intentions based on our considerations of power, empowerment, and responsible innovation in Section 6.2.4. We further anticipate outcomes of our innovations by engaging in a critical review of our case studies which in turn allow us to act by refocussing our efforts.

Insights from the first case study demonstrate opportunities and challenges related to attempts to empower privacy with a focus on designing better systems. While the case study design offers some improvement on existing designs, it also becomes clear that previous concerns around increasing 'vulnerable security' by designing for proxy interactions persist. The study encourages us to redirect research and innovation efforts in our second case study where the question centres on how innovators use the framework to minimise the risk of increasing 'vulnerable security' through proxy agency.

The two case studies explore possible futures for empowering communal use by design in which expectation and relationship management across digital and physical worlds (i.e., exercising anticipatory practice) are foregrounded. The chapter concludes with a broader discussion of implications for research and design for privacy and communal use.

7.2 Designing Responsibly for Communal Use and Privacy

As suggested in Section 6.4.2, there is a need to articulate *politics and conceptualisations of empowerment*. We understand "power as [...] the capacity to empower or transform oneself and others" [27] and "empowerment as a process by which [...] people gain mastery over issues of concern to them" [32]. Our goal is to create equality of opportunity to access resources [31]. Following [24], the design is carried out by non-participatory researchers. The context and motivation are opportunities to facilitate the *organisation of communal use* presented in Section 5.4 through *opportunities for empowerment* discussed in Section 5.5. Finally, it is prudent to use anticipation, reflection, engagement, and action to guide interventions, because outcomes of innovations are difficult to anticipate and power imbalances can be amplified by design as discussed in Section 6.2.4.

There are many different methods and approaches researchers and innovators might use to

> open up visions, purposes, questions, and dilemmas to broad, *collective deliberation* through processes of dialogue, engagement, and debate, inviting and listening to wider perspectives from publics and diverse stakeholders. [332, p. 38]

Within the scope of this thesis, participatory engagement (Chapters 4 and 5) and literature discourse (Chapter 6) served this need. Our engagement with possible futures as part of this thesis is the creation of low-fidelity prototypes and their evaluation in case studies.

In response to Wong and Mulligan's [126] call for designs that 'inform and support privacy' while also exploring people and situations, we create our first artefact—'Two-Getherness | Home Security'—an alternative application for home security that sets centre stage social goals and values. It accommodates for social negotiation and coordination of privacy-related interactions by design. The second artefact similarly seeks to 'inform and support privacy' by leveraging insights into the social organisation of the home to empower 'digital housekeepers'.

While Wong and Mulligan [126] characterise efforts to 'inform and support privacy' as one where a particular notion of privacy is assumed from the outset, our artefacts do not assume a particular conceptualisation of privacy but seek to support

the sociality of members' work in coordinating their use of a device [126]. Because privacy is not oriented to by community members, our efforts are organised around the *management of relationships and expectations* implicated in the communal use of smart technology (see also Section 5.4.4).

7.2.1 Case Study: Two-Getherness | Home Security

Taking inspiration from prior research exploring design for better social accountability and awareness [280, 309], we first aim to design for coordination (or social negotiation) between household members to empower privacy. Our suggestion is to enable members' interactions with a device to become socially accountable through technical mechanisms (design for 'articulation work'). This accountability is essential for other members to gauge whether interactions are naturally accountable to the moral order (i.e., if they are part of an activity coordinated between household members) and what purpose the activity serves.

The use of smart security cameras in and around the home brings about many privacy challenges such as where to position the cameras, how to use the recordings, and what moral or legal considerations are important. Based on the systems used as part of our study in Chapter 5, interviews in Chapter 4, and a review of available products in Section B.8 (see cards with details on cameras), we identify features of smart security cameras listed in Table 7.1 (not all cameras have all features).

Smart security camera manufacturers typically offer their own cloud services that support the services listed above. Consequently, each system requires the installation of a proprietary smart phone app. Manufacturers commonly also offer a web interface with the same functionality as the mobile app. Common features on web interface and mobile app include access to system settings (e.g., user account and cloud subscription), camera registration, management of camera features (e.g., activity zones), connection to third-party services, configuration of schedules and automation processes, and a log of all recorded events including captured videos. Access to these interfaces is typically configured with an administrator account. This administrator can delegate access to other users such as 'friends and family' sharing Arlo cameras.

Table 7.1: Common features[a] of smart security systems

Feature	Description
remote access	via smart phone app and internet connection
power	cameras can be run on battery power and/or plugged into mains power
alarm	an integrated alarm bell to deter burglars
inter-communication	cameras include a microphone and speaker that can be used as inter-communication device
recording quality	the video recording is captured in at least high definition (HD)
night mode	uses infrared to record in low light conditions
weather resistance	resistant to water and temperature impacts
motion detection	mostly with object detection (human, animal, and other things)
activity zones	notifications are only generated for motions in these zones
storage	recordings are stored in the cloud and/or on a local hard drive (automatically overwritten after 7, 10, or 30 days)
stand-alone	most cameras require connection to a base station while some can be used as stand-alone devices
integration	some systems can integrate with Google Home, Apple HomeKit, and Amazon Alexa
continuous recording	most cameras record on motion detection only; some offer continuous recording

[a] We exclusively reviewed cameras that were marketed as smart home products from major technology companies branching into the home security market and established home security providers.

7.2.1.1 Empathising

We follow the process detailed in 6.4.3 Practising Design Thinking with CoPrism to identify ways in which our framework can inform the design of a smart security camera interface that empowers privacy among the household community. The starting point of our engagement with the framework is *usability issues* discussed below and summarised in Table 7.2.

We begin by drawing out considerations related to the question (Section 6.5.1): How is communal use organised?

Interactions that are desired or might be welcome are not adequately supported by the system. The system *lacks appropriate levels of access* for all users, particularly where social competence is questioned: Household 1 used the security system to overlook

Table 7.2: Overview of vignettes related to smart cameras in Chapter 5

Reference	Summary
Household 1	
Vignette 5.6	Rosa gets access delegated from Jaco and renames cameras; she assumes a secondary role
Vignette 5.9	Jaco reviews recordings at night time
Vignette 5.14	Iria will not get access as she might delete videos
Vignette 5.11.2	neighbours are happy and keep asking if Jaco keeps checking the feed
Household 4	
Vignette 5.7	cannot adjust camera activity zones on Carla's phone though she wants to
Household 6	
Vignette 5.16	Tobias shares a link to access cat camera with his mum, of which Sylvie disapproves

the outside of their home, particularly areas where vandalism had occurred previously. The parents established use between themselves, with the mother assuming a "secondary role" to her husband. The father involved his sons in reviewing the video logs, and the mother shared a video recording with their teenage daughter. The daughter Iria was, however, interested in accessing the video feed herself, leading her mother to assume she might want to delete the videos. Ultimately, Iria was not given access. Outside the home, the parents coordinated the use of their system with the neighbours. When the neighbours (members of the same neighbourhood watch) took an interest in the recordings, Jaco reassured them that he intended to inform them right away should something happen to their property. We summarise three main insights: (1) the parents deem 'no available access' mode appropriate for their daughter; (2) Rosa expects her husband to review the videos; and (3) the system is appropriated for the neighbourhood watch through ongoing communication between families.

A system is perceived as problematic where it *places limitations on one's spouse's ability to share tasks* in maintaining the system: In households 2 and 4, the husbands had set up the security system. Their spouses struggled to configure the mobile application on their phones, realising after some time that their husbands had to delegate access. This limitation was not welcome. Furthermore, household 4 realised that some configuration options were limited to the administrator only, and the spouse

(Carla) had to receive shared access through a 'friends and family' function. This was problematic as it prevented Carla from completing a maintenance task she had set out to do. Systems ought not to make assumptions for the social order and relationships values users might have.

Orienting towards a social goal can facilitate an orientation to the moral order of a home, thereby preventing conflict as illustrated in the following incident: Tobias (Household 6) had created a cat camera using a Raspberry Pi and an old webcam. The live video feed was accessible via a web page. However, when Tobias shared the link with his mum, his wife disapproved. She did not want her mother-in-law to see whatever else was going on in the kitchen. This implies that systems should generally provide for better coordination of and adherence to social goals.

7.2.1.2 Defining and Ideating

We guided our efforts following considerations of the questions: 'How can communal use be facilitated?' and 'How can research perspectives contribute to communal use?'. Based on the insights above, communal use of smart security systems can be facilitated through *enablement*. However, we have documented how different smart security systems (self-built and off-the-shelf products) fail to provide appropriate affordances for spouses (e.g., when locking out spouses from administrative/maintenance activities), and the ways in which members can make the system accountable to the community (e.g., by sharing videos with children or talking to neighbours). Additionally, there is a need for better *embodiment* of information that helps members orient to social goals and hold themselves accountable.

Identifying At this point, one might be inclined to identify design goals to be appropriate/flexible access control, transparency of system state, visibility of interactions with the system, and appropriate levels of agency. These goals would be similar to ones identified by, for example, Zeng and Roesner's [213] design exploration of multi-user smart homes or Ur, Jung, and Schechter's [8] study on audit log interfaces for door locks and doorway cameras with parents and teenage children. These two user

studies set out to provide more sophisticated user interfaces that provided more people with more agency to carry out a diverse set of action. However, they reported limited uptake of these features among their users. Ur, Jung, and Schechter [8] have found that "even though we provided participants in our second study options that make monitoring transparent to teens without affecting home security, few participants used these options" [8]. Similarly, Zeng and Roesner [213] have found a dominance of social norms in "healthy", non-abusive households. They posit that these norms "were effective at mitigating multi-user security and privacy issues, sometimes more so than the features we implemented in our prototype" [213].

The authors suggest designing "systems that encourage the development of these norms" [213]. Social norms, as established in local social and moral order, are at the nexus of CoPriSm. We have stipulated that community members are equipped with the means to solve these situations (as they frequently did), and that their ability can be improved if systems and their use are made accountable to the local social and moral order of the home. Our framework has suggested that the coordination of social goals between community members is pivotal and needs to be designed for (see also [215]). We therefore identify the following design goals:

Social goals – support proxy users in establishing social goals to manage systems on behalf of the community

Expectation management – create local accountability to facilitate the management of expectations by providing other users with awareness of system state and state changes

Mindful interaction – encourage intentional use of a system

Realising and Mapping Our framework highlights the importance of socio-technical affordances. As the two studies above suggest, ethical issues around privacy cannot necessarily be addressed by more sophisticated affordances. Individuals generally don't want to be burdened by learning a system but instead rely on others to act in their best interest [320]. In the case of home security systems, adults usually prefer to share control among themselves but not with their children [8]. These observations highlight

the need for innovative solutions to support proxy agency as well as individual agency while adhering to social goals.

Social Goals In Chapter 6, we position social goals and values at the centre of our framework, postulating that moral agency is a process that allows individuals to orient to perceived social goals. Here, we first address the establishment of social goals before turning toward processes to respect social goals.

One system might serve different purposes and thus requires considerations of a number of social goals. For example, the security system might be bought to 'look after the dog', 'protect the home from burglaries', and 'monitor children returning home from school'. All of these social goals need to be articulated and captured as a mission statement, either for the whole system or for specific cameras that are part of it. Establishing these social goals provides guidance and facilitates efforts to make individuals' actions accountable to the local social order.

While these goals might appear in conflict, we trust the household members' ability to manage their relationships within the social and digital worlds. The system, hence, should support relationship management when establishing social goals by displaying a recorded mission statement at the right time (e.g., during set-up or configuration of the home security system) and at the right place (e.g., on its audit screen or configuration pages).

Expectation Management We have noted how the articulation of roles serves to highlight expectations, and how expectations are linked to an established set of 'differential rights' [184]. We have also discussed how rules are often only articulated to highlight moral order when it is breached, and that rules are not just role expectations, and neither are roles defined by a set of rules.

The actual challenge then is managing expectations. Expectations feature prominently in the literature on UX and Interaction Design, i.e., "Gulfs of Evaluation and Gulfs of Execution". Norman [139] defines the gulf of execution as the gap between users' intentions and what the system (technically) enables them to do or the degree to which intended actions are supported (similar to our *enablement*). The gulf of evaluation

is defined as the difficulty in understanding the state of a system and how well that sense-making process of the system state is supported (similar to our *embodiment*). While both of these notions are encapsulated in what we understand as socio-technical affordances, the additional perspective of *managing* communal use of devices is lacking. The gap that requires addressing is one of *intra-community expectation management*. The gulfs of execution and evaluation persist for all users, but mostly for adults as individuals and proxy agents in the case of home security systems.

An additional gulf of (intra-community) expectations describes the challenges individuals face in their best attempt to use and manage systems on behalf of the community. In other words, this gulf of expectations pertains to non-users (those relying on proxies or otherwise) who have little experience with gulfs of evaluation and execution but have to adjust their expectations based on little understanding and awareness. In addition, their understanding and expectations with regard to home security system functionalities and actual performance will be different from those of the proxies who have first-hand experiences with the gulfs of execution and evaluation. This corroborates with prior research on home contexts and tensions over technology use [354]. These expectations are as relevant to the functions of the device itself (affordances) as they are to the instrumentation of devices by proxies (socio-technical affordances).

How can design support the management of expectations? Minimising the gulfs of execution and evaluation is necessary but not sufficient. Expectations are part of an ongoing process of social negotiations, the reflexive establishment of moral order in the home. To make the current state of systems accountable to that order, changes to the state also need to be made accountable. From a cognitive perspective, changes to a system are products of agentic actions. Considered within the triadic reciprocal causation of environment, behaviour, and self, intentions can motivate actions that contribute to outcomes but do not determine them. Proxy agency requires "shared intention and coordination of interdependent plans of action" [320].

If expectations are a product of past actions (as part of the reflexively established moral order), then intentions can enable community members to contextualise their

meaning. Therefore, it seems important that the intentions behind interactions with systems be made visible. Non-users or non-primary users can benefit from awareness of their proxy agent's intentions. To this end, design frameworks such as social translucence [279] or designing for awareness in interactions with shared systems can provide valuable insights [280].

Mindful interaction Cox et al. [355] describe 'mindful' interactions as deliberate and intentional behaviour (c.f. mindfulness as awareness and acceptance [356]), which can be facilitated by design frictions. We can characterise this 'mindful' behaviour as orienting to social goals and moral order.

Mindful interaction can help proxy agents to anticipate expectations of others. We suggest by taking into account a previously communicated social goal, proxies can apply their own moral agency in their anticipation (foresight). One possible strategy to exercise foresight or guide communicative efforts is to use the ontology of contextual integrity to evaluate appropriateness of changes. Iterative applications of the theory could highlight that using a security camera feed to protect the home serves an established social goal whereas 'curtain twitching' (reviewing videos just for entertainment) is not permissible.

Mindful interaction can be complemented by elements of persuasive design such as Fogg's behaviour model [357] can provide further guidance. The model posits that motivation (sensation, anticipation, and social cohesion), ability (e.g.„ time, money, or effort), and trigger (facilitator, spark, or signal) need to converge for a specific behaviour to occur. However, appropriate timing is paramount in triggering behaviours, i.e., users must exert high levels of motivation and ability to perform actions. Naturally, persuasion can be used to increase the likelihood of actions/behaviours or to obstruct certain types of actions and dissuade people from behaving in particular ways[1].

In summary, the question of how this *management* of expectations can be enabled and embodied becomes one of *designing for awareness of intentions*, for mindfulness in interaction, for deliberate and intentional choices. After all, proxy users are most

[1]Fogg's model has been used in usable security research by Das, Dabbish, and Hong [350] to suggest design that encourages collective management of security and privacy.

challenged when they interact with the device. Hence, building this kind of support into the device is a good approach.

7.2.1.3 The Camera Feed

Figures 7.1, 7.2, and 7.3 show the low-fidelity prototype of the smart security application. An interactive version of the prototype is available online[2].

The prototype offers an alternative application for smart security systems with social goals at the centre stage. Three use cases for smart home security are reflected in this prototype: (1) to monitor children, (2) to monitor pets, and (3) to protect the home. While these use cases are common in marketing materials for smart homes, the implementation of companion apps does not provide for the work required to accomplish them (e.g., Arlo or Ring smart phone apps). Our low-fidelity prototype uses the three design goals (social goals and proxies, expectation management, and mindful interaction) to improve on this situation.

Social Goals for Proxy Users Designed under the assumption that a single individual carries out set-up and configuration on behalf of the household, the application creates awareness of relationships with other people from the outset (Figures 7.1a and 7.1b) and throughout the set-up and configuration.

As a first step, the application suggests establishing social goals (and their use cases) for the household, or at least to communicate these social goals to the household afterwards. The necessary configuration step in Figure 7.1f is to establish links between social goals, devices and their features, and individuals affected by or contribute to the social goal. These links encourage active consideration of relationships in the home, with devices, and implicitly between cohabitants.

This process allows proxy users to carefully consider each device's capability and how it might contribute to or hinder a social goal for a particular person. As children grow up, the means by which social goals are achieved might change (as also reflected

[2]https://github.com/markraemer/two-getherness-security

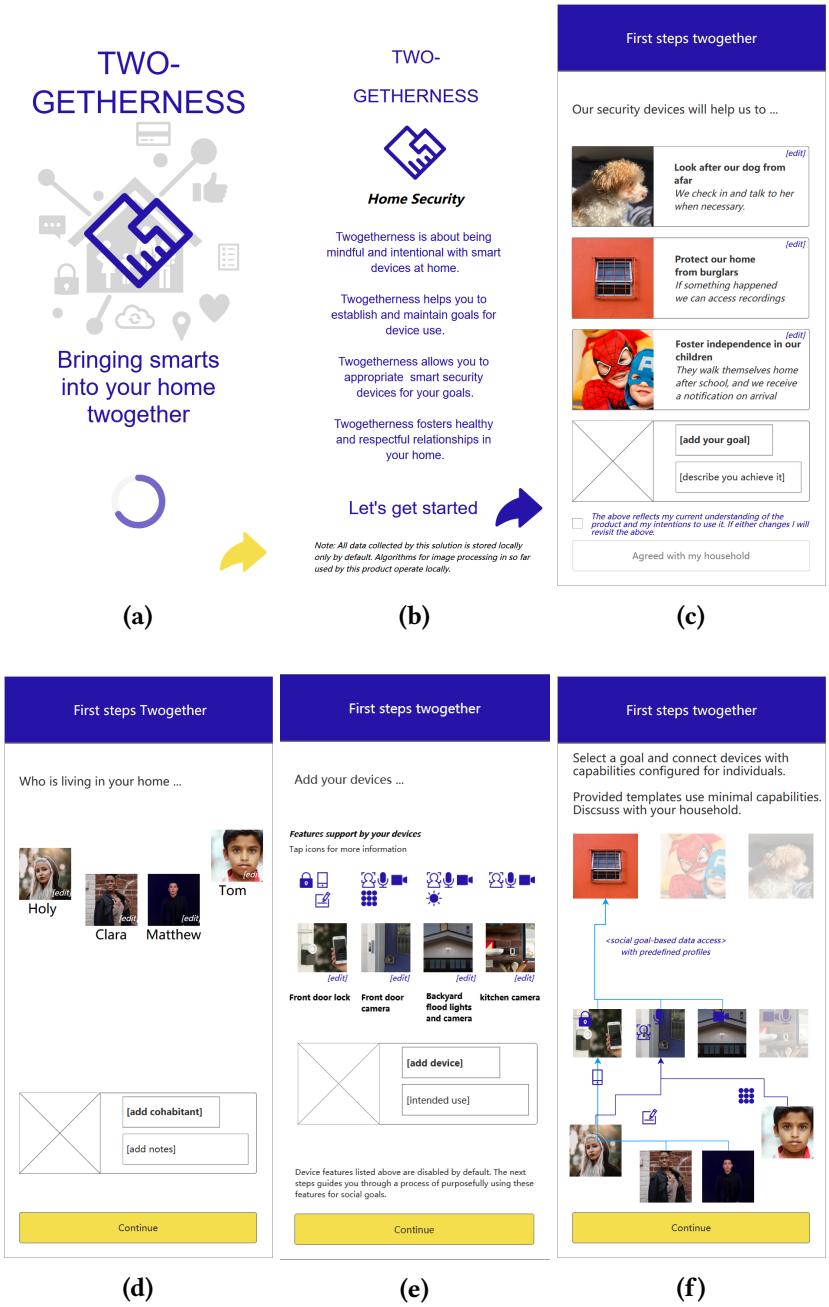


Figure 7.1: A mock-up of the 'Two-Getherness, Home Security' low-fidelity prototype: (a) - (f) show the initial set-up and configuration sequence from (c) establishing social goals/ purposes, to (d) adding inhabitants, to (e) adding devices, to (f) configuring relationships between social goals and inhabitants via devices

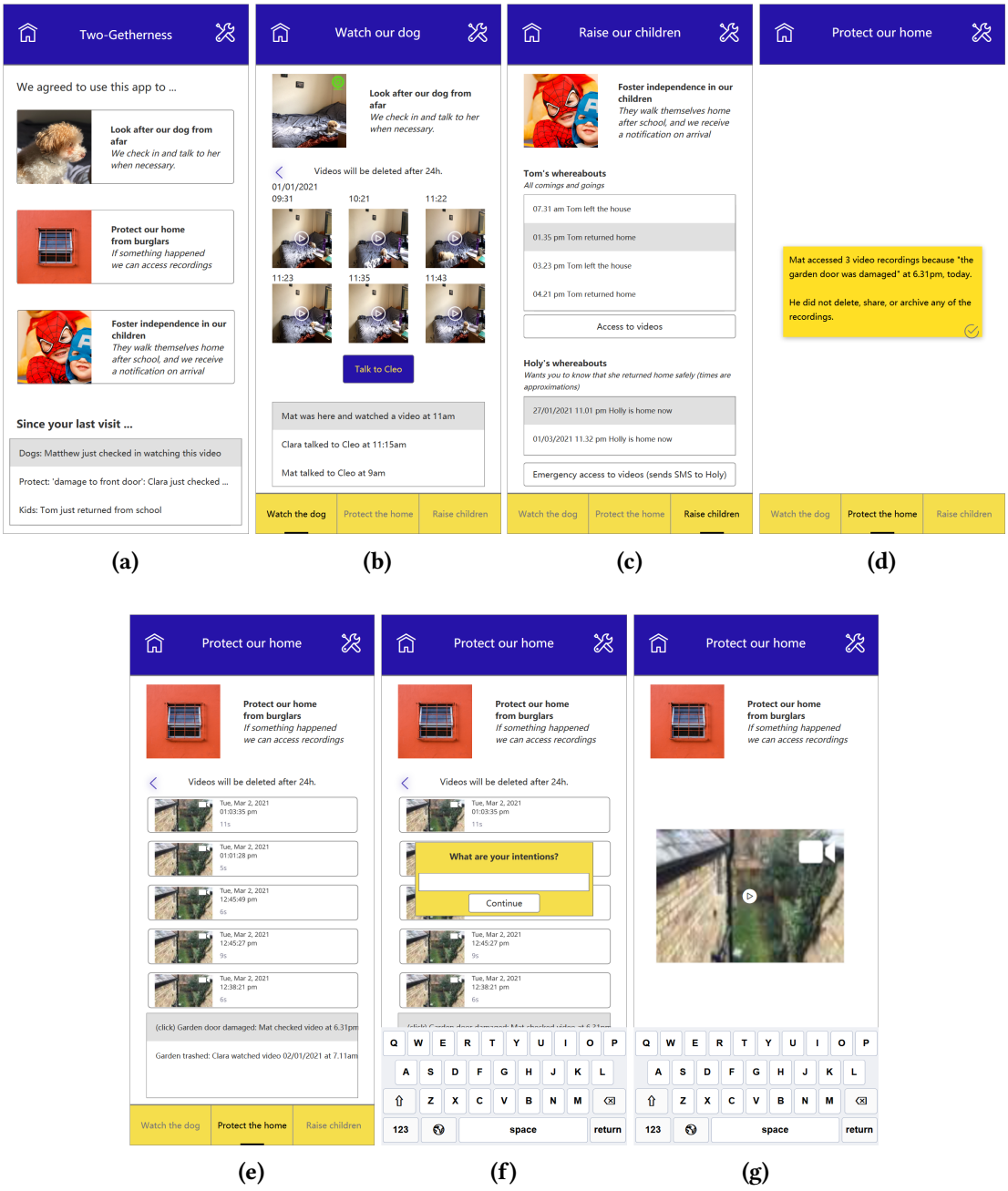


Figure 7.2: A mock-up of the 'Two-Getherness, Home Security' low-fidelity prototype (continued): (a) shows the home screen after initial set-up and configuration; access to devices and recordings is organised after social goals (b) 'looking after the pet', (c) 'good parenting', (d) – (g) 'protecting the home'

in different policies for children of different age (Figure 7.2c)). The application offers the possibility to revise and change configurations appropriately (Figure 7.3b).

Expectation Management A core aspect of the prototype is to facilitate interactions that contribute to communal use in transparent and constructive ways. The ongoing

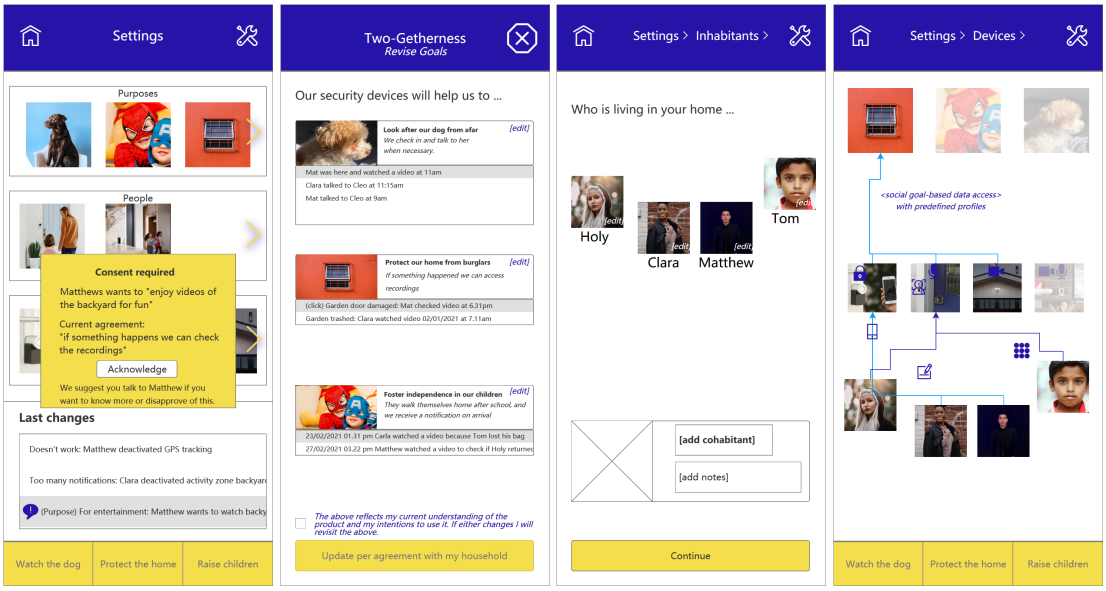
documentation of reasons for accessing privileged content (e.g., Figures 7.2b and 7.2c) and the ongoing creation of meaning by capturing users' intent (e.g., Figure 7.2f). Note that the system is not restricting interaction to agreed and defined patterns, but allows users to routinely redefine the meaning of their actions and how social goals are accomplished by documenting their actions.

Importantly, this information of social goals and intentions behind user interactions is also presented to other users (e.g., Figures 7.2c, 7.2e, or 7.2b). This process facilitates social accountability among users who can manage/adjust their own expectation based on this information and choose to have informed and targeted communication with cohabitants. Note that this kind of information should also be made visible to non-users of the application (e.g., children not having smart phones or adults fully delegating tasks). Integrating this information with products such as Apple's HomeKit especially where households rely on iPads as central home hubs can be one approach. The iPad could be positioned as an easily accessible information source in the home.

Figure 7.3a represents a case of prompting other users. One of the users suggests changing the social goals of using the system to better suit their interest. The prompt sent to other users highlights the need for social negotiation and a revision of the configuration structure in figure 7.3d. The app merely prompts the possibility of conversation as we do not think it sensible to implement such inherently social processes within the application.

Mindful Interaction The application supports mindful, deliberate, and intentional interaction throughout and in a number of ways.

From the outset, individuals are required to agree on social goals. The application supports them in respecting these goals when using the system. For example, in the implemented scenario household members agreed to access the security camera videos only "if something happened". This purpose is repeated at the top of the corresponding video gallery page and recent interactions with any of the recorded videos are documented (Figure 7.2e). This mechanism works through prompts (Figure 7.2f).



(a) **(b)** **(c)** **(d)**

Figure 7.3: Mock-ups of the 'Two-Getherness, Home Security' low-fidelity prototype (continued): (a) application settings main screen, (b) revision of social goals, (c) changing inhabitants registered with the system, and (d) linking social goals with inhabitants via devices and their features are used to serve these goals

Whether and to what extent this kind of doorway monitoring is acceptable to parents and teenage children has been previously explored [8]. Building on some of these insights and ideas, the prototype can be used in a similar manner for monitoring children in figure 7.2c. While the system routinely captures Tom's whereabouts (log only but no video), the daughter Holy's whereabouts are not. However, Holy can use the system to let her parents know she returned home safely.

7.2.2 Evaluation, Anticipation, and Action

We discuss further prototype contingencies to anticipate future impacts. There is no doubt that the prototype can be used to explore features of communities with 'healthy' relationships (as proposed by e.g., [213]). Here, we define 'healthy relationships' as those in which people frequently engage in conversation, look out for each other and exercise moral agency to guide their actions. The prototype fosters mindful interaction (define, revise, and adhere to social goals) and facilitates expectation management in an attempt to reduce the likelihood of disengaging moral agency, e.g., by avoiding diffusion of responsibilities (considering proxy agency) and promoting anticipatory action [321].

Indeed, an important assumption underpinning the prototype is that proxy agents will engage their moral agency in appropriate ways when reminders and opportunities are provided. Moreover, proxy agents will not exploit an increase of vulnerable security that results from acting on behalf of others. Critical questions immediately arise: what if they do *not* engage in moral agency? What if their relationships are 'unhealthy'? What if proxy agents choose to disengage self-sanctioning [321], or what if actors exhibit bad intentions? Little can be done if people truly have malicious intentions. However, we can explore 'more benign' issues such as the amplification of power imbalances in intimate relationships.

Even in 'healthy' relationships, designing for proxy actions means designing around existing power differentials. For example, single individuals may take over installation and configuration, and likely continue to look after the system. Several issues may not be easily addressed. For instance, as a "critical stage" that determines 'what can be done next', configuration can impact usability and undermine the idea of equal access to resources [330]. The first administrator's 'foot in the door' and possible tendency to ignore preferences can amplify power imbalances, not necessarily by design (each administrator has the same capabilities) but by testing boundaries as is common in coercive behaviour [9]. Even information leakage from the logging itself can create challenges in 'healthy' and 'unhealthy' relationships (see our earlier comments on access control and logging for children) [7].

To allow for adaptations in the dynamically changing nature of social relationships, we use goal-based access control models in combination with adaptive access control and monitoring features for children. We concede, however, that this practice is not fully aligned with our previous calls to wholly reconsider the nature of access control models. Besides, using any access control model which relies on a trusted root anchor (here, the first administrator) is consistent with neither our conceptualisations of power and empowerment nor our aim to create equal opportunity to access resources. However, this case study delivers on its goal to explore goal orientation, mindfulness, and relationship/expectation management as design angles. Through its orientation to social goals and everyday concerns, it recognises privacy in intimate relationships

"as a balance among multiple interests and values" [7, p. 7]. It is also an exercise in responsible innovation allowing us to anticipate the issues discussed in this section. Clearly, more research is needed. While efforts to rethink underlying paradigms of security and access control are already underway (e.g., [7, 23, 330]), we still hope to see further proposals for "genuinely multi-user" systems [7].

If issues of proxy agency and challenges of access control persist (for now), is there another way to empower communal use by design? How can we *act* on the insights from this case study? We explore further design opportunities to empower households in our second case study.

7.2.3 Case Study: Responsible Digital Housekeeping

If we struggle to readily address all challenges of communal use and privacy by design, then it is necessary that we explore alternative and complementary solutions that can support households to keep 'healthy' relationships with regard to technology use. The second artefact aims to provide 'household administrators' with a guidebook that helps them become 'more responsible' in their actions. Building on the considerations from the previous section, we are motivated by prior research which has reported the emergence of individual gatekeepers [205] or outsized agency of those setting up devices [5]. Some studies have argued that a particular burden rests on the more technological apt users [18, 295, 298].

Here, we draw on our framework and the empirical data presented in Chapter 5 to design an intervention with the goal to empower those who carry out digital housekeeping and/or frequently act as proxies in and around their household communities.

7.2.3.1 Empathising

To better support digital housekeeping, we stipulate that both the individuals doing the housekeeping as well as their community can benefit from improved means of support. Our starting point, hence, is to create a new design intervention that is goal driven (see Table 6.4).

We summarise our insights discussed in Section 6.6 as follows: Based on the division of labour in the home, a set of 'differential rights' for different roles implied expectations of these rights be exercised when necessary [184]. In Chapter 5, we could see how these rights and expectations included considerations of making devices work for the neighbourhood (Vignette 5.17) and that the neighbours sought reassurance of staying informed (Vignette 5.11.1). Exercising these rights, community members aim to orient to other routines (and to whatever else is going on) in the home, thereby orienting to moral order. Taking the perspective of human agency, they exercise moral agency by regulating their actions to comply with their own goals, values, and standards of behaviour they consider appropriate.

Those who frequently carry out digital housekeeping tasks then become responsible for their well-functioning in that they will be expected and approached to deal with any problems should they occur. It is also the task of such individuals to not only make devices work for the community but also anticipate and avoid 'negative effects' through anticipatory efforts. The 'responsibility' of digital housekeeping can be characterised as a set of actions to which members oriented in three ways: (1) 'taking on responsibility' as in making oneself answerable and admitting to a social obligation to care for others (e.g., reviewing security camera footage regularly to protect the household); (2) 'being considered responsible' as in being considered liable in the legal sense (e.g., for the camera above the front door); and (3) 'acting responsibly' as in exercising moral agency, showing care, and being responsive to any issues (e.g., showing the competence to adhere to social goals when accessing the camera feed).

Therefore, we identify 'making devices work for the household' and 'being responsible' in the ways described in the previous paragraph as broad social goals that underpin the activities of digital housekeeping. The task of digital housekeeping is occasioned not only when new devices require set-up, but also when existing devices need maintenance, or other community members face issues and require support. We also acknowledge that this activity requires a very high degree of care and caution. There is a current lack of adequate resources and support available for smart technologies design that can better accommodate digital housekeeping.

Notwithstanding the above, the previous case study suggests achieving these social goals should not solely be the task of 'the person setting up a device' or 'doing digital housekeeping' but should involve all household members to reduce vulnerable security. Instead, we ought to ask how we can address the challenges related to proxy agents.

These challenges are related to all household members having equal access to opportunities and resources [32, 330] as well as their knowledge of a system's affordances and ability to use them ('knowing what can be done next'). Other challenges are grounded in how the system is used to test out boundaries. Common among these challenges is the use of the system itself. If we struggle to address them within the system, pre-empting the cause by exploring options to complement the system may be a better alternative to trying to 'patch' the symptoms.

7.2.3.2 Defining and Ideating

This section follows the process detailed in Figure 6.4. After several iterations of defining and ideating, we arrived at a set of design goals which map with our intervention perspectives as discussed below.

Identifying The problems and challenges our participants encountered (e.g., an unwelcome discovery of a camera placement in Chapter 4) illsturate that managing relationships and expectations is more effective when it is approached proactively. As Venkatesh [176] suggests, it is difficult for anyone to accurately anticipate how users appropriate their products. Furthermore, proxy-users acting on behalf of others are limited in their ability to anticipate the needs of other community members. Because not all issues can be readily anticipated, it seems generally more prudent to prevent problems than to try to fix them. Digital housekeepers should be proactive, not reactive, in their work.

Notions of responsibility as liability, accountability, or blame are knowledge based and retrospectively applied, as Owen et al. [332] discuss, introducing their framework for responsible innovation. It therefore seems imprudent to represent our characterisation of responsibility as 'taking on responsibility', 'being considered

responsible', and 'acting responsibly' using analytic conceptualisation of social, legal, and moral responsibility. Such representation would suggest a reactive stance for digital housekeepers.

Instead, we take RRI's definition of parental responsibility as care and responsiveness for the rest of the chapter to inform the design goals for our artefact. This prospective view of responsibility encourages individuals and groups to agree on 'what they care about' by reflecting on purposes and articulating goals while being responsive to views and knowledge of other individuals and groups [332]. Key to this understanding of responsiveness is a willingness to not only challenge and adapt one's own views and decisions [333] but also deliberate the needs and views of others.

Any individual attempting to manage devices on behalf of the household will soon identify 'upskilling' other household members as an essential part of exercising care and responsiveness to share experiences and form preferences. Empowering other household members in technology-related activities can contribute to reducing power imbalances that are otherwise amplified by 'foot in the door' and 'knowing what to do next' problems. It can equally encourage the household to test out the social boundaries of device use. Households learn to strike a balance between privacy and "other interests and values" [7, p. 7].

Design Goals As documented in Chapters 4 and 5, technology use in the home is an essential part of social relationships. Our framework underlines the importance of roles and moral order which we frame in terms of responsibilities for digital housekeeping above. We derive a set of goals for 'Responsible Digital Housekeeping' from our observations. These goals are best approached with the help of other community members, particularly other adults as called for in the literature [45] and suggested in Section 6.6.

The following design goals are concerned with fostering management of relationships around the use of devices within the digital and social worlds. This is achieved by establishing social accountability for the use of smart technologies.

Understand Expectations – Understand which community members become involved in or affected by the use of a smart technology and how to identify and manage their expectations.

Negotiate and Respect Social Goals – Highlight importance of and opportunities for negotiation of social goals related to the use of smart devices.

Facilitate Relationship Management – Discuss what relationship-relevant information smart technologies are collecting and distributing to co-establish purpose and meaning of that information (e.g., through periodical joint-reviews of voice assistant logs).

Empower Community Members – Understand the implications of assuming digital housekeeping responsibility for other household members, i.e., *vulnerable security*.

Fostering Responsiveness and Responsibility – Offer help and approachable point of contact to foster social efficacy in others wishing to address issues by digital housekeepers.

Realising We briefly discuss the design goals to draw out details for our handbook.

Understanding Expectations Because every individual in the home will have a different idea of what a device can do and how it could be used to its maximum capacity (e.g., [197]). For instance, an open conversation within the household community might be best suited to understand everyone's perspective on a device purchase. The conversation might include establishing a common understanding of what a device does, how it works, and how it can be used.

Negotiating Social Goals Expectation might closely correspond with personal goals (e.g., entertainment). As our framework suggests, the negotiation of social goals is essential for the use of a device. Social goals allow community members to orient their actions to a shared cause (e.g., protecting the home or shielding children from the online world).

Key to establishing these social goals is an understanding of the device's features, and how these features can be appropriated towards achieving different possible goals. The digital housekeeper needs to lead this cognitive effort via the exchange of knowledge to establish a shared understanding of what constitutes 'use' for a purpose, and how that 'use' is realised with specific affordances of a smart technology. This enables community members to hold each other accountable for their use. Whether this exchange takes place in discussion, through trial and error, or by other means, we suggest keeping a single purpose in mind.

Respecting Social Goals Once agreed, social goals need to be respected and adhered to by all community members. This is not easy as smart technologies employ tactics to engage more with their users over time (e.g., 'foot-in-the-door' [200]) as frequently evident in individuals finding entertainment as a secondary purpose [48]. Where use for other purposes becomes desirable, the additional or new purpose would need to be negotiated within the community. This will allow individuals to reorient their actions, reflexively re-establishing moral order. After all, most actions are carried out on behalf of the community (proxy-agency).

Facilitating Relationship Management Firstly, digital housekeepers need to recognise that their decision over privacy choice controls affect not just themselves but also other community members. We are not suggesting to discuss these settings with all others, but to exercise care and foresight (parental responsibility) in full consideration of other community members.

Another task for digital housekeepers is to carry out relationship management actively. Many smart technologies offer access to device logs or other means of visualising collected data. It is beneficial to demonstrate these logs and visualisations to other household members for at least two reasons: (1) community members are able to create meaning from data, turning it into information (juxtaposed with oral accounts to contextualise it); and (2) community members can manage their relationships across the digital and social world at home (calculus of accountability).

Empowering Community Members Relationship management in the digital world just as much as in the social world requires specific competences, and these competences are typically not expected from children. We saw how Household 1 in Chapter 5 did not grant camera feed access to their daughter. However, we saw how the mother in Household 3 took the opportunity to teach her daughter about relationship management when both jointly set up their Google Home device. We conclude that it is important to establish and cultivate relationship management competence, and that device set-up processes present such opportunities.

Opportunities to empower others are also presented whenever problems with specific technologies occur (Section 6.6.5). As we suggested above, community members can engage others in various ways that enhance their self-efficacy such as creating experiences for others to succeed, asking others to observe how one succeeds, encourage and support others in their efforts, and finally create an environment that is conducive for others to succeed (e.g., manage expectations and create a relaxed atmosphere). This can be done at any point during the process from problem analysis to solution engineering to execution.

Fostering Responsiveness and Responsibility Most importantly, digital housekeepers should foster communication around the use of devices, including being open to assist others in carrying out tasks or clarifying questions. In order for people to exercise proxy agency through the digital housekeeper, it is important that a sense of social efficacy be fostered. Without this engagement, individual efforts may not culminate in collectively shared social goals.

Fostering social efficacy can also be improved by actively engaging others (e.g., asking for their feedback and satisfaction in using particular devices). Proactive digital housekeepers will be more successful in the long term, reducing possibility of disagreements before conflicts arise. Crucially, feedback of community members needs to be taken seriously and translated into action in transparent ways.

Mapping Empowering users can be achieved in several ways from technology enablement to relationship management to embodiment of information. We have discussed the issues of responsible digital housekeeping as inherently social, arguing that what we want to achieve is best facilitated by communication and relationship management rather than purely technology intervention (enablement). Of course, facilitators and features of responsible digital housekeeping can still be built into smart technologies (e.g., as part of set-up guides for central smart home administration apps such as Google Home, Apple HomeKit, or Samsung Smart Things). Social influence and nudges by design are indeed a frequently proposed approach towards fostering better security and privacy in communities [348]. For example, when setting up devices, installation guides can mention the need to involve family members [213].

As part of this thesis, however, we decided against using a smart phone application as delivery mechanism. Our reasons are threefold. Within smart home administration apps these insights might only become visible to those using them, the digital housekeepers. While these people are our audience, we also believe other household members can benefit from appreciating the work digital housekeepers do by providing more support or helping them improve the efficiency of their practice. Not least because proxy agency can also increase vulnerable security, it is key for other household members to understand and reflect on the use of technology by digital househkeepers that happens on their behalf. While we aim to liaise with industry stakeholders to raise awareness among product designers in the near future, such engagement is beyond the scope of this thesis.

Instead, we opt to raise awareness among householders through information dissemination in print and online media. Print media can be packaged with existing products that serve as bridges or central hubs for smart home set-ups (e.g., the Apple TV for their HomeKit). Alternatively, these leaflets can be placed close to smart home products in retail stores to better target our audience. In terms of online media, our findings are disseminated on our research group web page.

7.2.3.3 The Handbook

The final product of our design efforts is presented in Figure 7.4 (an interactive version is available online)[3]. The handbook is designed around the principles of empathising and raising awareness ('10 Facts on...'), establishing engagement and setting goals ('Make Things Run Smoothly' and 'Your Personal Goals'), and finally putting into action ('Take Action!'). In designing the artefact, we took inspiration from a Customer Journey Map which is often used to map users' engagement with different parts of the company. We similarly thought to link interactions with goals (Figure 7.4). Although the three personal goals (i.e., expectations, purpose, and empowerment) are linked to set-up & configuration and use, management of expectations and discussions around purpose may take place before a device is purchased. While we could have included considerations around purchase on page five (Figure 7.4), we did not want to imply that our recommendations only apply to new devices.

7.2.4 Evaluation, Anticipation, and Action

This case study took CoPriSm's *manage* perspective towards empowering communal use. That is, by helping housekeepers to (1) act responsibly, and to (2) empower other household members to participate in communal use. Its main goal for empowerment was therefore to create awareness, sensitivity, and guidance. We believe the handbook delivers on this promise by highlighting opportunities for empowerment to increase others' self-efficacy and by offering this knowledge to all household members that can get hold of the leaflet. Given that technical knowledge is not necessarily required, the leaflet is a starting point for discussion and conversation among household members. When all household members participate and become more sensitised to the challenges and opportunities of communal use, the level of 'vulnerable security' criticised in the first case study might be reduced.

The leaflet's value depends on which interactions are enabled by the technology. While it cannot address issues that are ingrained in 'bad' implementations, e.g., features that might rather amplify than rebalance existing power differentials in interpersonal

[3]https://github.com/markraemer/responsible-digital-housekeeping

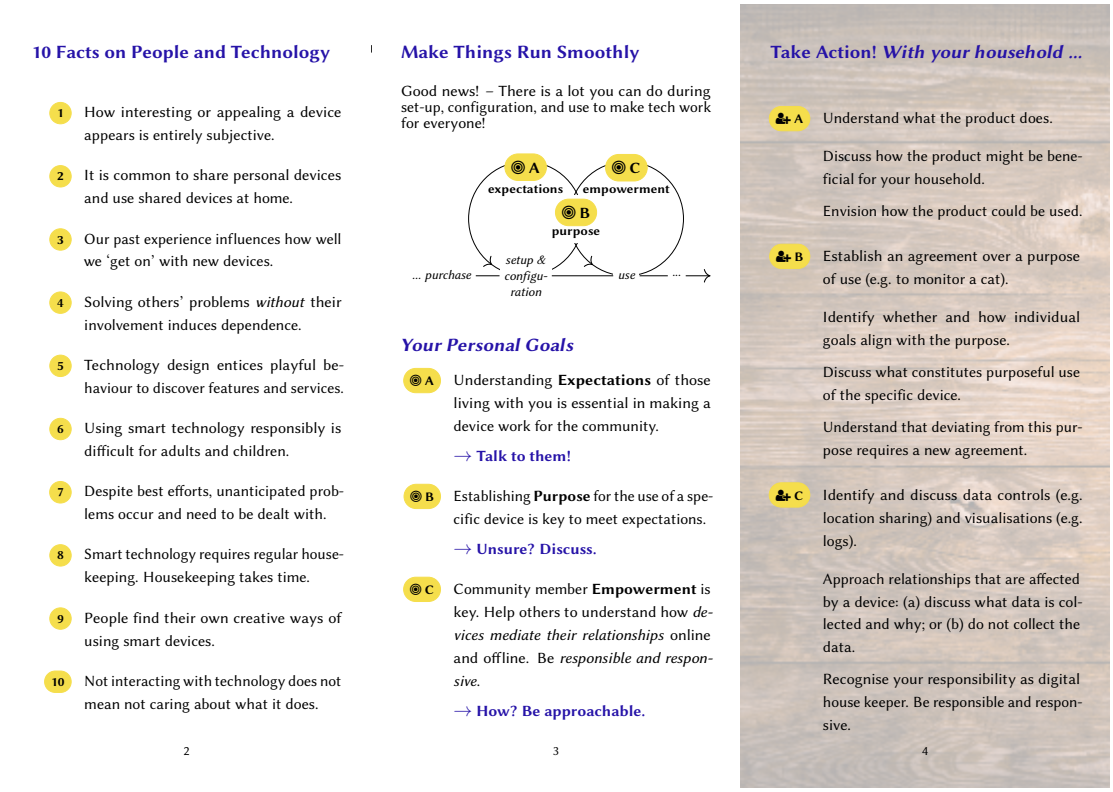


Figure 7.4: The handbook for Responsible Digital Housekeeping

relationships, it can complement good design to make it even more so acceptable for the community of users.

Overall, we argue to keep pursuing design ideas with proxy agency while exploring effects on interpersonal relationships. New design paradigms and approaches are always going to change household power dynamics, hopefully creating equality in access to opportunities and resources. However, it is in the nature of domestic life where tasks are shared and distributed in dynamic ways. The power dynamics of communal use remain unpredictable as discussed in the previous and in this chapter. Because power dynamics are an inherent feature of communal use, we encourage others to also use an RRI framed case study exploration.

7.3 Discussion

This section continues the discussion of communal use and privacy touching on the power imbalances that motivated this work. It also broadens the view to related considerations.

7.3.1 Foresight and Care to Address Privacy Issues

Taking into account all three perspectives (*manage*, *embody*, and *enable*), we proposed Two-Getherness as home security application. Instead of being technology-centred, our prototype used social goals and facilitated the management of relationships throughout set-up and configuration. Informed by our framework, the prototype enabled the work of proxy users. One of its core features was to support the management of expectations with the community while encouraging mindful technology use. However, protection against coercive or even abusive behaviours was limited with the prototype as proxy agency could increase vulnerable security.

The 'Responsible Digital Housekeeping' handbook was designed to reduce vulnerable security by raising awareness on issues of communal use and providing guidance for 'digital housekeepers' in empowering their cohabitants. The handbook was deliberately proposed as leaflet that could be added to any product and made available as separate source of information. With our considerations firmly grounded

in responsibility as responsiveness and care from RRI, the medium served the goal of empowering people by providing all household members with information that can enable them to understand and participate in communal use.

The Two-Getherness app in Section 7.2.1 and Responsible Digital Housekeeping handbook in Section 7.2.3 enable purpose orientation and social goal adherence. They show how manufacturers can use the framework to focus their design efforts. The artefacts also show how the perspective of parental responsibility provides important insights into foresight and moral agency in communal use. Parental responsibility overcomes the shortcomings of the 'data-before-market approach' by advocating responsible and precautionary anticipation of possible futures (i.e., ways in which a product might be used). Individuals are challenged to exercise foresight and care with regard to the needs of other users, the product, and the environment. From a design perspective, the Two-Getherness case study suggested and illustrated how designing for mindful interactions (deliberate and intentional) can be conducive to individuals' ability to exercise appropriate foresight.

Exercising appropriate foresight to manage relationships and expectations remains a challenging task for at least two reasons: (1) general purpose devices (e.g., mobile phones) must support a multitude of use cases by design, and 'purpose oriented' devices (e.g., security cameras) invite 're-purposing' [7, 8, 48]; and (2) data collection and processing practices of devices are attended to by single individuals (often by design) but affect other users and non-users alike (e.g., Chapter 5, [5]). Grounded in the understanding that a socially agreed-on purpose is more acceptable to the community of users, the 'Two-Getherness' case study suggests a possible solution that can address the first issue (purposeful design and purpose-oriented user experience). We encourage future research to use this angle and the prototype to explore features of 'healthy' relationships, heeding the call of [213].

Another important consideration for 'healthy' relationships and power differentials is their socio-cultural context. Earlier, we drew on our empirical observations to loosely define "'healthy relationships' as those in which people frequently engage in conversation and look out for each other" (Section 7.2.2). However, as demonstrated in

the following quotes, this definition of 'healthy relationships' is grounded in a specific socio-cultural background and thus may vary from one cultural context to another:

> Subjective culture may be defined as shared beliefs, attitudes, norms, roles, and values found among speakers of a particular language who live during the same historical period in a specified geographic region. [358, p. 6]

This is an important point to acknowledge because modern technologies transcend cultures whereas design, as we have argued and demonstrated, is inherently political and thereby specific to cultural considerations. Notions of power and empowerment used in this thesis stem from a Western humanistic tradition and may be conceptualised differently in other cultures. For example, the previously discussed gender performances of technology use are highly culturally dependent (e.g., [359]) and change over time (e.g., [170, 171]). While this does not necessarily curtail the significance of our findings in Chapter 4 and Chapter 5 (see also Crabtree, Tolmie, and Knight's [145] study the UK and France), considerations of goals, values and the politics of empowerment may nevertheless carry some form of cultural baggage. Hence, we again encourage researchers, and particularly designers, to follow our example of using CoPriSm as part of an RRI approach which we motivated in Chapter 6 and demonstrated in Chapter 7.

7.3.2 Building Bridges between Companies and Users

The second issue is rooted in the concept of 'notice and consent' which requires users to make situated or a priori decisions over the use of their data for a specific technical feature. Our study showed that technical data protection measures were rarely oriented to by the community of users (Section 5.5.4). 'Notice and consent' frameworks serve not only the documentation requirements of the GDPR but also 'purpose limitation'. This second principle requires companies to disclose details of their data collection and processing practices with regard to a purpose:

> 1. Personal data shall be:
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. (Article 5(1)(b) GDPR [63])

Designers describe data collection and processing needs of a technical feature as purpose. The accomplishment of communal use is, inherently social, however. Device use is a vital component of social and moral order. There is then a disconnect between data protection regulations and everyday practices, i.e., a disconnect of the values data protection regulations want to protect and the ways in which these values manifest in everyday use.

Companies ought to respect users' privacy, while everyday practices reflect an orientation to privacy in terms of mundane concerns that we can relate to social goals. Our case studies show that users can be encouraged to be more deliberate and mindful when interacting with devices by taking into account the users' intentions with regard to social goals. Capturing users' purposes and social goals offers insights into the way they appropriate their products to the social and moral order of the home. Usually, manufacturers have little information on the ways in which users actually use their products, and we suggest sharing this kind of information can be mutually beneficial.

Manufacturers are required to disclose the purposes of data collection and processing such that they can be "in line with the reasonable expectations of the individuals concerned" [40]. If complemented by perspectives that allow for better alignment of purposes and goals in households, these reasonable expectations may represent concerns of the whole household. Secondly, social goals and purposes show how users appropriate products and provide insights into their reasonable expectations. For example, the use of a voice assistant for homeschooling children renders the use of data for advertising unwelcome because it does not align with the social goals of education. However, content recommendation for better schooling materials might very well be appreciated.

Essentially, we are suggesting to apply Nissenbaum's *moral legitimacy* to avoid 'function creep' which is "fundamental in building public trust" [40] (see also [48]). However, the GDPR's 'purpose limitation' principle allows manufacturers to use collected data for other purposes insofar as "the new purpose is compatible with the original purpose"; consent for the new purpose is obtained; or the provision of the new service serves public interest [40]. Knowledge of social goals and purposes would allow manufacturers to identify compatible purposes. This provides an argument for including

social goals and purposes in software context representations. In these ways, users can be further empowered to make the management of their data more meaningful to companies (see also [345]). Enriching context with social goals and purposes would articulate "the social and moral organisation of domestic life" [344] which the authors suggest is crucial to understand context of use.

These considerations also become important in light of the Information Commissioner's Office (ICO)'s "*Age appropriate design: a code of practices for online services*" [360]. Although the code itself is not legally binding, it is supported by existing data protection laws, and the ICO reserves the right to hold companies accountable against the standards of the code starting in September 2021. Following Article 3 of the United Nations Convention on the Rights of the Child (UNCRC), the need to keep "children's interest at heart" features prominently in the ICO's 15 principles. While the UNCRC are aware of several trade-offs between the rights of children and other interests, the ICO highlight that it is unlikely "the commercial interests of an organisation will outweigh a child's right to privacy". At the same time, the UNCRC emphasises the role of parents as carers in charge of "protecting and promoting the best interest of the child" [360]. The steps we discussed above can support manufacturers in enabling parents to consider the best interests of their children.

The code also highlights children's privacy rights against their parents and the need for age-appropriate notice and consent frameworks. While parents can give consent on behalf of their children under 13, these children still need to be informed. For children between 13 and 18, appropriate information needs to be included in the decision-making process [361]. Because privacy policies and disclosure of data collection and processing are largely invisible to the community of users, particularly to children, more research on age-appropriate notice and consent frameworks for communal use is needed.

A related issue is the delineation of data protection responsibilities between data holders and data controllers. As Urquhart and Chen [273] argue, there is a need for not only domestic data controllers to demonstrate accountability to cohabitants but also for manufacturers as data controllers to show how they support domestic data controllers in their work. More research is needed to progress towards the proposed improvements

outlined in this thesis. For example, research can uncover ways in which social goals and purposes can be captured by design, and run user testing with the Two-Getherness application as a starting point. We further suggest discussing and use the CoPriSm Design Thinking approach with designers of smart home products.

7.3.3 Managing Relationships among Household Members

Chapter 6 and 7 explored challenges that account for power differentials in interpersonal relationships. Here, we summarise our efforts to highlight further implications for future research.

Privacy has long been conceptualised with emphasis on an individualistic perspective, such as a right to be let alone, a right to self-determination, or protection from interference (Section 2.2). Our account of interactions with a focus on social goals shared between household members might be criticised for neglecting such issues. However, we would like to highlight that violations to freedom, autonomy, right to be let alone, and other societal values commonly attributed to the concept of privacy also originate in 'healthy' environments and do not appear malicious. In our case, it could be the case that they were either unreported, downplayed, or just did not occur for our participants. With regard to intimate relationships, Levy and Schneier [7] point out that violations (e.g., surveillance of household members) can be circumstantial, unsolicited, and remain unknown to the disadvantaged party. We side with the authors' statement:

> we ought to be agnostic as to the nature of the behaviour or content detected, and be fundamentally concerned with how technology may facilitate involuntary information-sharing.

According to Levy and Schneier [7], there are multiple motivations for intimate threats; (1) co-presence of individuals facilitates device and account access (e.g., shoulder surfing or credential stealing), (2) the use of devices is frequently influenced by "inherently dynamic power differentials backed by implicit or explicit authority"; and (3) rich relational knowledge sources are common intimate threat features [7].

Our work corroborates with the second point. It investigated the ways in which power differentials might originate from the use of devices and contributes insights and

ideas as to how to mitigate them via creating communal experiences. For example, the Two-Getherness application requires household members to agree on goals, thereby addressing the issues concerning the sharing of devices and accounts, unrestricted access to usage logs of all users, and remote access to video feeds [196].

A key implication articulated in [7] is the "blank slate" problem, or adversarial effects of initial configuration and ongoing change of settings. The authors highlight that dealing with default settings in intimate contexts is challenging due to effects of "performative vulnerability" (i.e., visibility of a large number of changes undermines trust) [362]. The authors in [7] also highlight that prescribing limitations to children right from the outset a product is being set up is usually a source for conflicts [363]. Normalising this kind of discussions through establishing purpose with a community can facilitate how one navigates social negotiation and pre-empt the emergence of privacy issues.

This solution is, of course, only partial in requiring interaction with technology while many might already feel overwhelmed with the amount of security and privacy configurations they 'ought to' do [9, 196]. However, opting out of the use of devices is not always an option, and divisions of labour in households are very common. Therefore, we again emphasise the importance of CoPriSm to facilitate moral agency and foresight, as illustrated in the creation of the handbook for Responsible Digital Housekeeping.

Unlike the orientation of this thesis, interpersonal perspectives on *informational* privacy have been called for by other researchers who approach understanding privacy as a state so that one can have more or less control over one's data. We argue that these views are unhelpful and sometimes even harmful. They are unhelpful in advancing our understanding of an inherent social phenomenon because they encourage attempts to "graft …privacy onto a system" [22]. Privacy is not something that occurs at specific times but a pervasive feature of how a system is going to be used. The interpersonal perspective falls short of accounting for meaning brought about by interactions. What is problematic is not that a camera can be used to monitor the living room but *why and how* it is used for that purpose. Social goals can capture this meaning. We suggest considering this perspective when addressing questions such as:

> For example, a few questions arise when a user is attempting to access a live feed of an indoor security camera, while another is in the house — *How can users be guided through a set-up process that maximises interpersonal privacy? How can permissions between a user in the house and a remote user be better managed to maximise interpersonal privacy?* [196, author's emphasis]

Nevertheless, important questions remain as to, for example, what exactly the scope for non-adversarial approaches is, and how they should be complemented by adversarial safeguarding (e.g., [330]). Some proposals to address these questions have been made (e.g., a "dual control process [...] for infrequent high value access" that requires two users to agree on specific configuration settings [48], or Facebook's design for relationship breakdowns that offers cascading changes in privacy settings for ex-partners).

7.4 Conclusion

This chapter has documented how we have applied CoPriSm in two case studies: The Responsible Digital Housekeeping handbook as a cross-product intervention, and the Two-Getherness application for smart security systems. Both artefacts have been designed to manage social goals and purposes of technology use. Individuals act on behalf of the household and in consideration of each others' needs. To facilitate these tasks, we introduced the concepts of mindful interaction and parental responsibility. These concepts have guided our design efforts to support users in their establishment of and orientation to social goals and purposes.

The GDPR's 'purpose limitation' principle points to an opportunity to reconnect everyday concerns of privacy with goals of data protection. Once manufacturers are aware that decision-making is coordinated among household members through negotiation of purpose and social goals, and that purposes can be appropriated to limit their use of data, they can capitalise on the opportunity to meet users' 'reasonable expectation' with respect to data use.

The two artefacts have also demonstrated the value of CoPriSm in addressing interpersonal power imbalances. We postulate that normalising social negotiations of device use could help overcome the "blank slate" problem and thus pre-empt emerging

privacy issues. More broadly, CoPriSm allows us to consider privacy as a pervasive phenomenon as opposed to a set of controls that could be grafted onto an existing system. We thereby suggest that the use of common privacy controls (e.g., access control models) be rethought.

We also applied an RRI approach when considering the effects of our designs on ingrained and invisible power dynamics. This process of anticipation, reflection, engagement and action allowed us to highlight the challenges and shortcomings of our design ideas. As an inevitable feature of communal use, proxy agency remains a double edged sword. If not designed carefully, proxy agency can inadvertently affect power balances. Where it is noticable and welcome as described in this chapter, proxy agency can contribute to a better household experience of communal use.

The next and final chapter of this thesis summarises research efforts, outlining contributions and opportunities for future work.

8
Conclusions

Contents

8.1 Introduction

At the beginning of this thesis, we introduced two challenges that characterise privacy in the home: the Kayla doll which was found to 'surveil' children and their families, and adults misappropriating devices for coercive control in the example of the estranged husband. These two examples represent the under-researched areas of informational and interpersonal privacy in the home. Researching everyday interactions along with the social and collaborative use of computing devices in a complex setting of the home

has provided insights that inform our main research question ("How can households living in connected homes be empowered in their privacy?") and are reflected in the sub research questions.

RQ–1 What is the nature of the relationship between internet-connected technology use and privacy in the home?

RQ–2 How does the nature of the relationship between internet-connected technology use in the home and privacy manifest in-situ?

RQ–3 How can the resulting findings inform innovation in research and design for privacy in the home?

This thesis provides an everyday perspective of technology use to empower households in their privacy. By employing this everyday perspective to inform innovation for communal use and privacy in research and design, this thesis has made important contributions to privacy research and design practice in HCC. We first review the goals and findings of this thesis, before moving on to discuss its contributions and to highlight directions for future work. Following a feminist conceptualisation of empowerment as "capacity to empower or transform oneself and others" [27], the thesis' general orientation to empowerment is to reduce instances of power-over while increasing opportunities of power-to. Note that the ethical maxim of empowerment in this thesis is equality of opportunity to access resources [31].

8.2 Review of Research Goals and Findings

This thesis set out to advance the understanding of privacy in the connected home in order to inform future research and design. Based on the literature review in Chapter 2, we devised three research questions to guide our efforts and research approaches in Chapter 3. Findings and insights into each of these research questions are presented in the four subsequent chapters: RQ–1 in Chapter 4; RQ–2 5; and RQ–3 in Chapter 6 and Chapter 7.

8.2.1 What is the nature of the relationship between internet-connected technology use and privacy in the home?

The answers to RQ–1 are presented in Chapter 4. The chapter *explores* the relationship between internet-connected technology use and privacy based on data from 34 semi-structured interviews. A thematic analysis reveals how household members do not usually talk about or orient to privacy but are concerned with more mundane matters of technology use. These concerns suggest that technology use in the home is in fact communal. We present insights into the ways in which it is communal and discuss implications.

In their use of technologies at home, household members orient towards personal characteristics (attitude, aptitude, skills, and abilities). However, decisions to share devices with household members are fundamentally embedded in considerations of managing relationships with these household members. For example, they consider the appropriateness of sharing access to personal devices with spouses. The chapter also shows instances of household members negotiating the use of smart technologies. The social acceptability of anticipated and unanticipated interactions with devices by household members as well as guests and visitors becomes a matter of concern for device owners. Household members are concerned with upholding a moral order in conducting their everyday interaction. Different arrangements of shared technology use reflect qualities of the home as a place where facilities and resources are shared between household members and where relationships are nurtured. The home is therefore a community in its own right [154].

The communal nature of technology use in the home offers important insights for research and design. Since the set-up, administration, and use are arranged for between individuals, it is difficult to define 'the' community of users in the home (e.g., [217, 295, 329]). Contrary to a common perspective in privacy research and system design concerned with user categories (e.g., [143, 208]), we suggest that personal attributes such as being a resident, a mother or father, or a guest might not be as important for regulating access as becoming familiar with the local moral order. Within this moral order, communally used devices technically require management assumed by individuals

who can also hold other users accountable [34, 194]. Device design currently affects communal use in ways that are difficult to anticipate, with encounters between people and technology sometimes being invisible. This presents a challenge where effects of technology on users cause tension between household members [5]. Such tension raises questions of who does/did what with which device and why.

Researching communal use is thus a matter of understanding everyday interactions and the concerns implicated in them. In everyday use, these interactions also contribute to the establishment of moral order. However, the moral economy [154] of a household is not stable but constantly evolving. Therefore, researching communal use requires perspectives that focus on meaning-making in interaction. The research approach in Chapter 5 meets these requirements.

8.2.2 How does the nature of the relationship between internet-connected technology use in the home and privacy manifest in-situ?

To address RQ–2, Chapter 5 *unpacks* the 'on-the-ground' relationship between technology use and internet-connected technology. The chapter reports on a six-month ethnographic diary and interview study documenting six households' experience with smart devices. During the first phase of the study ('acquainting'), a smart home planning workshop was conducted to identify smart devices, which were later deployed in the second phase ('experiencing'). Field notes, interview transcripts, and diary entries were analysed using our grounded analysis approach with sensitising concepts from EM.

The analysis highlights the organisation of communal use across a division of labour as manifested in interactions with devices and between household members. These interactions reflect a broad array of household members' everyday concerns, such as being a good parent, safe-guarding children, or protecting the home. However, conceptualisations of privacy are not explicitly oriented to but implicated in the values and social goals that support everyday concerns. Through everyday interactions, roles are constituted and related to rules. Household members can invoke either of these concepts to highlight their expectations with regard to social and moral order: when

roles are articulated, expectations of use with regard to specific social goals and purposes are highlighted [302]; and when rules are invoked, then they illustrate aspects of the moral order that are meant to provide meaning for specific interactions [188, 303, 305]. Drawing these insights together, we present the framework of the social organisation of communal use where the relationships between moral order (social goals, values, and everyday concerns) and interactions, roles, and rules are described.

In reporting these findings, we also illustrate the ways in which challenges of communal use are related to the nature of devices themselves. Devices are considered problematic where their features fail to accommodate for the fluidity of roles in the home (e.g., devices that only offer one administrator account). This example illustrates an unanticipated and unwelcome power imbalance between household members. However, device limitations can be socially navigated within 'non-adversarial' households [213]. Where alternative models of access control are infeasible, more support for this kind of social navigation and negotiation is required.

The organisation of communal use offers important insights for research and design. It suggests designers can do more in supporting social negotiations in interactions with devices. These devices can be more easily and transparently incorporated into the social order in the home. Within the fields of CSCW and HCI, frameworks for 'articulation work', awareness, transparency, translucence, and accountability offer starting points [279, 280, 306]. We suggest that facilitating social negotiation by design can result in more purposeful use of access control models in 'non-adversarial' homes [213].

The division of labour during set-up and configuration provides opportunities for research and design interventions. While the division may further complicate existing problems with informational privacy measures related to notice and consent (e.g., individuals needing to account for others' preferences; privacy preferences in set-up guides not being accounted for; and a lack of social or technical means to make privacy decisions accountable to the community of users), household members' everyday concerns (e.g., being a good neighbour) offer an opportunity for research and design to rethink device use. We suggest future research may reconcile social goals and values with purposes of device use because 'purpose limitation' as a principle is a crucial

aspect of consent under the GDPR. Another opportunity within the division of labour pertains to the enablement of users. When single individuals assume tasks on behalf of the household, they can use their privileged position to help others [213]. 'Digital housekeepers' [184, 199] can use their position to elicit and share expectations and experiences so as to facilitate their community to become conversational with devices.

8.2.3 How can the resulting findings inform innovation in research and design for privacy in the home?

With RQ–3 the hitherto focus on exploring and unpacking communal use is broadened to *inform* innovation in research and design (Chapter 6) in order to *empower* privacy (Section 7.3.3). To innovate for privacy in communal use, user experience and system design is needed (see Section 2.3). We aim to empower households through design and innovation following a conceptualisation of empowerment as the "capacity to empower or transform oneself and others" [27] so as to foster equality of opportunity to access resources [31]. However, the outcomes of interventions are difficult to anticipate and possibly problematic, especially where they contribute to coercive or even abusive behaviours. It would be unreasonable to assume that all households are 'non-adversarial' [213]. Therefore, we use the RRI framework to guide our efforts in anticipation, reflection, engagement, and reaction.

Informing In Chapter 6, we apply conceptual framework analysis drawing on empirical data, insights from this thesis, and insights from prior research to create the framework 'CoPriSm'. The chapter presents a design thinking approach to empowering privacy through *informing* innovation in research and design. CoPriSm builds on the conceptualisation of communal use from the previous chapter and supplements the interaction perspective with an agentic perspective. The framework introduces different modes of actions in communal use (self, proxy, and collective) and highlights opportunities for design perspectives to empower communal use: (household) community members manage; smart technologies enable; and information is embodied in interactions of communal use. These interactions in turn contribute to everyday

concerns of privacy within the organisation of communal use. CoPriSm also illustrates how research can sensitise research and design disciplines to the ways in which it is accomplished, thereby contributing to the empowerment of communal use in the home (contextualising information; awareness and intelligibility of data flows and device functionality; socio-techincal affordances for communal use).

These research and design perspectives provide opportunities to empower privacy in communal use. However, this emphasis on using proxy agency to empower communal use needs to consider the nature of power relationships in the home. Power relationships might not be visible but ingrained, and the effects of technology use are often difficult to anticipate. Proxy agency creates 'vulnerable security' which is sometimes welcomed as part of relationship-forming behaviours but which can decrease agency and thus lead to an unwelcome dependency. When relationships turn 'sour' or individuals exhibit coercive, controlling, or even abusive behaviours, 'vulnerable security' will be exploited. Facilitating proxy agency therefore requires careful consideration during the design process. To this end, the RRI approach is suited to guide anticipation, reflection, engagement, and action. It is prudent to employ the approach when innovating for communal use and privacy in the home.

Drawing on CoPriSm, the chapter further discusses opportunities to design for social goals and coordination while considering different modes of action (self, proxy, and collective). Expanding on the idea of using social goals as central design concern, we suggest designing for everyday interactions by rethinking access controls models from a goal-focused perspective [351]. In further characterising communities, the chapter highlights that proxy-agency is very commonly exercised among household members but under-researched [324] and not supported by design (e.g., Kumar and Schoenebeck [121] on parents and children or Murthy et al. [298] on older adults). It further suggests considering communities as constituted in proxy relationships, and that engaging in such relationships also requires orientation to moral order.

Finally, the agentic perspective offers insights into more specific ways digital housekeepers or administrators can empower other users [322]. There is currently no support for proxy users acting on behalf of others by design. Instead, proxies are forced

to impersonate others creating challenges in finding the right amount of advice. Design can support the work of proxy agents and help householders to become more familiar with devices in at least three principled ways: (1) by supporting alignment between self and proxy goals; (2) by encouraging proxies to articulate to other household members about the specific solutions for problems they solved; and (3) by encouraging proxies to demonstrate the implementation of a solution to others.

These insights and proposals are implemented in reviewing and designing interventions to empower privacy in communal use in Chapter 7.

Empowering Chapter 7 evaluates CoPriSm and demonstrates its ability to empower privacy through innovation in research and design. Two case studies representing research and design efforts are presented: a 'Case Study: Responsible Digital Housekeeping' handbook; and the 'Case Study: Two-Getherness | Home Security' mobile application prototype. While the two case studies backed by the previous chapters propose foresight and care as a way to ***address power imbalances among household members***, the extent to which these design goals and approaches are appropriate for 'adversarial households' [213] remains an open question. Power and control are ingrained in social systems, and design itself carries political implications [126].

The Case Study: Two-Getherness | Home Security application is built to *enable* communal use by dynamically establishing and maintaining social goals and purposes in interactions with a home security system. The prototype draws on the concept of mindful interaction [355] to support proxy users' decision-making by design. This processes of social negotiation can help mitigate power differentials that might otherwise emerge from the use of devices [7]. The design prevents unrestricted access and unregulated remote control that have been reported to contribute to misappropriation of devices [196]. In introducing social negotiation by design, approaches like the Two-Getherness application can normalise conversations about access, thereby preventing the "blank slate" problem (awareness of changes in settings causing friction and undermining trust) and conflict with children regarding access to devices.

However, while encouraging mindfulness and social engagement, CoPriSm might still increase 'vulnerable security' given its heavy reliance on proxy agency. There is reasonable doubt over its suitability for 'unhealthy' relationships. How can CoPriSm be used to limit the potential for such effects? The handbook Case Study: Responsible Digital Housekeeping is a cross-product intervention that encourages community members to actively *manage* communal use. As a leaflet, it can be added to product packaging of any smart home device. The intervention is targeted at proxy users, drawing on the concept of 'parental responsibility' [332] to instil foresight, responsiveness, and care. Due to its nature, it can also be picked up by other users, allowing 'non-administrators' to learn about ways in which they can get involved more closely. These users can thus encourage and support the main administrators in their work as well as deliberating and sharing their own goals and intentions. The leaflet also potentially limits unwelcome effects of increasing 'vulnerable security' in existing designs.

In presenting these two prototypes, we have documented the ways in which designers can draw on CoPriSm to design for social negotiation of goals and purposes while facilitating proxy actions through considering *foresight* and *care* as design goals. In so doing, design can facilitate users' management of relationships and expectations in the physical and digital world [145]. While these approaches work towards an equality of opportunity to access resources, future research can explore their feasibility further. As we have demonstrated in the previous chapter, using CoPriSm with RRI is a worthwhile approach to explore opportunities for design.

Another issue with existing designs are notice and consent frameworks. Our study in Chapter 5 highlights that such frameworks are designed to interact with a single user and usually not oriented to by the community. Notice and consent frameworks are pivotal efforts by legislators to ***address the power imbalance between users and manufacturers*** through legislation. While these frameworks have well-documented shortcomings that cannot be addressed as part of this thesis, our findings offer interesting implications for the GDPR's 'purpose limitation' principle, which is commonly practised by documenting ways in which data collection and processing practices serve technical

product features. While this technical purpose is fundamentally different from the social purposes of communal use, the disconnect between data protection regulations and everyday interaction offers an opportunity. By rethinking 'purpose limitation' in terms of social goals and purposes, communal use by design can be facilitated (assuming household members can align on a purpose) *and* manufacturers can learn more about the actual use of products. As we argue in the chapter, this kind of information is valuable for manufacturers in aligning their practices with reasonable expectations of individuals. Furthermore, manufacturers can determine whether any new purpose is compatible with an old one by considering users' ascribed purposes. We therefore suggest considering social goals and purposes as 'context of use' [1] information. Relatedly, knowledge of social goals and purposes pertaining to parenting or involving children by other means can also help manufacturers comply with requirements of the age appropriate design code where children are required to be included in consent processes.

On a final note, we urge researchers and designers to reflect on interpersonal privacy perspectives when addressing these issues. Those who understand privacy as control over information might be inclined to conclude that one can have more or less privacy through control over information. This perspective might distract from considering privacy as pervasive feature and favour "grafting" privacy onto a system [22]. Such a perspective would discount the meaning that provides for privacy in concerns of everyday interactions. CoPriSm's linking of interaction with agentic perspectives can help us understand this complexity. More research is also required to understand the margins of non-adversarial approaches at which adversarial safe-guarding is required.

8.3 Contributions

Based on the review in Chapter 2, we have identified an everyday perspective of technology use as most suited to filling a gap in the literature on understanding and empowering household privacy in smart homes. To this end, Chapter 3 highlighted opportunities for privacy research. This thesis' main contributions are to the scholarship

[1] Context of Use – https://www.interaction-design.org/literature/book/the-glossary-of-human-computer-interaction/context-of-use

on privacy in HCC and in cybersecurity as emerging 'meta-discipline' [38]. The thesis also makes contributions to the sociology of technology and social research more widely. In summary, the contributions of this research are:

An Everyday Perspective on Communal Use and Privacy – The exploratory interview study (Chapter 4) and longitudinal ethnomethodologically informed study (Chapter 5) unpack and document an organisation of communal use of smart technologies. Communal use is manifested in interactions of household members with devices which are oriented to everyday concerns of managing relationships [145] and expectations. These interactions are arranged for within a community of users and across divisions of labour at home. The division of labour contributes to conceptualisations of roles as 'who typically does what with which device' that are fluid, and thus in conflict with generative concepts of roles in system design. When roles are articulated by household members, they highlight expectations in relation to a social goal or established purpose of using devices. Relatedly, roles cannot be defined by a set of role expectations (rules) [305]. Fulfilling a role is not about executing tasks. Roles are evaluated against the meaning brought about by interactions ascribed to them [302]. Similarly, rules (role expectations) are not just about restricting behaviour but are also used to highlight meaning of interactions (e.g., attending to 'higher level' concerns of parenting [145]). For example, rules of regulating screen time are supposed to teach children self-control but they can also be broken due to contingencies such as doing home work.

Privacy is not an immediate concern in communal use, but implicated in everyday concerns, social goals, values, and societal norms. Sometimes it is brought about by past experiences and a sense of normalcy. In this sense, the concept of privacy involves everyday concerns related to the management of relationships and expectations [145]. However, household members' ability manage these concerns is crucially different outside the home, where a different sense of normalcy and, perhaps, stronger conceptualisations of societal norms persist. Outside there is little opportunity for communal use and notions of moral order to evolve in everyday interactions. For

example, a fluidity of roles, while visible inside the home, is not available to the wider community to the same extent.

Details of this contribution are presented in Section 5.4 and its implications for sociology of technology studies, usability and privacy research in HCI, access control models in system design, and relevance to data protection legislation are outlined in Section 5.5. To the best of our knowledge, the thesis is the first 'in-the-wild' investigation of household/communal privacy with off-the-shelf smart home technologies. The ethnographic data focusing on interactions (behaviour) itself has contributed to the field of usability research on smart homes and on privacy in particular. It has responded to a long-standing call for more empirical and observational investigations of smart device use in the home in HCC.

A Research Approach to Everyday Technology Use – The EM informed grounded analysis motivated in Section 3.2.2.2 and implemented in Section 5.2 has succeeded in providing rich insights into the organisation of communal use in the home. This is evidenced by the findings presented and discussed in Chapter 5.

The strength of the approach in investigating communal settings lies in a combination of rich data collection and a principled focus on social and moral order during data analysis. Observational and conversational (reported behaviour) insights on technology use from repeated household visits, group interviews, and participant diaries are complemented by occasional smart home planning workshops and participants' photographs of device placements. These data allow the researcher to thoroughly triangulate research insights and serve as tried-and-tested sources for research insights in HCC (e.g., [5, 205, 364]).

A GT inspired approach to an EM informed study and ethnographic data more broadly can help overcome challenges researchers face in documenting their findings and providing HCI and system design audience with appropriate representations of their insights [227, 242, 365]. Furthermore, the analysis in Chapter 5 demonstrates the power of drawing on EM sensitising concepts (i.e., everyday activities, natural

accountability, and dimensions of work – Section 3.2.2.2). These concepts suggest perspectives on practical work and provide questions that focus on the accomplishment of social order in interaction.

We believe that this approach can inform future research in HCC and the use of GT analysis in social research more broadly such as in other cultural contexts, with different kinds of technology, or for other forms of cohabitation. Details on the implementation of this approach are documented in Section 5.2 with all materials available in Appendix B and in an online repository[2].

The Conceptual Framework "Communal Privacy in Smart Homes (CoPriSm)"

Data protection professionals have called for "supporting trust in innovative data use" by considering privacy from "the earliest stage of development" [314]. However, appropriate frameworks for user experience and system designers to sensitise to the needs of household technology use are lacking. Therefore, CoPriSm was constructed to empower privacy through innovation in research and design (Chapter 6).

CoPriSm contextualises the everyday perspective on communal use and privacy (Chapter 5) by highlighting the involvement of community members, smart technologies, and information in the accomplishment of communal use. In complementing the interaction perspective of communal use with an agentic perspective, it recognises the need and/or preference for actor-focused perspectives in system design and policy. Drawing on SCT, the framework links everyday concerns reflected in interactions with functions of foresight and moral agency that regulate action. It further highlights that household members at times act for themselves (self-agency), on behalf of others (proxy-agency), and sometimes in coordinated ways (collective-agency).

In addition to offering the perspectives to empower communal use by design, the framework identifies related research perspectives that can contribute to the empowerment of communal use: contextualising of information, supporting awareness and intelligibility, and devising socio-technical affordances. Design thinking in Section 6.4.3 provides the approach to empowering privacy through innovation in

[2]https://osf.io/9ztk2/ – includes source code of the study dashboard

research and/or design areas, highlighting the importance of considering social goals of interactions when designing for privacy in communal use. We caution researchers and designers to explore future impacts of their innovations, especially with regard to power relationships. As demonstrated previously, an RRI approach allows for careful consideration of effects of design and innovation on existing power dynamics through anticipation, reflection, engagement and action. Responsible innovation is required to empower households in communal use and privacy.

The applicability of the framework for responsible empowerment of communal use and privacy is evaluated in two case studies in Chapter 7. The framework makes important contributions to research and design in HCC (Section 6.6), including (1) sensitising designers of smart technologies to considerations of communal use, highlighting the relevance of roles, rules, and moral order; (2) helping designers and researchers when identifying requirements for new products; and (3) serving as 'boundary object' [39].

Low Fidelity Prototypes as Design Interventions The design interventions, Case Study: Two-Getherness | Home Security and Case Study: Responsible Digital Housekeeping prototypes, are depicted in Chapter 7 and also available online[3,4].

The case studies draw on concepts of 'parental responsibility' [332] from RRI and 'mindful interaction' [355] from interaction design. As discussed in Section 7.3, they highlight opportunities to empower privacy by supporting foresight and care as design goals across different modes of action (self, proxy, and collective) and demonstrate the ways in which interaction designers and user experience researchers can draw on CoPriSm to foster innovative thinking in their respective disciplines. The RRI process documented and demonstrated the need for anticipation and reflection. Further engagement with stakeholders and users is required. Researchers and designers can, for example, build on these insights in a user study of the mobile application.

[3]https://github.com/markraemer/responsible-digital-housekeeping
[4]https://github.com/markraemer/two-getherness-security

Theoretical Contributions to Research and Practice in HCC As discussed in Sections 6.6 and 7.3, our findings contribute to the academic debate on privacy in HCC and cybersecurity in the following ways:

There are ongoing efforts to identify appropriate ways of regulating access for a community of users (e.g., [194, 213, 216, 217]). We have argued that social goal-focused design (e.g., goal-based access control [351]) can overcome analytic privacy dilemmas (which user group *should* have what level of access) by (1) recognising peoples' ability to navigate these questions and (2) reconciling interaction design with the social order in everyday interaction.

Efforts to foster security and privacy behaviours across a community of users draw on SCT [297, 327, 329]. However, these efforts appear to fall short of considering the importance and complexity of proxy-agency [319]. Relatedly, proxy interactions are poorly supported by contemporary device design. We suggest rethinking communities as networks of proxies that can support and challenge one another by exercising appropriate levels of foresight and care (Section 7.3). To reduce power imbalances resulting from different levels of access and knowledge with regard to smart technologies (increasing self-efficacy in others [325]), we further suggest a number of principled ways in which community members can empower each other: (1) working towards goal alignment (for self and proxy actions); (2) supporting others in creating executable plans for given problems; and (3) demonstrating problem solving approaches to others.

The perspective of designing for negotiation of social goals and purposes of device use contributes to debates on power imbalances between users and manufacturers (e.g., [17, 103, 193]). As argued in Section 7.3, legislation can be realigned with everyday concerns by rethinking the 'purpose limitation'. We suggest interpreting purpose to serve users' social goals rather than manufacturers' technical requirements. Learning about social purposes means having fulfilled data protection requirements of establishing 'reasonable expectation'. Agreement between household members on the purpose of a device and the social goal it serves enables users' to consent

meaningfully, even on behalf of the community. We encourage future research to investigate this line of inquiry.

Additionally, we contribute to the debate on interpersonal power imbalances in smart homes (e.g., [5, 7, 196, 213]) by suggesting that design goals of foresight and care can support social negotiation and help prevent 'function creep' [40, 48]. Normalising social negotiation of device use can also help address the "blank slate" problem of diminishing levels of trust through significant configuration changes [7]. However, community members consistently 'reconfigure' their relationships in everyday interactions. Future research can explore the ways in which this can be reflected by design.

8.4 Reflections

This work is the result of about four years of independent research. We use this section to reflect on this journey and the outcomes.

No doctoral journey is complete without any misadventure or rejection. It can be argued that misadventures offer the most important learning opportunities. An earlier version of Chapter 4 reported on a GT analysis of user experience with technology. The emerging theory highlighted social factors that influenced behaviour such as the presence of others or the devices others had installed. However, conference reviews critiqued its incompleteness and lack of explanatory power to model household members' experience and decision-making based on the chosen set of social and environmental factors. Inspired by existing research on technology use in the home that successfully dealt with social complexities, we revised our paradigmatic orientation to focus on everyday interactions. Adopting this new orientation has led to what is now Chapter 4.

At that point, we had already used the GT analysis to inform an exploratory survey (n=852) on attitudes towards technology and situational decision-making. We used a factorial vignette survey design to capture facets that might inform privacy related decision-making. The survey included qualities of relationships, different kinds of devices, and other social and physical factors in vignettes. However, the results were not sufficiently significant to capture contextual variations and personal preferences.

The initial GT of Chapter 4 and this survey were therefore ill-suited to uncover how the use of devices is organised among household members. Some parts of the survey, however, did offer interesting insights into attitudes and preferences, and were published as extended abstract [45] and further disseminated in outreach activities[5].

In other research that is not part of this thesis, we conceptualised and evaluated a design artefact and a design technique for usable privacy and security. The idea of the artefact was in line with our RQ–3, that is, to empower users through design. The artefact tried to model the context of privacy behaviours drawing on an array of contextual factors derived from empirical work and commonly used privacy theories. A first submission of a case study paper with the artefact faced critique for not being evaluated with designers, and as we subsequently were only able to run design workshops with student participants, we faced similar critique after a second submission. A third re-framing of the paper lacked analytic depth to make significant claims. However, we advocated for the method in non-peer-reviewed venues[6] and presented some intriguing insights from the workshops at a practice-focused conference [47].

These experiences motivate a closer look at the role of the researcher. It is in the nature of doctoral work that the author of this thesis was the sole, leading researcher who created and evaluated the CoPriSm framework. Although the case studies demonstrate the usefulness of the framework, further validation by other researchers and/or designers is desirable.

This leads us to further reflect on the nature of the research at hand. The empirical contributions and analytic insights in this thesis are limited to their research context (Oxford and London, United Kingdom) and derived from a small sample size of five/six households. While we do not consider the sample size as problematic for the trustworthiness of our findings (Section 3.4), future research can draw on larger sample sizes and other research contexts. Similarly, researchers might also want to apply our findings to other cultural research contexts where similar conceptualisations of privacy (e.g., as control over information) may be assumed.

[5] See Linacre News https://martin-kraemer.net/paper/navigating_Linacre-news.pdf

[6] See the Oxford Cyber Security CDT year book https://martin-kraemer.net/paper/dpbd-Cdt-Yb2020.pdf

Like other studies that involve human participants, our study may also be subject to the *Hawthorne Effect* [366], which we broadly describe as reorientation in research participants' behaviours due to the awareness that their behaviour is being studied [367]. While the effect cannot be avoided in participatory and ethnographic research, it can be accounted for (see section 3.4 and section 3.5). For example, prolonged engagement with participating households provided for better rapport and richer research insight, as well as detailed researcher field notes and participant diaries to be triangulated with interview data.

Given that *self-reported data* (interviews and diaries) does not guarantee 'complete' results, it is problematic when self-reported behaviour is the central focus of the research. To account for the issue, different data sources from our longitudinal investigation (Chapter 5.2.3) and a large number of interviews (Chapter 4) are triangulated. Researchers can apply different methods and repeat our efforts for future validation of our findings.

On a personal note, the reflections document the researcher's professional development and may serve as source for encouragement to other researchers looking for perseverance to continue their research efforts. Besides, these reflections are believed to provide starting points for future work.

8.5 Directions for Future Work

This section summarises and expands on opportunities for future work that have been highlighted throughout the thesis.

Design Patterns and Frameworks for Communal Use The case studies presented in Chapter 7 include design patterns around 'mindful interactions' and 'responsible use' that can be applied to other products. In future research, these artefacts can be evaluated with regard to the effectiveness of these design patterns. Researchers can also draw on CoPriSm and related frameworks (Section 6.2.1) in HCI and CSCW to propose new design patterns that accommodate for coordinate ('articulation' [306]) work. Most importantly, research and design need to appreciate that a communal

design orientation cannot be 'grafted on to a product' but carefully considered from the outset—much like what Dourish and Bell point out, privacy is a pervasive feature of a system that cannot be added as an afterthought.

Access Control for Communal Use Access control is often considered the panacea of security and privacy. Throughout this thesis, we have documented several shortcomings of models that try to accommodate for the realities of use (e.g., people moving in and out of roles), arguing for the more appropriate uses of access control (e.g., accommodating for egalitarian spousal relationships, or goal oriented access control approaches). However, we have left a number of questions for further investigation. For example, how can access control accommodate 'adversarial' and 'non-adversarial' relationships [7, 213]? Similarly, what are mechanisms and controls that can support this kind of access control [48, 351]?

Supporting Communities of Use As suggested in 6.6.4, a new perspective on shared use inside and outside the home can expand on existing work. Our exploration focuses on households (i.e., families with children), and while considerations of others surface, more research is needed. Building on Chapter 5 which highlighted a different orientation to moral order and social values by non-household members, we suggest adopting a perspective of proxy-relationships when identifying communities, that is to designing for the support of these relationships in ways that reflect social goals and purposes of device use (e.g., Two-Getherness application in Chapter 7).

Agency and Control in the Connected Home In discussing the power imbalance between users and manufacturers, Chapter 7 offered suggestions to rethink 'purpose limitation' within the current legislative framework for data protection. The extent to which the manufacturers' interpretation of purposes can be realigned with the social purposes in everyday use is subject to future research (Section 7.3.2).

The same power imbalances has also been addressed by other researchers, some of whom essentially propose that data storage be relocated to peoples' home. In their 2016 paper "Personal Data, Privacy and the Internet of Things: The Shifting Locus of

Agency and Control", Crabtree and Mortier have urged the nascent field of Human Data Interaction (HDI) to provide necessary research perspectives on the ways in which users can truly be in control of their data [368]. In response to Crabtree et al. [207], our findings provide a group management mechanism to negotiate device use. Future research needs to investigate the extent to which the mechanism is applicable to questions of data management. CoPriSm's 'actionising' perspectives can serve as a starting point (Section 6.5.1.3).

Informing Privacy Theory This thesis has provided an everyday perspective on privacy in communal use without engaging with existing privacy theory—with the exception of Contextual Integrity's *moral legitimacy* argument [21, p. 166] in Section 7.3.2 to discuss purposeful use of data.

The theory holds that information flows are considered appropriate as long as they comply with context-specific informational norms which are specific to social domains (e.g., healthcare, finance, or family). Information flows are combinations of a sender, a receiver, a data subject, a transmission principle, and a type of information. Inside the home, however, there is no single social domain, and the home itself cannot be considered as one. Instead, there is a mesh of social goals and mundane concerns reflexively established by household members in their actions. It is important to note that this mesh constitutes the social domain of the home occasioned in local, moral order. While household members are able to orient their actions within the mesh of values and goals, outsiders are unlikely to do so to the same extent. The nature of local, moral order at the intersection of household communities with the 'outside' world may be further explored in future work, e.g., using a research approach similar to Chapter 5.

8.6 Concluding Remarks

Reflected in the power imbalances between users and manufacturers as well as those between users, privacy, and other ethical concerns are grand challenges for the emerging field of Human Centred Computing. While privacy is a busy research area across HCC, there is a need for empirical, longitudinal, and exploratory research on technology use.

Addressing the challenge of household privacy in smart homes, this thesis has explored the phenomenon from an everyday perspective and made a number of important contributions to HCC. First, it provides empirical insights into the organisation of communal use and its relationship to privacy. Second, it offers a grounded analysis approach informed by EM sensitising concepts as another methodological tool for future research on issues of communal use. Third, it provides a framework for research and design to empower privacy in communal use through innovation. Fourth, it contributes two low fidelity prototypes as design interventions that demonstrate the value of the framework for interaction design and user experience research; and finally, it makes important theoretical contributions to the debate on privacy in HCC. We encourage researchers and designers to draw on these insights to further research and empower privacy in communal use.

Appendices

A

Supplementary Material Chapter 4

Contents

A.1 Ethics Application and Approval

CENTRAL UNIVERSITY RESEARCH ETHICS COMMITTEE (CUREC)

Form CUREC 1A Checklist for the Social Sciences and Humanities

The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure that the University is meeting its obligations as a responsible institution.

They start from the presumption that all members of the University will take their responsibilities and obligations seriously and will ensure that their research on human subjects is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

- Please check the **CUREC flowchart and NHS flowchart** first to see if you need ethics approval.
- Please complete this form using a word processor and email it, together with your supporting documents, to your **Departmental Research Ethics Committee (DREC)** (**if applicable**). If you don't have a DREC please email this form to **ethics@socsci.ox.ac.uk** using your official **ox.ac.uk email** address. **Only emailed applications will be accepted.**

WHAT THIS CHECKLIST IS DESIGNED FOR

This **CUREC 1A checklist** is designed largely for research that falls within the Divisions of Social Sciences and Humanities where ethical issues are relatively few and straightforward. Interviews, field work and oral history are also included in the CUREC process.

The **full CUREC 2 application** is only required where certain project characteristics (e.g. type of participants, or procedures) result in a more complex set of ethical issues. It is expected that only in a limited number of cases will it be necessary for researchers to complete a CUREC 2 application. The checklist below will direct you to a CUREC 2 application if needed.

WHAT THIS CHECKLIST WILL NOT ASSESS

This checklist does not cover research governance, satisfactory methodology, or compliance with the requirements of publishers when administering their tests or questionnaires. As principal researcher, it is your responsibility to ensure that requirements in these areas are met.

CUREC does not review studies classed as **audit** (see Glossary and Decision Flowchart for CUREC on our website).

If your study involves **NHS patients, NHS staff / data / facilities, or human tissue**, please check the Decision Flowchart for NHS approval and contact the Clinical Trials and Research Governance (CTRG) team in the first instance.

Further information on the University's research ethics procedures is available from the CUREC website: www.admin.ox.ac.uk/curec.

SECTION A: Filter for CUREC2 application This section determines whether your study raises more complex issues which require the completion of a full application for ethical review, known as the CUREC 2 application. **(Please mark 'X' in the Yes/No column as appropriate to indicate your response.)**		
1. Are research participants classed as **people whose ability to give free and informed consent is in question**? (This may include those under 18 (though see "competent youths" in **FAQ C12**), prisoners, or adults "at risk".) Your attention is drawn to the University's **Safeguarding Code of Practice** and its implications for researchers involving children or adults at risk, including the need for the work to be risk assessed and for researchers to undertake related training. (**Note**: If any of your participants are aged 16 or under, please answer 'Yes' here **and** also answer question 5 below.)	Yes	No X
2. By taking part in the research, will participants be at serious risk of criminal prosecution (e.g. by providing information on drug abuse or child abuse)?	Yes	No X
3. Does the research involve the **deception** of participants?	Yes	No X
4. Does your research raise issues relevant to the **Counter-Terrorism and Security Act (the Prevent duty)**, which seeks to prevent people from being drawn into terrorism? Please see advice on this on our **Best Practice Guidance web page**.	Yes	No X
If you have answered 'No' to all of the questions above please go to **Section B**. If you have answered 'Yes' to any question above continue to question 5 below.		
5. Is your project covered by a CUREC **approved procedure** (formerly known as "CUREC Protocols")?	Yes	No X
If yes, please give research procedure number(s):		
If you answered '**Yes'** to **ANY** of questions **1-4**, **and** answered '**No'** to question **5**, **please stop completing this checklist and do not submit it for ethical review**. Instead, please complete the CUREC 2 application form from the CUREC website. Then submit the CUREC 2 form for ethical review. If you answered 'Yes' to ANY of questions 1-3, **and** answered 'Yes' to question 5, please go on to **Section B**.		

SECTION B: Contact details and project description (NB: must be typed not handwritten)	
Contact details:	
1. **Principal researcher/**supervisor (title and name) (if student research):	Prof. Ivan Flechais
2. Name of student (if student research):	Martin J. Kraemer
3. Degree programme, e.g. DPhil, BA, MPhil, BSc, MSc (if student research):	DPhil
4. Department or Institute name:	Department of Computer Science
5. Address for correspondence (if different from above):	Martin Kraemer Linacre College St Cross Road Oxford OX1 3JA
6. University e-mail (**not** private email) and telephone:	Martin.kraemer@linacre.ox.ac.uk

7. Name and status of others taking part in the project, e.g. third year undergraduate; postdoctoral research assistant:	

SECTION B continued	
Project description:	
8. Title of research project:	The Smart Home: A Socio-Cultural Perspective
9. List of location(s) where project will be conducted:	Online: We will use Skype to conduct interviews online where meeting in person is not possible. UK (Oxford, Birmingham, Cambridge, Liverpool, and London) 1. Department of Computer Science, University of Oxford 2. Community Centres: Oxford (North Oxford Association, South Oxford Community Centre, Cheney Community Centre); Birmingham (The Irish Centre, Newtown Community Centre); Cambridge (Buchan Street Neighbourhood Centre, Meadows Community Centre); Liverpool (Croxtech Gems Community Association, Sri Lankan Community Centre); London (Ralph Perrin Club, Artizan Street Library and Community Centre, African Cultural Association)
10. If your research involves overseas travel or fieldwork, by the time the research starts, will you have completed and returned a travel risk assessment form? (This has to be approved by your department before you travel. If you are travelling overseas, you are strongly advised to take out University travel insurance.)	Yes X No N/A
11. Anticipated duration of research project overall:	months or 1 years (maximum 5)
12. Anticipated start and end dates of the research project involving human participants:	From: (01/11/2017) To: (31/03/2018) Extension to (31/05/2018) Please note that you will need ethics approval **before** you start your research. CUREC1As may take up to 30 days to process.
13. External organisation funding the research (if applicable): UK National Cyber Security Centre (NCSC) Small Grant Scheme through The Research Institute in Science of Cyber Security (RISCS)	
14. Title and very brief and simple lay description of **research** (about 150 words), plus description (about 200 words) of the nature of participants.	

a) Title, brief lay description of research (150 words). When describing the research, please include your methodology, how you are applying professional guidelines, and the use to which results/data will be put. **Please also declare any conflicts of interest here.**

Title: "The Smart Home: A Socio-Cultural Perspective"

This work is the first phase of my DPhil which aims to understand privacy in smart home environments. Smart homes are expected to reduce the time we spend on routine activities. Data becomes an enabler and asset, as smart devices collect and process it. Smart homes also have the potential to exaggerate bewilderment and resistance, feelings people express when their privacy is infringed. Because privacy is being influenced by socio-cultural factors and shaped by technology, this work argues for a thorough understanding of the home's socio-cultural context.

Focus groups and interviews will provide insights into social and cultural aspects of the home, e.g. structured social settings (norms, hierarchies, power). We will use grounded theory to develop a model of activities. These activities will be compared across demographics, forms of cohabitation, and different cultures. Considering the diverse demographics, a sub-sequent survey will validate the model to generalise the findings.

SECTION B continued

b) Description of participants and **obtaining informed consent** (200 words). When describing participants, please include

- criteria for inclusion/exclusion
- method of recruitment
- processes for consent to participate

Please ensure you attach as separate documents (if applicable, in English translation):

- your recruitment and advertisement material e.g. a poster or brief invitation letter/ email
- information for participants to read (or hear) before they agree to take part e.g. written information sheets or (only if applicable) oral information scripts.
- a document to record informed consent. Templates for written consent forms and/or oral consent scripts (in case of an oral consent process) are available from the CUREC website
- a guide to interview questions (this may be a list of questions to be asked, or a preliminary scope of questions), or a sample of other instruments (such as a sample questionnaire)
- (if relevant) debriefing document after participants have taken part

Focus groups and interviews are conducted in the Oxford/London area, and hence participation is geographically limited. In exceptional cases where meeting in person is not possible, Skype will be used to interview participants online. The survey will target people in the UK.

Participants for the study include individuals (over 18) and households (groups of people over 18). Children will not be included. At the beginning of each interview/focus groups written consent wil be seeked from all participants. An information sheet explaining the purpose of the study and intended usage of data (see attachement) will be presented alongside the consent form (in person or via email). The information sheet will be provided to the participants at least 24h in advance to their participation.

For interviews via Skype the consent form is signed electronically (by typing initials) and emailed back to the researcher as the first step during the interview (see attached form).

Participants of the pilot study will be recruited from the deparment. Initial contact will be made via emails and letters (example attached). We use snowballing to identifiy further participants within the department.

Recruitment for the main study will be done through community centres. We make contact with adults only by making contact with leaders of community centres. Community centres will be asked to forward the invitation to participate to their members. We might also use outreach events run by the University and engage with potential participants at other social events in Oxford, e.g. by handing out flyers at community centre events.
Other recruitment channels include online social media (Facebook, Twitter) and online/print versions of local news papers.
Participants may be pre-screened before they are allowed participation in the study. Pre-screening follows initial email contact by the participant and is done using an anonymous Google Form. Submissions of this form are registered with a unique ID which only the researcher can link to a name. These links are stored separately on an encrypted hard drive. Information on the pre-screening form will be a subset of the demographics questionnaire, e.g. form of housing (renter, owner); household size; relationship with other residents; and smart home devices (entertainment, health care, ...). Future versions might require futher limitations, e.g. gender, highest education, income. However, the form will at no point ask to provide an email address, IP, or the participant's name nor will this information be recorded online by other means known to the researcher.
Independent of the recruitment, consent for participation will be seeked from individuals directly at the beginning of an interview.

Participants for the quantitative study will be recruited online. We will use tools like Academic Profilic or Amazon mTurk, which already have a pool of registred users. Participation will be incentivised through a smapp payment (about £1).

We aim to engage with the following numbers of participants.

1. Pilot Study: 12 – 15
2. Main qualitative interviews and focus groups: 30 – 50
3. Online Survey: 1000 – 1500

We will start with interviews (see preliminary questions attached). Based on these interviews we might extract a group of individuals for a specific focus group (see prelminary questions attached).

The survey will be designed based on information derived from interviews and focus groups.Quesitons will hence be around the same topics mentioned in interviews and focus groups. The exact questions, however, will be available only after analysing our initial results.

15. What are the ethical issues connected with your research and what steps have you taken to address them? Please do not answer 'none'. The committee needs to see evidence that you have identified potential ethical issues with respect to your research and have taken steps to address them. These issues could relate to:

- your own physical and psychological safety as a researcher (please see the University's and Social Science Division's Safety in Fieldwork guidance
- participant burdens and/or risks, and
- data protection/ confidentiality.

For more guidance on ethical issues, please see www.admin.ox.ac.uk/curec/resources/.

1. Use of direct quotes; participants data will be anonymised and only identified by a code
2. Confidentiality of collected data; precautions and safeguards to protect the collected data will be taken; data will be securely stored
3. Privacy issues – participants are queried about their personal life at home; e.g., they might disclose the usage of certain devices that point to medical conditions they might have (see preliminary questions). We ensure participants that their data will be kept secure, not shared, and all information treated as highly confidential. We inform about the possibility to withdraw of the study at any point in time in which case all their records will be erased.

Section B continued

16. Will you obtain informed consent according to CUREC guidelines and good practice in your discipline before participation?	Yes X	No

If you have marked '**No**', please give a brief explanation and justification for this decision here:

17. Will your research involve discussing sensitive issues? This could be information relating to race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities.	Yes X	No

The conversations might touch on sensitive issues such as the aforementioned usage of health devices. However, the researcher will not acquire any further information about any such condition or related activity participants describe (see preliminary questions)

Conversations might touch on sensitive topics around living in the home. If participants feel uncomfortable about talking about any such issue, then there are sufficient other topics the research can direct the conversation to. The researcher will not actively acquire more information on any sensitive topic but take note of everything participants voluntarily share. All information will be kept secure following the recommendations.

If you have marked '**Yes**', please make sure that you have included some **supporting information** (as directed in question 14 of this section) showing the range of questions covering these issues.

18. Will you ensure that **personal data** collected directly from participants or via a **third party** is held and processed in accordance with the provisions of the Data Protection Act?	Yes X	No

19. How will you ensure that any personal and/or sensitive data are captured, transferred and stored securely?

In particular if data are to be captured electronically, please consult with the University's research data team (**researchdata@ox.ac.uk**) and your local IT department and, with respect to University IT security policies, please comment on how you will capture such data in the first instance, how you will transfer them over networks or via portable media and how, where and how long data will be stored. For more information please see the University's web pages on research data management:

http://researchdata.ox.ac.uk/university-of-oxford-policy-on-the-management-of-research-data-and-records/

All data gathered as part of this research will be securely stored backed up on an encrypted hard drive. The hard drive will kept under lock in the department (researcher's office). The working copy of the files will be stored on the researcher's laptop which uses whole disk encryption (Bitlocker) to protect the data. Personal data will be destroyed as soon as it is no longer needed for the study.

SECTION C: Methods and procedures to be used

Method used: Please ensure you have addressed any potential ethical issues related to these methods in Section 14 and in your Participant Information Sheet	**Please mark 'X'**
1. Analysis of existing records	
2. Snowball sampling (recruiting through contacts of existing participants)	X
3. Use of casual or local workers e.g. interpreters	
4. Participant observation	
5. Covert observation	
6. Observation of specific organisational practices	
7. Participant completes questionnaire in hard copy	
8. Participant completes online questionnaire or other online task	X
9. Using social media	
10. Participant performs paper and pencil task	
11. Participant performs verbal or aural task (e.g. for linguistic study)	
12. Focus group	X
13. Interview	X
14. Audio recording of participant (you will generally need specific consent from participants for this)	**X**
15. Video recording of participant (you will generally need specific consent from participants for this)	
16. Photography of participant (you will generally need specific consent from participants for this)	
17. Others (please specify):	

SECTION D: Professional guidelines and training		
In this section, please mark 'X' against at least one of the following professional guidelines you aim to adhere to. You should use the principles listed in your chosen guideline(s) in conducting your own research. **Note**: this is not an exhaustive list.		**Please mark 'X'**
Research specialism/ methodology	**Association and guidance document**	
Anthropology	Association of Social Anthropologists of the UK and Commonwealth	
Criminology	British Society of Criminology: Code of Ethics for Researchers in the Field of Criminology	
Education	British Educational Research Association Ethical Guidelines for Educational Research	
Geography	Association of American Geographers Statement on Professional Ethics Royal Geographical Society: Research Ethics and Code of Practice	
History	Oral History Society of the UK Ethical Guidelines	
Internet-based Research	British Psychological Society: Conducting Research on the Internet Association of Internet Researchers Ethics Guide Also see our Best Practice Guidance on internet-based research	
Law (Socio-Legal)	Socio-Legal Studies Association: Statement of Principles of Ethical Research	
Management	Academy of Management's Professional Code of Ethics	
Political Science	American Political Science Association (APSA) Guide to Professional Ethics in Political Science	
Politics	Political Studies Association. Guidelines for Good Professional Conduct	
Psychology	British Psychological Society Code of Ethics and Conduct British Psychological Society: Conducting Research on the Internet Also see "Internet-based Research" guidance above	
Social Research	Social Research Association: Ethical Guidelines	X
Sociology	The British Sociological Association: Statement of Ethical Practice	
Visual Research	ESRC National Centre for Research Methods Review Paper: Visual Ethics: Ethical Issues in Visual Research	
Other professional guidelines. Please specify the other guidelines used here*:*		
Please indicate what training in research ethics the researchers involved with this study have received, e.g. the title of the course and date completed (online training available at www.admin.ox.ac.uk/curec/training). If no formal training has been undertaken, please indicate any discussions of research methodology between researchers and supervisors here.		
Introductory session at the CDT "Research Ethics at Oxford"		

SECTION E: Signatures

- 'Electronic signatures' sent as email confirmations from a University of Oxford email address can be accepted. Separate emails should come from each of the relevant signatories as outlined below, indicating acceptance of the relevant responsibilities.
- If you have obtained handwritten (wet-ink) signatures, please scan them and the rest of the checklist pages to create a single PDF document and email through.

Please ensure this checklist is signed by:

For staff research:	**For student research**:
1. **Principal researcher**	1. **Principal researcher (project supervisor)**
2. **Head of Department (or nominee)**	2. **Head of Department (or nominee)**
	3. **Student researcher**

1. **Principal researcher signature/supervisor signature (if student research)**

I understand my responsibilities as **principal researcher** as outlined in the CUREC glossary and guidance on the CUREC website.

I declare that the answers above accurately describe the research as presently designed, and that a new checklist will be submitted should the research design change in a way which would alter any of the above responses so as to require completion of CUREC 2 (involving full scrutiny by an IDREC). I will inform the relevant IDREC if I cease to be the principal researcher on this project and supply the name and contact details of my successor if appropriate.

Signature: ……..

Print name (block capitals): …….. **Date**: ……...

2. **Departmental endorsement signature**

I have read the research project application named above. On the basis of the information available to me, I:

(i) consider the principal researcher to be aware of her/his ethical responsibilities in regard to this research;
(ii) consider that any ethical issues raised have been satisfactorily resolved or are covered by relevant professional guidelines and/or CUREC approved procedures, and that it is appropriate for the research to proceed (noting the principal researcher's obligation to report should the design of the research change in a way which would alter any of the above responses so as to require completion of a CUREC 2 full application);
(iii) am satisfied that: the proposed project design and scientific methodology is sound; the project has been/will be subject to appropriate **peer review**; and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the **public interest**.

Signed by Head of Department or nominee *(example nominees for student research include the Director of Graduate Studies/ Director of Undergraduate Studies)*:

Signature: ……..

Print name (block capitals): …….. **Date**: ……...

3. **Student signature (if student research)**

I understand the questions and answers that have been entered above describing the research, and I will ensure that my practice in this research complies with these answers, subject to any modifications made by the principal researcher properly authorised by the CUREC system.

Signed by student: ……

Date: ……...

Print name (block capitals): ……..

SECTION F: SUBMITTING THE COMPLETED CHECKLIST	**Please mark 'X'**
1. Check you have completed all sections (A-E)	X
2. Ensure your application is signed by you, your supervisor (if student) and department	X
3. **Please attach all supporting documents (see section B, question 14b for details).** If the appropriate supporting documentation is not included with your application, you will then be asked to provide this separately. **This may well delay the ethical review process, and thus the start of your research.**	X
4. Ensure you have declared conflicts of interest (if any) in Section B, question 14a.	X
5. If your department has a Departmental Research Ethics Committee (DREC), submit this checklist and supporting information to the appropriate departmental officer.	O
6. If your department does not have a DREC, submit the checklist and supporting information to the SSH IDREC (email ethics@socsci.ox.ac.uk).	X
7. Applications must be sent by email from your official ox.ac.uk email account. Please do not send applications by post.	X

SOCIAL SCIENCES & HUMANITIES
INTERDIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

2 November 2017

Martin Kraemer
Department of Computer Science
University of Oxford

Dear Mr Kraemer,

Research Ethics Approval (CUREC 1A)
Ref No: R54434/RE001

Title: The Smart Home: A Socio-Cultural Perspective

The above application has been considered on behalf of the Social Sciences and Humanities Interdivisional Research Ethics Committee (IDREC) in accordance with the procedures laid down by the University for ethical approval of all research involving human participants.

I am pleased to inform you that, on the basis of the information provided to the IDREC, the proposed research has been judged as meeting appropriate ethical standards, and accordingly approval has been granted.

Should there be any subsequent changes to the project, which raise ethical issues not covered in the original application, you should submit details to the IDREC for consideration.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager and Secretary SSH IDREC

cc: Prof Ivan Flechais, Sharon Lloyd

SOCIAL SCIENCES & HUMANITIES
INTERDIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

20 March 2018

Martin Kraemer
Department of Computer Science
University of Oxford

Dear Mr Kraemer

Amendment of research ethics application

Ref No: R54434/RE003

Title: The Smart Home: A Socio-Cultural Perspective

Number of Amendment: 2

Month notification received: March 2018

Subject of amendment: extension of project end date, additional Skype interviews

The above request for amendment has been reviewed on behalf of the Social Sciences and Humanities Interdivisional Research Ethics Committee (IDREC).

I am pleased to inform you that, on the basis of the information provided to the IDREC, this amendment has been judged as meeting appropriate ethical standards.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager & Secretary SSH IDREC

cc: Prof Ivan Flechais, Sharon Lloyd

SOCIAL SCIENCES & HUMANITIES
INTERDIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

28 November 2017

Martin Kraemer
Department of Computer Science
University of Oxford

Dear Mr Kraemer

Amendment of research ethics application

Ref No: R54434/RE002

Title: The Smart Home: A Socio-Cultural Perspective

Number of Amendment: 1

Month notification received: November 2017

Subject of amendment: Pre-screening of participants

The above request for amendment has been reviewed on behalf of the Social Sciences and Humanities Interdivisional Research Ethics Committee (IDREC).

I am pleased to inform you that, on the basis of the information provided to the IDREC, this amendment has been judged as meeting appropriate ethical standards.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager & Secretary SSH IDREC

cc: Prof Ivan Flechais, Sharon Lloyd

A.2 Participant Information Sheets

DEPARTMENT OF
COMPUTER
SCIENCE

The Smart Home: A Socio-Cultural Perspective
Researcher: Martin Kraemer
Document Version: 23/04/2021

Principal Investigator
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

Researcher
Martin Kraemer, DPhil student
martin.kraemer@cs.ox.ac.uk

The Smart Home: A Socio-Cultural Perspective

PARTICIPANT INFORMATION SHEET

Ethics Approval Reference: R54434/RE001

1. ***What is the purpose of this study?***
   This research aims to provide insights into the socio-cultural context of the smart home. An understanding of which activities, in which way, and with which intended purpose are being carried out in the home is essential for our future research. We combine this understanding with the role smart technology plays as of today.

   This study is funded by the Engineering and Physical Science Research Council (EPSRC) and supported by the Research Institute in Science of Cyber Security (RISCS).

2. ***Why have I been invited to take part?***
   You have been invited to take part in this study as we aim to include people who are above 18 years old and are interested in smart home technology.

3. ***Do I have to take part?***
   No. You can ask questions about the study before deciding whether or not to participate. If you do agree to participate, you may withdraw yourself and your data from the study at any time, without giving a reason and without penalty, by advising the researchers of this decision. All your data will be erased from our records. Withdrawal is possible within 4 weeks from the date your interview or focus group took place.

4. ***What will happen to me if I take part in the study?***
   If you are happy to take part in the study, you will be asked a number of questions about yourself, the household you are living in, activities in the home, and smart technology you use.
   This should take approximately 45 minutes, but not longer than one hour.
   The study will take place at a public location convenient for you. That might be a nearby community centre, or at the University in Oxford. The consent letter includes the option to withdraw of follow up enquiries we might have. If you wish to do so, please check the respective box.

   With your consent, the interviews and focus groups will be recorded on audio. If you don't wish to be audio recorded, please inform the researcher. Audio recording is mandatory for focus groups. In interviews the researcher can refrain to note taking. The researcher will transcribe the interview. However, neither the

audio file nor the transcription made available to any other person than the researcher and principal investigator.

5. ***Are there any potential risks in taking part?***
We collect information about yourself and your household. To guarantee appropriate data management we will fully anonymize this information and store it on an encrypted and password-protected hard drive within the University. We will apply appropriate safe-guards to protect your data.

6. ***Are there any benefits in taking part?***
You will receive an £10 Amazon voucher in compensation for your time.

7. ***What happens to the data provided?***
The **research data** will be stored confidentially using an encrypted hard drive and kept locked away in the University. Your responses will be fully anonymized. Anonymised data will be accessible to the researcher and principal investigator.

Personal/sensitive data will be stored separately and confidentially, only accessible to the researcher.

All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

8. ***Will the research be published?***

The research will be published as part of the RISCS research scheme. Future research papers might be published at academic conferences.

The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to the full text of freely available theses, thereby increasing the likely impact and use of that research.

If you agree to participate in this study, the research will be written up as a thesis. On successful submission of the thesis, it will be deposited both in print and online in the University archives, to facilitate its use in future research. The thesis will be published open access.

9. ***Who is organising and funding the research?***
This research is part of a DPhil thesis investigating privacy in smart homes. The research is funded by the Engineering and Physical Science Research Council (EPSRC) and the Research Institute in Science of Cyber Security (RISCS).

10. ***Who has reviewed this study?***

This study has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Reference number: R54434/RE001).

11. ***Who do I contact if I have a concern about the study or I wish to complain?***

If you have a concern about any aspect of this study please contact Mr. Martin Kraemer

best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:

Chair, **Social Sciences & Humanities Interdivisional Research Ethics Committee**; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD

12. Further Information and Contact Details

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

Researcher
Martin Kraemer, DPhil student
University of Oxford
Linacre College, St. Cross Road
Oxford, OX1 3JA

Oxford email address: martin.kraemer@cs.ox.ac.uk

A.3 Interview Guide

DEPARTMENT OF
COMPUTER
SCIENCE

The Smart Home: A Socio-Cultural Perspective
Researcher: Martin Kraemer
Document Version: 23/04/2021

Interview Guide

Participant number *(filled in by the researcher)*

This is the researcher's guide for semi-structured interviews with participants. Interviews will be audio-recorded and fully transcribed by the researcher.

1 Introduction

☐ explain interview procedure and estimated duration of the interview

☐ hand out, explain, and sign documents

- ☐ information sheet for participants (provided via email/post in advance)
- ☐ consent form

⚠ **START audio-recording**

2 Technology

2.1 What technology do you have in your home?

Might include connected and not connected devices: household appliances, entertainment systems, communication systems, healthcare, home automation

2.1.1 What devices do you have in your home?

2.1.2 What devices are continuously present/unobtrusive/integrated in your home?

2.2 Product usage. The most useful product and the least useful procurement.

This is ideally but not necessarily about connected devices.

2.2.1 What is the latest product you have bought?

2.2.2 Do you get the expected benefit in so doing?

2.2.3 Among all devices you own, which product are you using the most? What is the reason?

2.2.4 Among all devices you own, which product are you using the least? What is the reason?

2.2.5 Which product provides the biggest benefit to your daily life? Please describe how.

2.2.6 Which product is the most troublesome to you? Please describe why.

DEPARTMENT OF
COMPUTER
SCIENCE

The Smart Home: A Socio-Cultural Perspective
Researcher: Martin Kraemer
Document Version: 23/04/2021

2.3 Procurement intentions.

2.3.1 Which other products are you planning to buy (or would you like to have)?

2.3.2 What is your motivation of buying these products?

2.3.3 What benefit do you expect from using them?

2.3.4 What is stopping you from buying them?

2.3.5 Do you have any concerns towards a specific product?

2.4 Future Technology Improvements.

2.4.1 What would be an activity you'd really want to be supported by technology?

2.4.2 Could you describe your perfect piece of technology and its usage?

3 Activities in the home

For the following will be discussed in context of connected devices. If the household does not own any connected device, the discussion will use examples of un-connected technology.

3.1 Please describe your typical week day routine.

3.1.1 What are your activities from getting up to leaving the house/flat/building?

3.1.2 What are your activities after returning home from work until you go to bed?

3.1.3 Which technology do you use in either part of your daily routine at home, e.g. your alarm clock?

3.2 Please describe your typical weekend routine.

3.2.1 What are typical activities you do at home?

3.2.2 Which technology do you use in either part of your daily routine at home, e.g. gaming console?

3.3 How much time do you usually spent at home (week day / weekend)?

DEPARTMENT OF
COMPUTER
SCIENCE

The Smart Home: A Socio-Cultural Perspective
Researcher: Martin Kraemer
Document Version: 23/04/2021

4 Impact on Cohabitation

4.1 Roles and responsibilities.

4.1.1 How would you describe your own affinity and that of your co-residence towards technology?

4.1.2 Who is usually taking care of/managing the technology you have?

4.2 Changes in cohabitation.

4.2.1 Have you recognised any change in cohabitation after you bought new technology?

4.2.2 Could you image a way in which new technology would change the way you spend time in your home?

4.3 Usage Pattern.

4.3.1 What is the usage pattern of technology among residents?

4.3.2 Do you share technology/share access to technology with your co-residents?

4.3.3 Is a specific piece of technology used by all residents?

5 Relationships

Many of these questions touch on rather private topics. However, there are plenty of things to talk about without touching sensitive matters.

5.1 The following questions are to be discussed for:

- co-residents (family/partner/flat mates/tenants)
- partner/significant other
- family members
- friends

5.1.1 How would a typical get-together with them in your home look like? (time, activities, …)

5.1.2 Where in your house/flat would you host them/not host them?

5.1.3 Please describe your relationship to them.

5.1.4 How do you use technology while spending time with them?

DEPARTMENT OF COMPUTER SCIENCE

The Smart Home: A Socio-Cultural Perspective
Researcher: Martin Kraemer
Document Version: 23/04/2021

6 Closing

⚠ **STOP audio-recording**

☐ closing notes / information

☐ provide Amazon voucher / get email address to send voucher to

Figure A.1: Interview guide for our semi-structured interviews in Chapter 4

A.4 Consent Form

DEPARTMENT OF
COMPUTER
SCIENCE

The Smart Home: A Socio-Cultural Perspective
Researcher: Martin Kraemer
Document Version: 23/04/2021

Principal Investigator
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

Researcher
Martin Kraemer, DPhil student
University of Oxford
Linacre College, St. Cross Road
Oxford, OX1 3JA

Oxford telephone number: 077 843 95 991
Oxford email address: martin.kraemer@cs.ox.ac.uk

PARTICIPANT CONSENT FORM

CUREC Approval Reference: R54434/RE001

The Smart Home: A Socio-Cultural Perspective

Purpose of Study:

This research aims to provide insights into the socio-cultural context of the smart home. An understanding of which activities, in which way, and with which intended purpose are being carried out in the home is essential for our future research. We combine this understanding with the role smart technology plays as of today.

		Please initial each box
1	I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
2	I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason, and without any adverse consequences or academic penalty.	☐
3	I understand that research data collected during the study may be looked at by designated individuals from the University of Oxford where it is relevant to my taking part in this study. I give permission for these individuals to access my data.	☐
4	I understand that this project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee.	☐
5	I understand who will have access to personal data provided, how the data will be stored and what will happen to the data at the end of the project.	☐
6	I understand how this research will be written up and published.	☐
7	I understand how to raise a concern or make a complaint.	☐

8	I consent to being audio recorded	☐
9	I understand how audio recordings will be used in research outputs	☐
10	I agree to take part in the study	☐
11	I understand that all my data will be anonymised.	☐
Optional:	I agree for my personal data to be kept in a secure database for the purpose of contacting me about future studies.	☐

Name of Participant	Date	Signature
Name of person taking consent	Date	Signature

A.5 Recruitment Poster

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF OXFORD

Principal Investigator
Prof. Ivan Flechais
Ivan.flechais@cs.ox.ac.uk

Researcher
Martin Kraemer, DPhil student
martin.kraemer@cs.ox.ac.uk

The Smart Home: A Socio-Cultural Perspective

Ethics Approval Reference: R54434/RE001

November 2017 – January 2018

NEEDED: VOLUNTEERS FOR INTERVIEWS

£10 Amazon voucher as compensation!

What: *45-60 minutes* of audio recorded interview
What are our daily activities and routines in the home?
Do we use smart technology in the home?
How could we improve such technology to better fit our needs?

Who: *over 18s*, no need to own a "smart home device"

Where: your *community centre*

When: at a *convenient time*

Contact: Martin Kraemer – martin.kraemer@cs.ox.ac.uk – 077 843 95 991

Smart Home Study Volu Contact: Martin Kraeme Martin.kraemer@cs.ox. Reward: £10 Amazon vc

B

Supplementary Material Chapter 5

Contents

B.1 Deployment Pictures and Notes

Taking pictures of the devices was entirely voluntary and optional. Hence, we only have picture of some devices in some households.

B.1.1 Household 1

Household 1 installed their smart security cameras outside the building, overlooking their own property and the public foot path / school path in front of their house. The household also received an Amazon Alexa which was placed in the kitchen and used by all household members; the teenage daughter exclusively used an Amazon Echo Dot in her room.

Figure B.1: Devices in Household 1: All smart security cameras were positioned outside the house

B.1.2 Household 2

One Google Home Mini was placed in the living room, and another Home Mini was placed in the parents' bedroom. A Home Hub was used in the kitchen. Only the device in the kitchen was used on a regular basis, and the two Home Minis remained frequently unplugged for several days. An Arlo Smart Doorbell and a security camera overlooking the front door approach were installed and configured for use by both adults.

B.1.3 Household 3

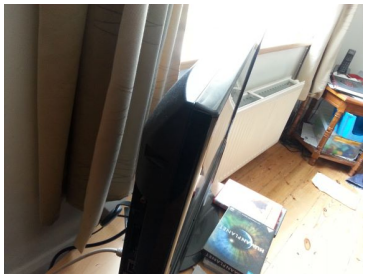
At the beginning of the study, it became apparent that household 3 required a more recent smart phone to use any of the companion apps that came with smart home devices. Household 3 then chose a Hive Smart Thermostat that was installed professionally

(the internet connection bridge was later on unplugged) and a Google Home Hub Max. The household members decided later on to get a Google Home Mini and a Google Chromecast.

Figure B.2: New devices in Household 3

(a) Google Home Hub Max on dining table in the kitchen

(b) Google Home Mini on the living room floor



(c) Google Chrome Cast plugged into the living room television

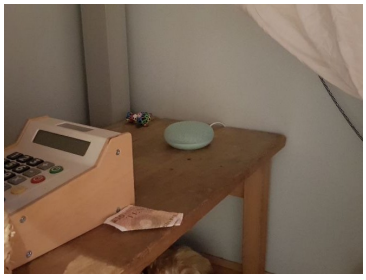
B.1.4 Household 4

Household 4 chose a Google Home Mini for the daughter, an Echo Show for the living room which later was used in the bathroom, a smart camera with doorbell and chime for the front door to keep track of their son, and smart lights for their son.

Figure B.3: Pictures of deployed devices in Household 4

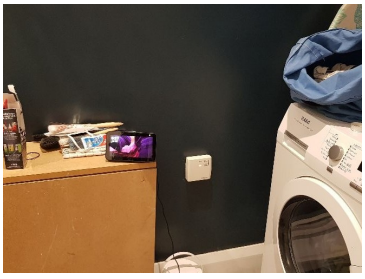
(a) Smart light in parent's bedroom

(b) Smart light and Amazon Echo Dot in son's bedroom



(c) Google Home Mini in daughter's bedroom

(d) Smart camera above the front door



(e) Echo Show in bathroom

(f) Smart camera upstairs to observe birds

B.1.5 Household 6

The household members built their smart home system with Apple's Homekit as central control unit. Hence, they chose a new Apple TV, a bridge to their existing smart thermostat, a smart switch for a lighting system, and a set of lights for their landing. During the study, they purchased a ring doorbell off their own account.

B.2 Ethics Application and Approval

CENTRAL UNIVERSITY RESEARCH ETHICS COMMITTEE (CUREC)

CUREC 2 Application form

The University of Oxford places a high value on the knowledge, expertise, and integrity of its members and their ability to conduct research to high standards of scholarship and ethics. The research ethics clearance procedures have been established to ensure that the University is meeting its obligations as a responsible institution. They start from the presumption that all members of the University will take their responsibilities and obligations seriously and will ensure that their research involving human participants is conducted according to the established principles and good practice in their fields and in accordance, where appropriate, with legal requirements. Since the requirements of research ethics review will vary from field to field and from project to project, the University accepts that different guidelines and procedures will be appropriate.

ONLY FULLY SIGNED TYPE-WRITTEN CHECKLISTS WILL BE ACCEPTED, BY EMAIL

WHAT THIS APPLICATION FORM IS DESIGNED FOR

This **CUREC 2 application form** can be used for applications **either** to the Social Sciences and Humanities **or** to the Medical Sciences Interdivisional Research Ethics Committees (SSH IDREC and MS IDREC respectively).

The form is designed for research where certain project characteristics (e.g. type of participants, or procedures) result in a set of ***complex ethical issues***. It is expected that only in a limited number of cases will it be necessary for researchers to complete a CUREC 2 application. Therefore, if unsure whether your project is complex, please check (i) on our website: http://researchsupport.admin.ox.ac.uk/governance/ethics (see Glossary and our Contacts); (ii) with your department; or (iii) with your departmental research ethics committee (if you have one).

The use of an ***asterisked word*** in this application form indicates a phrase defined in and linked to the CUREC's Glossary. The Glossary and further information on the University's research ethics procedures are available on our website.

WHAT THIS APPLICATION FORM WILL NOT ASSESS

The application form should not be used for research with ***straightforward ethical issues*** (see Glossary). For such research, please use the CUREC 1A checklist (for applications to SSH IDREC), the CUREC 1 checklist (for MS IDREC) or the minimal risk application form (for OxTREC). To access these documents please go to our How to Apply pages at http://researchsupport.admin.ox.ac.uk/governance/ethics/apply.

This form does not cover research governance, satisfactory methodology, or compliance with the requirements of publishers when administering their tests or questionnaires. As Principal Investigator, it is your responsibility to ensure that requirements in these areas are met.

CUREC does not review studies classed as ***audit*** (see Glossary and the Decision Flowchart for CUREC on our website).

If your study involves **NHS patients, NHS staff / data / facilities, or human tissue**, please check the Ethics Decision Flowchart and contact the Clinical Trials and Research Governance (CTRG) team in the first instance.

Please complete the sections that follow and follow prompts to stop completion and/or submit other documents.

Please indicate your answer to all the Yes / No questions by typing 'X' in the appropriate box.

Example:		
*1. **Involvement of other ethics committees. Will you submit or have you submitted this project to another ethics committee?***	*Yes X*	*No*

SECTION A: Principal Investigator contact details, other researcher(s) contact details, and project description	
***Principal Investigator** / Supervisor (if student research) contact details:	
1. Title of person and name:	Prof. Ivan Flechais
2. Title and name of student (if student research):	
3. Degree programme, e.g. DPhil, BA, MPhil, BSc, MSc (if student research):	
4. Department or Institute name:	Computer Science
5. Address for correspondence (if different from 4 above):	
6. University E-mail address:	ivan.felchais@cs.ox.ac.uk
University telephone number:	
7. Training in research ethics: please indicate what training you have received with title and date completed (online training available)	Research integrity online training, social and behavioural sciences
Other researcher(s) - these 6 questions may be duplicated below for each individual:	
8. Title of person (or people) and name(s):	Prof Max Van Kleek
9. Department or Institute name:	Computer Science
10. Address for correspondence (if different from 4/5 above):	
11. University e-mail and telephone contact:	max.van.kleek@cs.ox.ac.uk
12. Role(s) in project: please give role(s), qualifications and relevant experience and degree course (if relevant):	Co-I
13. Training in research ethics: please indicate what training other researcher(s) received with title and date completed (online training available)	Research integrity online training, social and behavioural sciences
8. Title of person (or people) and name(s):	Dr Helena Webb
9. Department or Institute name:	Computer Science
10. Address for correspondence (if different from 4/5 above):	
11. University e-mail and telephone contact:	Helena.webb@cs.ox.ac.uk
12. Role(s) in project: please give role(s), qualifications and relevant experience and degree course (if relevant):	Researcher
13. Training in research ethics: please indicate what training other researcher(s) received with title and date completed (online training available)	tbd
8. Title of person (or people) and name(s):	William Seymour
9. Department or Institute name:	Computer Science
10. Address for correspondence (if different from 4/5 above):	
11. University e-mail and telephone contact:	william.seymour@cs.ox.ac.uk
12. Role(s) in project: please give role(s), qualifications and relevant experience and degree course (if relevant):	DPhil researcher
13. Training in research ethics: please indicate what training other researcher(s) received with title and date completed (online training available)	Introductory session at the CDT “Research Ethics at Oxford”
8. Title of person (or people) and name(s):	Martin Kraemer

SECTION A (continued): Principal Investigator contact details, other researcher(s) contact details, and project description	
10. Address for correspondence (if different from 4/5 above):	
11. University e-mail and telephone contact:	Martin.kraemer@cs.ox.ac.uk
12. Role(s) in project: please give role(s), qualifications and relevant experience and degree course (if relevant):	DPhil researcher
13. Training in research ethics: please indicate what training other researcher(s) received with title and date completed (online training available)	Introductory session at the CDT "Research Ethics at Oxford"

Project description			
14a. Full title of research project:	Informing the Future of Data Protection by Design and by Default in Smart Homes		
14b. Short title (optional – for use on participant-facing documents):	Informing the Future of Smart Homes		
15. List all *__sites__* where project will be conducted:			
Department of Computer Science; Participants' homes; Facilities of our industrial partners			
16. If your research involves overseas travel or fieldwork, and your department requires a travel risk assessment, will you have completed and returned a risk assessment form before the travel/fieldwork commences? (This has to be approved by your department before you travel). If you are travelling overseas, you are strongly advised to take out University travel insurance	Yes	No	Not required X
If no, or not required, please give further details:			
Study takes place within the UK, travel only to participants homes within the UK			
17. Anticipated duration of project: (Maximum duration is 5 years)	1 year		
18. Anticipated start and end dates of the project:	From: asap after ethics approval (dd/mm/year) To: 01/04/2020 (dd/mm/year)		
19a. External organisation funding the research (if applicable):	Information Commissioner's Office (studies, PDRA and developer) EPSRC UK (PhD studentships for Martin Kraemer and William Seymour)		
19b. Funder reference number (if applicable):	Tbd EPSRC UK P00881X/1		

20. Involvement of other ethics committees		
Will you submit or have you submitted this project to another ethics committee?	Yes	No X
If other relevant approvals for this research are required (e.g. from other universities' ethics committees) please attach them and give more details below:		

21. Have you used any of the following to develop your application:	Yes X	No

- CUREC approved procedures (see http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/ap)
- Professional guidelines (see our website for a selection of professional guidelines)
- CUREC Best Practice Guidance

If yes, list relevant documents and give details.

If no, please explain why not below:

We consulted British Psychology Society (BPS) guidelines and British Educational Research Association Ethical Guidelines for Educational Research:

1. For children participating in our research, we will seek explicit consent from parents or guardians for participation and, audio and video collection.

   We will ask children to assent to participation in our study. Before doing so, Children will be provided with an information sheet written in appropriate language and illustrating the purpose of this study (see attachment). At any point, there will be an opportunity to ask any questions. Participants can withdraw at any point in time before or during the last interview. Participants can also withdraw their data up to one month after the last interview took place. If a single individual decides to withdraw, the rest of the household may continue the study. If the participants also decides to withdraw consent for data usage, any of their recorded data removed from the study. For interviews, this means their quotes will be deleted from transcripts, and video material with their participation will be deleted fully.

   Should a whole household decide to withdraw from the study, they will be given the option to also withdraw consent with regards to their data being used, and we will delete all their data we hold.

2. This study touches on sensitive issues of privacy. During interviews participants are likely to discuss situations where they feel their privacy was infringed or violated. This may include personal information, e.g. they might disclose their usage of devices associated with medical conditions. We will reassure participants that their data will be kept secure, not shared, and that all information will be treated as highly confidential. We will also remind them that they have the option of withdrawing their data from the study at any point.

22. Description of the project **in lay language** (200 words max)

Please say why your project is important and valuable. Describe briefly your methodology. Although it's important to describe any aspect of your project which is beyond already established and accepted techniques, **we do not require a detailed scientific background unless directly relevant to ethical issues**.

At home, we share devices and systems with our cohabitants making privacy practice and system design even more complex than for individual use. Smart devices, e.g. voice assistants or light systems, are always connected and share information with external entities. They are able to act, react, and adapt by sensing their environment, that is collecting data. This data supports device functionality but sometimes may also be used for other purposes. Legislation has addressed collection and sharing practices through the General Data Protection Regulation turning 'Data Protection by Design and by Default' into a legal obligation. Yet, there is no guide comprehensively addressing the need for compliance guidelines.

This project aims to fill this gap by understanding the unique privacy needs arising in smart homes, and exploring the design space to meet these needs.

WP1 **Understanding socially embedded privacy** – conduct a four to six months longitudinal study of 6-8 households living in smart homes to understand socially embedded privacy: a series of unstructured interviews with households in their home will be audio and video recorded. Households might be families or other forms of cohabitation, with and without children.

SECTION B: Research involving contact with human participants

If the project involves **contact** with ***human participants*** (in person or virtual), or **observation** of them, ***please complete this section (Section B).***

If the project involves **no contact** with ***human participants*** (in person or virtual) and **no observation** of them, but only use of data about them, ***please do NOT complete this section, but go to Section C.***

23. Description of participants (300 words max).

Please describe (for each different participant subgroup):

- number of participants to be recruited and age range;
- Inclusion and/or Exclusion Criteria
- Other ***defining criteria*** for participation including what type of people are sought (e.g. students, children, politicians, prisoners, refugees, NHS staff). Please state if the participants' ability to consent may be compromised in any way (i.e. 'at risk' participants). Researchers need to be sensitive to safeguarding issues for at risk adults and children, and follow the guidance set out in the University's 'Safeguarding Code of Practice'. This includes ensuring that a safeguarding risk assessment of the proposed research has been completed when planning the research and appropriate training has been undertaken.
- How, where and by whom participants will be identified and approached to take part in the project. (possible routes to consider include poster, flyer, email, in-person approach, word of mouth / snowball sampling, newspapers, Social media (e.g. twitter/Facebook), specific website recruitment sites (e.g. Amazon Turk), other ongoing studies, etc.)
  If co-researchers are conducting any part of the consent process, give their qualifications and experience.

WP1 Understanding socially embedded privacy

a. Methodology

This is a 6 months long ethnographic interview study taking place at participants' homes. Interviews (up to 8 in total) will be unstructured, will take place at participants' homes, and will be centred around the use of internet-connected as part of daily routines. Devices will be given to households early in the study. The interviews will be driven more by participants than by the researcher, that is there will be no pre-defined agenda.

b. Number of participants and age range

Participants will include adults and children aged six or above. We will aim to recruit 6-8 dual-income families with or without children because of their complexity of daily life making them more interesting as subjects for our study.

Safeguarding

Children will be allowed to participate in our conversations as much as their parents do, whenever and however they would like to. While we will not strictly require all household members to be present, we will require one adult/guardian to be co-present for children below the age of 16.

Our ethnographic research approach requires a detailed account of conversations between household members and their smart home devices. While we can audio-record conversations easily and take notes of what we see when we are present, some of the participants work will be done without our presence. We might ask them to comment on their experiences with smart devices and are interested in placement and interaction. This information is best and easiest video recorded. The recordings will be transcribed and then analysed by our research team. We will require parents'/guardians' consent and children's assent prior to audio and video recording the conversations. All research staff involved in this work package will be required to familiarise themselves with the University's Safeguarding Code of Practice and complete OSCB's (Oxfordshire Safeguarding Children Board) online training. Prof Flechais will be appointed as the "Designated Safeguarding Lead" of the study and work together with the University Safeguarding Officers to ensure all safeguarding processes are in place and the project complies with the University's Code of Practice.

We provide the attached risk assessment form in which we describe how we further control risks.

c. Inclusion / exclusion criteria

We will exclude children below the age of six. Households will be pre-screened for their intentions to obtain devices, that is to make sure we understand their interest in products and the study. No prior

knowledge of or experience in using smart home technology will be required.

d. Other defining criteria

e. Recruiting details

We will recruit participants from a pool of past studies, online portals such as peopleforresearch.co.uk, and through posters in the department and around the university.

We will not exclude participants from particular social, ethical or economic backgrounds. The consent process will be mainly carried out by Martin Kraemer who has received appropriate training and has carried out interview research before

24. Will any of your participants be *__children__*?	Yes	No

If yes, please describe:

- How they are defined as children based on cultural context. I.e. the age of adolescence and adulthood varies by country.
- Any CUREC approved procedures or CUREC guidelines relating to children that you feel apply (if not stated at question A21). In particular, see CUREC guidance on Competent Youths, (BPG 04 at http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/bpg) and our FAQ C11-C12 at http://researchsupport.admin.ox.ac.uk/governance/ethics/faqs-glossary/faqs#tab-1-2.
- In particular, please state why either CUREC Approved Procedure 15 or 25 (research on children) cannot apply wholly to your project.

WP1 Understanding socially embedded privacy

We will focus on dual-income families with or without children. Because our research will take place in-situ, at our participants homes, we cannot follow approved procedure AP25.

/Section B (continued)

SECTION B (continued): Research involving contact with human participants		
25. Will ***unequal relationships*** exist between participants and those obtaining informed consent? **If yes,** describe nature of unequal relationship and how arising ethical issues will be resolved.	Yes X	No
Children of the age of 6 and above may participate in this study if they wish to do so. However, there's no requirement for households to participate with all members, neither are their any negative consequences for the rest of the household in case individuals drop out of the study and withdraw their consent of data being used (see Q21). The same is true for children. They may drop out during or before the last interview and withdraw their consent for data usage up until one month after the last interview took place while other household members continue the study. If guardians drop out of the study and/or withdraw their consent, this will be treated as withdrawing the consent for their wards.		
26. Will the research involve deliberate ***deception*** of participants? **If yes**, justify why deception is used, describe deception and debriefing process, and include debriefing documents in the application. Please also state why Approved Procedure 07 (Deception of adult participants) cannot apply wholly to your project.	Yes	No X
27. By taking part in the research, will participants be at risk of prosecution? **If yes,** justify why incriminating data are sought in the research, and how risks to participants are minimised.	Yes	No X
28. Does your research raise issues relevant to the Counter-Terrorism and Security Act (the Prevent Duty), which seeks to prevent people from being drawn into terrorism? **If yes,** please say how you plan to address any related risks. Please see advice on this on our Best Practice Guidance Web Page.	Yes	No X
29. Will you obtain ***informed consent*** from participants according to CUREC guidelines and good practice in your discipline before participation?	Yes X	No
If yes, please describe the process including whether it is oral (available as an option for applicants to SSH IDREC only) or written; and why, and how long people will have to decide about participation. You should include examples of oral scripts or written forms with your application. See http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/consent. Participants must be informed about, and give specific consent for, any audio recording, video recording, photographs or collection of any other personal or special category (i.e. sensitive) data. **If recruiting children** Note that children have emerging mental capacity and so cannot generally consent to research (except in the case of "Competent Youths"). In this case, you should describe the ways in which parents/guardians will give consent,		

Please also supply age-appropriate information for child participants and assent forms as appropriate to their age and ability to understand the "research contract".

If no, please give a justification for why not.

Copies of consent forms, assent forms, and information sheets have been submitted with this application.

WP1 Understanding socially embedded privacy

Informed consent will be obtained from parents or guardians of participant children before the study, and **assent** will be obtained from every participant child.

During the recruitment, **information sheets** will be provided to parents or legal guardians as well as to children, which brief on the purpose and objectives of the study, and what they will be asked to do. The information sheet for the children will be written at a reading level that is appropriate for their age, supplied with diagrams. In the sheets, parents and children will also be told about how their data will be handled according to the latest General Data Protection Regulation (GDPR), including what personal data will be collected, how it will be stored and anonymised to ensure confidentiality, and their rights to withdraw data from the study (either during or up to one month after the last interview took place).

30. Participant pathway through the research (max 400 words)

Please describe the participant's experience of the research from the point of them having given consent until the end of their involvement with researchers. This would include:

- Number, duration, frequency and type of activities/interventions/investigations
- Any potential risks or actual ill effects of participation e.g. invasive procedures, distress and how these will be minimized
- Implications for disclosure of incidental findings (and see also Section D)
- Who these risks/ill effects may affect e.g. participants, researchers, third parties
- Any reputational risks e.g. to the University

Please also describe any proposed benefits (if applicable)

To support your description please attach documentation such as:

- Recruitment/advertisement material e.g. poster, invitation letter/email, social media advert, website text
- informed consent documents (participant information sheets, consent forms)
- any other forms participants will need to complete e.g. blank questionnaire
- any questions they are asked (e.g. guide to interview questions or a preliminary scope of questions)

Detailed guidance about documentation is found on the CUREC website

Participant experience (split into subgroups if necessary):

Risks:

Benefits:

WP1 Understanding socially embedded privacy

Experience

At least one member of each household is expected to participate in the following activities:

1. Pre-screening using JISC Online Survey (attached study plan) using the following criteria: demographic information on household and all members (gender, age, income, location); wish list of devices (which, when started considering to buy, when planning to buy)
2. Main study phase: For up to 6 months participants will be using smart devices (e.g. Amazon Alexa or Netgear Arlo) in their homes and participate in a series of up to 8 interviews lasting approximately 60-90minutes; participants will be able to contact us with questions or concerns at any time during the study via email, phone, or WhatsApp. Interviews will take place in participant's homes, and we will ask all household members to participate, whenever possible

During the interviews, we will talk about new and old experiences of participants in using and maintaining internet-connected devices in their home. This interview will be audio and video recorded, for later reference, analysis, and transcription. The study will have 4 phases (see attached study plan):

(A) *Introduction* (requires all members of the household in order to obtain consent): We inform about the study schedule and its goals, benefits of participations, ways of interaction, and participants rights. We obtain consent from each adult and children's parents/guardians. We ask children for their assent to participate in the study.

Using our knowledge and the wish list from (1), we initiate a conversation about technology use in the home. We are interested how and where participants make use of their devices. For that purpose we might use home tours, allowing participants to show-case their home and devices. This interview will be audio and video recorded, for later reference, analysis, and transcription.

(B) *Introducing new devices* – After four weeks, households get to choose (worth up to £500) from a pool of selected devices. Devices are left with them to use and to take care of (if they break we might be able to replace them but there is no repercussion for participants) . While they will be tasked with setting up and configuring these devices, we will observe and take notes. Due to time constraints, this process might also take place in several interviews or without our participation, documented by participants themselves. Participants will be asked to video record the process of setting up and configuring devices in this case. We are interested in this process and given that children might be involved or co-present, we need their guardian's consent for the recording. In this context, participants are at liberty to record whatever they deem important. If their children are a part of the process, then it is important for the quality of the data collected that participants can include them in the recordings. **NB**: We will not have access to any accounts or data collected by any of these devices during the course of this study. Installation, configuration, and maintenance are left to participants.

As mentioned in the participant information sheet, guardians might want to limit the recording to the relevant interaction. They might also prefer to not show faces of children, but choose a shoulder surfing perspective

(C) and (D) *Routines and problem solving* – this and any subsequent visits will assume similar form. We will talk to households (unstructured interviews) about their present and past experiences with using their old and new devices. During this process we might again tour their home, following our participants and observing whatever they want to show us. These interactions will predominantly be driven by participants.

3. Wrapping up: We will close the study during our last interview. We will ask participants to voluntarily share their smart device log data with us (e.g. Amazon Alexa voice command logs). Should they choose to do so, we will support them in screening and redacting their data wherever they see fit.

Risks

. The introduction of new devices to the household is not expected to cause any distress, and we will put measures in place to protect all data we collect. That will include anonymising data wherever possible and NOT disclosing any data to a third organisation.

If participants are at unease about being video recorded or video recording, they can opt-out from this recording at any point in time.

The devices we give to participants are 'off-the-shelf'. It will be left to participants to setup and configure these devices using their own accounts and based on their own preferences. Manufacturers and service providers are bound by regulations and laws. They will provide details on their data collection and processing practices in privacy policies, and they will offer privacy settings.

At no point will they be asked to or would they be obliged to install and use any of the devices. It is the process of participants dealing with these devices independently we are interested in. We will make sure that participants at no point will feel pressured in installing or using the devices. We will also choose devices which have good records with respect to privacy, that is no reported malicious/mal-intentioned behaviour.

Benefits

Participants will be given the opportunity to engage with new internet-connected technology in their homes.

innovations. Households might also benefit from sharing experiences with devices, related discussions, and group activities of exploring their benefits.

Given that the study includes up to 8 interviews of ca. 60-90 minutes each over a course of up to 6 months, we separate the study into four phases. Your *household* will be rewarded at the end of each phase. Withdrawal of the whole household during any phase will not lead to deduction of compensations of prior phases. To receive the reward, at least one household member has to complete each phase.

Phase	Interviews	Topic	Reward
A	*Week 0*	Introduction and existing practices	£40
	Week 2		
B	*Week 4*	Introducing new devices	£40
	Week 6		
C	*Week 12*	Routines	£60
	Week 16		
D	*Week 20*	Problem solving and wrapping up	£60
	Week 24		

At the end of the study, you will also be given the option to keep the device you have been using.

Attachments to this application:

WP1 Understanding social embedded privacy

- 110-risk_assessment
- 120-study_plan
- 130-information-sheet-parents
- 140-consent-form-parents
- 145-consent-form-adults
- 150-information-sheet-6-10_years
- 155-information_sheet_11-15_years
- 160-assent-form-under-16s
- 170-poster-recruiting
- 180-email-recruiting
- 190-online survey consent

31. **Management and handling of personal and other research data**

Management and handling of **personal data** and **special category data** of human participants, either directly or via a third party, will need to comply with the requirements of the General Data Protection Regulation (GDPR) and the new Data Protection Act, as set out in the **University's Guidance on Data Protection and Research**. In answering the questions below, please also consider the points raised in the **Data Protection Checklist**. For advice on research data management and security, please consult with the University's Research Data Team (**researchdata@ox.ac.uk)** and/or your local IT department and the University's web pages on research data management.

a. Will your research involve the collection of **records of consent** (e.g. written forms, audio-recorded, or other recorded consent)? **If 'yes', these will be classed as fully identifiable personal data (directly linked to an individual).**	Yes X	No ☐
b. Will your research involve the collection of **other *personal data***? **If 'Yes**', specify in what form(s) this will be stored:	Yes X	No ☐
• Fully identifiable (directly linked to an individual)	Yes X	No ☐
• Pseudonymised (potentially identifiable as data may be attributed to an individual if linkage information can be accessed elsewhere by researchers)	Yes X	No ☐
• Fully anonymised (i.e. cannot be linked to an individual)	Yes X	No ☐
c. Will any of the personal data that you collect classify as *special category data*? **If 'Yes**', specify in what form(s) this will be stored:	Yes ☐	No X
• Fully identifiable (directly linked to an individual)	Yes ☐	No ☐
• Pseudonymised (potentially identifiable as data may be attributed to an individual if linkage information can be accessed elsewhere by researchers)	Yes ☐	No ☐
• Fully anonymised (i.e. cannot be linked to an individual)	Yes ☐	No ☐
d. How will any personally identifiable data be collected, transferred and backed up? Please describe the arrangements for any physical transfer of personal data (including paper records and data captured electronically via portable media) from where it is collected to local storage		

We will use the following services and processes to collect, transfer and backup research data:

- *Voice and video recordings* – collected by either researcher or participants; if collected by researcher, then *transferred to secure digital and physical storage* at the department via cable connection; if collected by participants, then we offer a secure way of sharing that data with the main researcher. The data will subsequently be stored in the department. We will make sure that it is not backed up to any other service, or shared otherwise.
- *JISC Online Survey* (JISC) – for any pre-screening or online survey activity with our participants

  At the Department's suggestion, we will use JISC for online surveys. To comply with GDPR we will sign a Data Processing Agreement (DPA) with JISC. Information collected via online surveys will be downloaded to the researcher's computer and stored securely and backed up using department facilities (see below).
- *Transcript Divas* – Transcription service based in London, UK

  We will use Transcript Divas to transcribe audio recordings from all interviews conducted as part of the project. Transcript Divas are GDPR compliant[1] and offer to sign a confidentiality agreement[2]. We will receive anonymised transcriptions and delete audio recordings at this point. We use a secure connection to transfer data, encrypted and password protected, to Transcript Divas.
- *Secure digital and physical storage* at the department

  Digital personal data on encrypted drives that are physically located in the department and are only accessed by the lead researcher (see below).

  Printed personal data will be stored in a secure locker/cabinet in the department.

  We will anonymise research data to comply with funder requirements.
- *Backup* on department servers

  Personal data will be backed up in encrypted form to external drives which we lock in the department.

  Contact information such as addresses and emails will be managed by the main researcher only and encrypted wherever possible.

e. Where, and for how long, will participants' personally identifiable data be stored during and after the study? (Please outline the procedures for ensuring confidentiality, e.g. security arrangements, anonymisation or pseudonymisation of such data. Please distinguish between records of consent and other forms of personally identifiable data stored. State whether or not you will seek to retain contact details of participants beyond the duration of the study (e.g. for advertising further studies))

[1] https://transcriptdivas.co.uk/transcription-services/academic-transcription-services/

Personal identifiable information will be handled by researchers as follows:

- Consent/assent forms will be collected by researchers at the beginning of the study. These will be on paper and kept for at least 10 years (April 2031) in a secure locker/cabinet in the department (see above).
- Pre-screening/ demographic information will be collected using *BoS* and downloaded to the machine of the lead researcher for that work package and then deleted. This data will be on their machine only..
- Audio recordings will be collected by researchers during interviews using Dictaphones. Recorded data will be stored securely (see digital and physical storage). Audio recordings will be shared with Transcript Divas as above for transcription purposes and immediately deleted after transcription is finished (from our servers and theirs).
    - Audio recordings might also be collected by participants using their mobile phones and transferred to the research through a secure channel, either upload to dedicated folders on Nexus 365 by participants directly or transfer to the researcher through a secure channel. This information, too, will be transcribed and deleted immediately thereafter.
- Video recordings will be collected by researchers . Recordings will not be shared with 3rd parties . All video recordings will be deleted one year after the project finishes (April 2021).
    - Video recordings might also be collected by participants using their mobile phones and transferred to the research through a secure channel, either upload to dedicated folders on Nexus 365 by participants directly or transfer to the researcher through a secure channel.
- Emails and other correspondence will be kept in the main researchers inbox and under their management. This information will be deleted one year after the study finishes (April 2021). Contact information my be kept for future studies with participants' consent.

f. If storing pseudonymised data, please confirm that identifiers will be held separately from the research data and linked through a unique study number. Specify how and at what point the pseudonymisation will occur, how the linkage information will be stored and state whether or not (and when) the linkage will be destroyed.

- Interview transcripts are fully pseudonymised once received from Transcript Divas transcription service

  A unique study number will be assigned to participants by the lead researcher, and linkage information stored separately, encrypted on his local machine. Other researchers will not have access to linkage information. These pseduonymised transcripts will be shared between all researchers on the project.

  This process is relevant for work packages 1, 2, and 3.

g. Who will have access to the personally identifiable data? If personally identifiable data is to be shared with another organisation, how will it be transferred/disclosed securely?

- Access to personally identifiable information will be limited to project researchers. Where possible this will be further limited to the lead researcher of each work package.
- Personally identifiable information will not be shared with sponsors.

h. When and how will personally identifiable data be destroyed? (NB. Personally identifiable data should be destroyed when no longer required).

Participants will be notified via email on deletion of any personal information

- Consent/assent forms: 10 years, or sooner if no longer required by the project (but at least 3 years after the last publication)
- Audio recordings: immediately after transcription
- Video recordings: one year after completion of the project (April 2021)
- Demographic information: one year after completion of the project (April 2021)

At the indicated points in time:

- Digital copies of data will be deleted
- Hard copies of data will be shredded

i. How, where and for how long will other research data be stored after the study has finished? For more information about University and research funder retention policies, please see the University's web pages on research data management.

- Interview transcripts will be kept for at least 10 years (as described above)

32. What are the major ethical issues connected with your research and what steps have you taken to address them?

Please do not answer 'none'. The committee needs to see evidence that you have identified potential ethical issues with respect to your research and have taken steps to address them. These issues could relate to:

- your own physical and psychological safety as a researcher;
- participant burdens and/or risks;
- data protection/confidentiality

For more guidance on ethical issues, please see http://researchsupport.admin.ox.ac.uk/governance/ethics/resources/

Working with children

- Prof Flechais has been designated as the project "Safeguarding Lead" and will work with the University Safeguarding Officers to ensure safeguarding processes are in place and the University's Code of Practice is followed.
- The Safeguarding Lead has carried out a risk assessment (attached) for all members of staff involved in the study and has identified the need for pre-employment/pre-activity checks where in accordance with the University's guidance.
- The Safeguarding Lead will also ensure that members of staff will always be under appropriate supervision.
- Contact of details of the University's Safeguarding Officer and the Safeguarding Lead will be made available to parents and children at the start of the study. The procedure outlined in the University's Safeguarding Code of Practice (Section 4) will be followed to ensure that issues are dealt with in a timely and thorough manner. Any allegations will be reported to the relevant University Safeguarding Officers ***without delay***. Any such allegations that may need onward referral to external agencies will be dealt with within one working day. The Designated Safeguarding Lead will not investigate the matter, and will complete the referral as promptly as possible.
- The Safeguarding Lead will complete the OSCB's (Oxfordshire Safeguarding Children Board) online training on Safeguarding Children in January 2019 (certificate attached).

Research Locations

WP1 Understanding socially embedded privacy

Risks to researchers

Researchers will visit participants' homes to carry out interviews. It is expected that two researchers will attend these visits, although that may not always be possible. Following BPG01 the time and location of these

Code of Practice.

Risks to participants

We do not anticipate any ethical, emotional, physical or political risks to our participants, given that our topic focuses on understanding technology usage patterns. As outlined above, we have ensured that all research staff have received appropriate training, including 1) the use of appropriate research methods, 2) conduct relating to engagement with children, 3) recognition of and dealing with ethical issues, and 4) recognition of and dealing with situations where abuse and/ or serious risk is identified.

Tensions between participants over the use of the internet-connected devices provided to them with may arise. However, interviews in this study are driven by participants rather than researchers, and as a consequence, participants will not be required to talk about topics they are uncomfortable with.

In any case, participants can drop out from the study at any time before or during the last interview as well as withdraw consent for data use up to one month after the last interview, and studies will be stopped immediately if young children show signs of distress or unwillingness to cooperate.

Other participants are equally able to drop out and/or withdrawn from the study at any point.

Data protection

- Recruitment and start of study – pre-screening information (demographics) and consent forms
- During interviews – audio and video recordings

Video recordings in participants homes might be perceived as particularly sensitive. Therefore we will offer participants to opt-out of video recording. Voice recording, however, is mandatory. Our research approach relies on transcripts of conversations as they will take place during our visits. We require a detailed account of this conversations, as our analysis will focus on how households deal with and make sense of technology in their home.

The types of personal data to be collected and why they are needed will be clearly explained to the participants in the information sheets before they joined the study. Participants will be provided with the identity and contact details of the researcher(s) who will determine how the data is processed. Participants will be informed of their rights to withdraw their consent at any time up to one month after the last interview, without giving a reason.

A token will be generated and used to identify all data collected for each participant family, in case they expressed a desire to withdraw from the study. In this way, all data related to the family can be deleted from our hard drive. The token is only accessible to lead researchers.

SECTION C: Research involving secondary use or disclosure of personal data or special category data[1]		
NB This section of the form is only to be completed for research activity (as part or all of a project) where there is no contact with *human participants* (in person or virtual) and no observation of them, but only use of data about them. Your project must meet the standards laid down in the General Data Protection Regulation (GDPR) with respect to the collection, use, and storage of ***personal data*** about ***human participants***.		
33. Will you seek data access agreements for these data?	Yes	No
If yes, • list the individual(s) or organisation(s) from which information will be sourced. • attach a copy of the agreement with the individual(s) or organisations in question. • provide details of any conditions imposed by the organisation(s) concerning the release of the information. **If no**, please explain how and when the agreement of the disclosing organisation(s) will be obtained.		
Individuals / organisations from which data has been sourced: *Any conditions:*		
34. Could these data be linked back to an individual or individuals?	Yes	No
If yes, please explain and describe: • why data cannot be collected in a way which prevents linkage with an individual/individuals • say how individual consent was obtained for the collection, use or disclosure of linkable data **If no** (i.e. you can't link these data back to individuals), continue to question 37.		
Linkage: *Consent for linkable data:*		
35a. How will any personally identifiable data be transferred to you? Please describe the arrangements for any physical transfer of personal data (including paper records and data captured electronically via portable media) from where you are obtaining it from to local storage		
35b. Where, and for how long, will participants' personally identifiable data be stored during and after the study? (Please outline the procedures for ensuring confidentiality, e.g. security arrangements, pseudonymisation of such data)		
35c. Who will have access to the personally identifiable data? If personally identifiable data is to be shared with another organisation, beyond its original source, how will it be transferred/disclosed securely?		
35d. When and how will personally identifiable data be destroyed? (NB. Personally identifiable data should be destroyed when no longer required).		

36. How will the privacy of individuals be respected in any publication arising from this project?

SECTION D: Miscellaneous issues – conflicts of interest, peer review, adverse events and monitoring		
37. Do you or other researchers have a potential or actual *__conflict of interest__* in this project's conduct or outcomes?	Yes	No X
If yes, state nature of conflict (financial or otherwise), and any potential risks arising from this.		
38. Has the project been subject to *__peer review__*?	Yes X	No
If yes, please explain by whom and give outcome. **If no**, explain why not.		
This application has been reviewed by Dr Jun Zhao who is a Senior Researcher at the department and has experience with research involving children. She has provided feedback on the research protocol, to clarify the need of involving children in the study and steps to take to safeguard the well-being and personal privacy of participating children. She also supported the need for such a *field study*, which can provide an in-situ understanding of co-habitants' privacy practices in their daily environment that is lacking in existing literature.		
39. How will the project be **monitored / overseen** and by whom? Please describe monitoring / oversight and reporting arrangements with particular attention to: • student research e.g. supervisory process • ethical issues • adverse events e.g. incidental findings, injury to participants, leaks of data, study protocol breaches.		
This research will be overseen by Principal Investigator Prof. Ivan Flechais and the majority of the work, data collection, will be carried out by DPhil student Martin Kraemer. Prof Max Van Kleek and DPhil student William Seymour will be involved in analysis and dissemination of results. They may occasionally support data collection, that is help with interviews in participants' homes. In his role as PI and safeguarding lead, Prof Flechais will be responsible for appropriate processing of any arising ethical issues or adverse events. Project members are sensitised for related situations and protocols through safeguarding training. As shown in sections related to A31 (a-i) and A32, a variety of research data will be collected (incl. survey results, demographic information, consent forms as well as audio and video recordings). Careful considerations have been given to the handling of personally identifiable research data, and anonymisation and pseudonymization of all research data is in place wherever applicable. Prof. Flechais will monitor the data handling throughout the study process to ensure that all procedures are compliant with the latest GDPR. We have taken careful steps to safeguard data leakage by storing data on a secure and encrypted hard drive within the internal network of the department of computer science. No data will be shared with external organisations. Prof. Flechais will ensure that access to research data will be permitted for the named researchers only and that the study protocol is strictly followed through.		

40. How will you disseminate and feedback project outcomes at the end of the research?

Please describe your plans with respect to participants as well as public dissemination plans, e.g. in journals and conferences.

- To disseminate the findings of our work, WP 4 includes scientific publications to benefit members of the academic community, as well as industry professionals. We will draw on our collaborations with partners (NCSC and others) to help ensure advice to industry is sensitive to commercial contexts and practices (see attached letter of support).
- In work packages 3 and 4, we will work with product and developer groups to reach practitioners who may not be otherwise engaged with academia.
- With the support of the National Cyber Security Centre (see letter of support), our outreach activities will also target policy makers and national cyber security stakeholders.
- WP 4.1 Scientific publications at conference or journals
    - D 4.1.1 - Late breaking work on research intention (CHI 2019)
    - D 4.1.2 - Poster on initial results of WP1 (SOUPS 2019)
    - D 4.1.3 - Disentangling Household's Privacy Practices (CHI 2020)
    - D 4.1.4 - Exploring DPbD With Prototype Smart Things (CHI 2020)
    - D 4.1.5 - Future challenges for DPbD (research paper (published online and submitted to a top-tier academic venue, executive summary delivered at project end)
- WP 4.2 Public engagement activities
    - D 4.2.1 - Outreach activities, e.g. science festivals
    - D 4.2.2 - Oxford University Medium blog post
- WP 4.3 engagement with developer groups
    - D 4.3.1 - IoT London, Developer MeetUp
    - D 4.3.2 - Cyber Cluster Oxford

Section E. Signatures and declarations

You need to obtain handwritten (wet-ink) signatures. Please then scan this entire checklist containing the signatures to create a single PDF document and email through. **Pasted images of signatures cannot be accepted in the sections below.**
If applying to the SSH IDREC, then email confirmation from a University of Oxford email address may also be accepted, provided separate emails are sent from each of the relevant signatories.

41. **Declaration by researchers**

Full project title: Informing the Future of Data Protection by Design and by Default in Smart Homes

I/We, the researcher(s) agree:

- To start this research project only after obtaining approval from IDREC/CUREC;
- To carry out this research project only if funding is adequate to enable it to be carried out according to good research practice and in an ethical manner;
- To provide additional information as requested by IDREC/CUREC before approval is secured and as research progresses;
- To maintain the confidentiality of all data collected from or about project participants;
- To notify IDREC in writing immediately of any proposed change which would increase the risks that any participant is exposed to and await approval before proceeding with the proposed change;
- To notify IDREC if the Principal Investigator on the project changes and supply the name of the successor;
- To notify IDREC in writing within seven days if any serious ***adverse event*** occurs in the course of research;
- To use data collected only for the study for which approval has been given;
- To grant access to data only to authorised persons; and
- To maintain security procedures for the protection of personal data, including (but not restricted to): removal of identifying information from data collection forms and computer files, storage of linkage codes in a locked cabinet and password control for access to identified data on computer files.

Signed by Principal Investigator/supervisor: ……..

Print name (block capitals): …….. **Date**: ……...

Signed by student (for student projects):……

Print name (block capitals): …….. **Date**: ……...

Signed by associate/other researcher:……

Print name (block capitals): …….. **Date**: ……...

Signed by associate/other researcher:……

Print name (block capitals): …….. **Date**: ……...

Signed by associate/other researcher:……

Print name (block capitals): …….. **Date**: ……...

/Section E (continued)

Section E (continued). Signatures and declarations

42. Certification by *Principal Investigator*/supervisor and head of department

Full project title:	Informing the Future of Data Protection by Design and by Default in Smart Homes

Certification by *Principal Investigator*/supervisor

- I accept responsibility for the conduct of this research project.
- I certify that all researchers and other personnel involved in this project are appropriately qualified and experienced or will undergo appropriate training to fulfil their role in this project.

Signed by ***Principal Investigator*/supervisor**:
……..

Print name (block capitals): …….. **Date**: ……

43. Acceptance by head of department (or other senior member of the department if the Principal Investigator is the head of department)

- I have read the research project application named above.
- On the basis of the information available to me, I judge the ***Principal Investigator***/supervisor and ***student researcher*** (if applicable) to be aware of their ethical responsibilities in regard to this research.
- I am satisfied that the proposed project has been/will be subject to appropriate peer review and is likely to contribute to existing knowledge and/or to the education and training of the researcher(s) and that it is in the public interest.

Signed by head of department/faculty or nominee: ……..

(example nominees include Chair of DREC, or, for student projects, Director of Graduate Studies / Undergraduate Studies)

Print name (block capitals): …….. **Date**: ……

SECTION F: Final check

Please use this section to check that you have completed the following tasks:	**Please type 'X'**
Have you completed all questions in Sections A, B, D & E? And, if using personal data obtained from a secondary source, section C?	X
Have you included copies of any documentation produced in support of your application? **If the appropriate supporting documentation is not included with your application, you will then be asked to provide this separately. This may well delay the ethical review process, and thus the start of your research.**	X
Have you included copies of data access agreements with third parties (see Section C, question 33) if appropriate?	X
Have you included debriefing documents for projects involving deliberate deception?	
Have you checked that all documents for participants are clear and easy to read (pilot-testing with lay readers, or using reading-age checking software as appropriate)?	X
Have you signed as Principal Investigator and gathered signatures of the student (for student research) and department nominees as appropriate?	X
Have you declared conflicts of interest (if any)? (See Question D37)	X
Are all pages (including supporting document attachments) numbered?	X

Have you defined all technical terms and abbreviations used?	X
Have you obtained all necessary departmental approvals for this project to proceed?	X

SOCIAL SCIENCES & HUMANITIES
INTERDIVISIONAL RESEARCH ETHICS COMMITTEE

Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD
Tel: +44(0)1865 616576 Fax: +44(0)1865 280467
ethics@socsci.ox.ac.uk

29 March 2019

Professor Ivan Flechais
Department of Computer Science
University of Oxford

Dear Professor Flechais,

Research Ethics Approval (CUREC 2)
Ref No: R59140/RE001
Title: Informing the Future of Data Protection by Design and by Default in Smart Homes

The above application has been considered on behalf of the Social Sciences and Humanities Interdivisional Research Ethics Committee (IDREC) in accordance with the procedures laid down by the University for ethical approval of all research involving human participants.

I am pleased to inform you that, on the basis of the information provided to the IDREC, the proposed research has been judged as meeting appropriate ethical standards, and accordingly approval has been granted.

Should there be any subsequent changes to the project, which raise ethical issues not covered in the original application, you should submit details to the IDREC for consideration.

Please note that you may be required to submit an annual progress report on each anniversary of study approval, until the study is completed, and that your study may be selected for review by the SSH IDREC during an annual audit. External funders may also request ethics audits of any studies they have funded.

Yours sincerely,

Claudia Kozeny-Pelling
Research Ethics Manager and Secretary SSH IDREC

cc: Professor Max Van Kleek, William Seymour, Martin Kraemer, Sharon Lloyd

B.3 Recruitment Advertising Page

HOME > FIND RESEARCH > STUDY OVERVIEW

Informing The Future of Smart Homes

28 October 2020

The Internet of Things brings a manifold of different devices to our homes. We use smart voice assistants to play music, ask for the weather, and order things online; we use smart TVs for entertainment; our kids use smart toys, have their own tablets, and mobile phones; we might secure our home with cameras and motion sensors.

We are interested in how you as a household might be using such devices, even if you don't own any yet! We will get them for you. Get in touch!

Requirements

- One person per participating household should be familiar with the use of smart phones and mobile apps in general.
- We are targeting mainly 'nuclear' families (partners living with kids) but are also interested in other household arrangements.
- Your children are invited to participate in the study but need to be 6 years or older.
- Your family home should be somewhere in or close to Oxford.

☐ YES, I MEET THESE REQUIREMENTS

TAKE PART IN THIS STUDY

Keywords

University of Oxford | Social Internet of Things; | data privacy | IoT Usability;

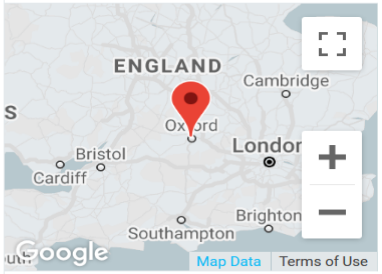
Ethical approval

ACADEMIC STUDY

STUDY ESSENTIALS

- University of Oxford, GB
- 6 month(s) to complete
- financial reward
- Ethnographic Study

STUDY LOCATION



SHARE THIS STUDY

- Facebook
- Twitter
- LinkedIn
- Reddit
- Pinterest
- Email this study
- Print a poster version (PDF)

B.4 Recruitment Information Web Page

DEPARTMENT OF COMPUTER SCIENCE

PI: Prof Ivan Flechais – Ivan.flechais@cs.ox.ac.uk
Co-I: Prof Max Van Kleek – max.van.kleek@cs.ox.ac.uk

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD UK

Ethics approval: R59140/RE001

Participants wanted!

Does your household include two or more adults?
Have you been living at your current address in Oxford or proximity for more than one year?
Are most people in your household smart phone users?
Would you like to participate in research on smart homes?

Apply now!

Who?

We are looking for two or more person households in Oxford and proximity (including children above the age of six). The majority of householders should be smart phone users, e.g. they should now how to take a picture and send that to someone else. You should be living at your current address for at least one year.

If you are a university employee and interested in supporting our research on smart homes, please get in touch with Martin (martin.kraemer@cs.ox.ac.uk) directly.

How does it work?

We would like to schedule a series of visits (max 1.5hrs each) to your home over the course of up to 6 months (no more than bi-weekly). During our visits we would like to talk to you about experiences with internet connected devices you use in your home, and at some point, we will offer you to choose from a new set of devices. In the meantime, we ask each household member to maintain a diary of experiences, thoughts, and feelings with regards to using the devices.
[more ...]

Will I get paid?

You will receive a monetary reward, and you may keep the devices we are giving you.

What data will be collected?

We will audio record our conversations. You may also be asked to maintain a diary using a mobile app we provide or another method we can discuss, and we would ask you to video record the installation/use of the devices yourself. We would like to relate to your experiences as much as possible, which video recording will enable us to do more easily.
[more ...]

Who is behind this?

This study is part of our research on the Future of Data Protection by Design and by Default in Smart Homes project. The project was approved by the Central University Research Ethics Committee under reference number R59140/RE001. For any quesitons, please get in touch with Martin Kraemer or Ivan Flechais.

How can I take part?

We are now recruiting for this study. If you'd like to register your household for this study, please follow the application process.

What are we trying to find out?

The Internet-of-Things has long arrived in our homes. A variety of devices offers to use internet-connected (smart) technology for numerous purposes including housekeeping, entertainment, fitness-tracking, organising, and safe-guarding. We are interested in how households organise the use of 'smart' devices as part of their daily routine. This includes your experience as much as the perspective of all other people in your household.
[more...]

Application Process

What's next? - If you are interested in participating, please follow the application process.

1. Apply now!
   Please submit the pre-screening questionnaire.
2. A first check with our eligibility parameters takes place, and you'll be informed about the outcome.
3. After this, we might arrange for a face-to-face interview.
4. We will communicate our decision within one week after the interview.

Please appreciate, that we have to meet the recruiting criteria detailed on the left, and that spaces are limited.

Contact

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD UK

Ethics approval: R59140/RE001

Lead Researcher:
Martin Kraemer - martin.kraemer@cs.ox.ac.uk - 01865-986331

Principal Investigators:
Prof Ivan Flechais
Prof Max Van Kleek

B.5 Pre-Screening Survey

Informing the Future of Smart Homes

Welcome!

Thanks for your interest in our study. This survey will ask you a few questions about yourself, your household, and the smart / internet-connected technology you might already be using. We will use this information to determine your eligibility for the study.

Please read all questions carefully and provide information as accurately as possible.

Participant Consent

Ethics Approval Reference: R59140/RE001

General Information

The Internet-of-Things has long arrived in our homes. A variety of devices offers to use internet-connected (smart) technology for numerous purposes including housekeeping, entertainment, fitness-tracking, organising, and safe-guarding. We are interested in how households organise the use of smart devices such as voice assistants, thermostats, and other devices as part of their daily routine.

You are invited to fill in this survey on behalf of your household because you expressed interest in our study. Please consult your household members before filling in this survey. On behalf of your household, you are invited to fill in this survey because you expressed general interest in the study. The survey allows us to better understand if your household would be a good fit for our study. Please appreciate that we can only accept 8 households for participation.

The information will only be used for this purpose and accessed by the principal researchers: Martin Kraemer and Ivan Flechais (contact details below).

Do I have to take part?

Please note that your participation in this pre-screening survey is voluntary. You may withdraw at any point during the questionnaire for any reason, before submitting your answers, by pressing the 'Exit' button / closing the browser. However, we are only able to consider households for participation who finish the survey and provide accurate information.

How will your data be used?

This is a pre-screening survey which will help us to select households for our study. Please answer the questions accurately and truthfully.

Your data here is pseudonomysed, that is the unique token you received via email is only known to the main researcher.

We will minimise our use of personal data in the study as much as possible, and we will use all reasonable endeavours to keep them confidential, during collection and processing of data.
For data collection, we use Jisc Onlinesurveys to run the survey. We will receive personal data from both as detailed below.

- We use Jisc Onlinesruveys to run the survey (privacy policy). Compliant with the General Data Protection Regulation. We collect the following personal data as part of the survey:
    - **pseudonyms** for people in your household, age range, and gender identity.

After data collection, you data will be fully deleted from Jisc Onlinesurveys. Your data will be stored fully encrypted within the Department of Computer Science. It may be used in academic publications. Your IP address will not be stored. All questions are optional and we have included a 'Prefer not to say' option for each set of questions if you prefer not to answer a particular question. All research data and records will be stored for a minimum retention period of 10 years after publication or public release of the work of the research.

The data that we collect from you will NOT be transferred to, and stored or processed at, a destination outside the European Economic Area ("EEA").

Who will have access to your data?

Jisc Onlinesurves and the University of Oxford are the data controllers for the purposes of the Data Protection Act 2018. The University will process your personal data for the purpose of the research outlined above. Research is a task that we perform in the public interest.

Responsible members of the University of Oxford, funders may be given access to data for monitoring and/or audit of the study to ensure we are complying with guidelines, or as otherwise required by law.

The principal researcher is Martin Kraemer, who is attached to the Department of Computer Science at the University of Oxford. This project is being completed under the supervision of Ivan Flechais.

This project has been reviewed by, and received ethics clearance through, the University of Oxford Central University Research Ethics Committee (Ref: R59140/RE001).

What if there is a problem?

If you have a concern about any aspect of this study please contact Mr. Martin Kraemer (martin.kraemer@cs.ox.ac.uk) or Ivan Flechais (Principal Investigator - ivan.flechais@cs.ox.ac.uk), who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Research Ethics Committee at the University of Oxford who will seek to resolve the matter in a reasonably expeditious manner:

Chair, Social Sciences & Humanities Interdivisional Research Ethics Committee; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD

The Chair will seek to resolve the matter in a reasonably expeditious manner.

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started. ✱ *Required*

- ○ Yes, I agree to take part
- ○ No, I do not agree with the terms

Please note that you may only participate in this survey if you are 18 years of age or over. ✱ *Required*

- ○ I certify that I am 18 years of age or over.

Your unique reference (provided via email) ✱ *Required*

[ ]

Household Information

Please provide information on all persons in your household

	pseudonym (nickname) *Optional*	age *Optional*	gender *Optional*	highest level of education *Optional*	skills with smart devices *Optional*	profe
person 1		Please select	Please select	Please select	Please select	
person 2		Please select	Please select	Please select	Please select	
person 3		Please select	Please select	Please select	Please select	
person 4		Please select	Please select	Please select	Please select	
person 5		Please select	Please select	Please select	Please select	
person 6		Please select	Please select	Please select	Please select	
person 7		Please select	Please select	Please select	Please select	
person 8		Please select	Please select	Please select	Please select	
person 9		Please select	Please select	Please select	Please select	

total household income ✱ *Required*

post code ✱ *Required*

Internet-Connected Technology

Which internet-connected devices does your household own and who uses them? Think of your computers, smart phones, fitness trackers, TVs, Amazon Alexa, and so on ✱ *Required*

Do you intend to purchase any other devices in the near future? If so, which, why, and when? ✱ *Required*

Have you heard of any other internet-connected (smart) devices that you thought were interesting? ✱ *Required*

Administrative

Do you have any travel longer than 2 weeks planned (including all your household)? ✱ *Required*

Why would you like to participate in this study? ✱ *Required*

Not consent

Seems like you do not consent to our way of collecting and dealing with your data. Please share your concerns with us at martin.kraemer@cs.ox.ac.uk

Final page

Thank you for filling in the survey. We will be in touch within two weeks. If you have any questions, please email us at martin.kraemer@cs.ox.ac.uk

---

Key for selection options

4.1.b - age
- <18
- 18-34
- 35-64
- 65+

4.1.c - gender
- male
- female
- prefer not to disclose

4.1.d - highest level of education
- no school completed
- Nursery
- High School
- Trade/technical/vocational training
- Undergraduate studies
- Postgraduate studies

4.1.e - skills with smart devices
- novice
- competent
- expert

4.2.b - age
- <18
- 18-34
- 35-64
- 65+

4.2.c - gender
- male
- female
- prefer not to disclose

4.2.d - highest level of education
- no school completed
- Nursery
- High School
- Trade/technical/vocational training
- Undergraduate studies
- Postgraduate studies

4.2.e - skills with smart devices
- novice
- competent
- expert

4.3.b - age
- <18
- 18-34
- 35-64

65+

4.3.c - gender
male
female
prefer not to disclose

4.3.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training
Undergraduate studies
Postgraduate studies

4.3.e - skills with smart devices
novice
competent
expert

4.4.b - age
<18
18-34
35-64
65+

4.4.c - gender
male
female
prefer not to disclose

4.4.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training
Undergraduate studies
Postgraduate studies

4.4.e - skills with smart devices
novice
competent
expert

4.5.b - age
<18
18-34
35-64
65+

4.5.c - gender
male
female
prefer not to disclose

4.5.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training

Undergraduate studies
Postgraduate studies

4.5.e - skills with smart devices
novice
competent
expert

4.6.b - age
<18
18-34
35-64
65+

4.6.c - gender
male
female
prefer not to disclose

4.6.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training
Undergraduate studies
Postgraduate studies

4.6.e - skills with smart devices
novice
competent
expert

4.7.b - age
<18
18-34
35-64
65+

4.7.c - gender
male
female
prefer not to disclose

4.7.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training
Undergraduate studies
Postgraduate studies

4.7.e - skills with smart devices
novice
competent
expert

4.8.b - age
<18
18-34
35-64

65+

4.8.c - gender
male
female
prefer not to disclose

4.8.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training
Undergraduate studies
Postgraduate studies

4.8.e - skills with smart devices
novice
competent
expert

4.9.b - age
<18
18-34
35-64
65+

4.9.c - gender
male
female
prefer not to disclose

4.9.d - highest level of education
no school completed
Nursery
High School
Trade/technical/vocational training
Undergraduate studies
Postgraduate studies

4.9.e - skills with smart devices
novice
competent
expert

5 - total household income
less than £10,000
£10,001 – £20,000
£20,001 – £30,000
£30,001 – £40,000
£40,001 – £50,000
£50,001 – £60,000
£60,001 – £70,000
£70,001 – £80,000
£80,001 – £90,000
£90,001 – £100,000
£100,001 – £150,000
more than £150,000

B.6 Participant Information Sheets

DEPARTMENT OF
COMPUTER
SCIENCE

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD UK

Ethics approval: R59140/RE001

PI: Prof Ivan Flechais – Ivan.flechais@cs.ox.ac.uk
Co-I: Prof Max Van Kleek – max.van.kleek@cs.ox.ac.uk

Informing The Future of Smart Homes

INFORMATION SHEET FOR PARENTS / GUARDIANS/ADULTS

Oxford University's Ethics Approval Reference: R59140/RE001

We are researchers from the Department of Computer Science at Oxford University and would like to invite your household to be part of a new research study. You will be offered smart home devices for use in your home, and we will be interested to see how you organise the configuration, setup, and use of these devices in your household. Before deciding whether you want to take part, we think it is important that you understand **why** the study is being done and what it involves.

this paragraph only applies if there are children in the household
If there are any children (6 years or older) in your household, they will also be able to participate in this research. You will be asked to provide consent for them, and they will be asked to assent to participation. If, at any point, you should wish for your child or your child should wish to drop out, there are NO consequences for other household members participating in the study. If you (for your child) or your child should also wish to withdraw consent for data usage, we will delete / redact all data we have collected on your child. Please appreciate, that your child (under the age of 16) cannot continue with the study if you yourself should wish to stop.

After reading this information sheet, if there is anything that is not clear or you would like more information, please do not hesitate to contact the research team:

- Lead Researcher: Martin Kraemer
- Researchers: William Seymour, Dr. Helena Webb
- Principal Investigator: Prof Ivan Flechais, Prof Max Van Kleek

What are we trying to find out?

The Internet-of-Things has long arrived in our homes. A variety of devices offers to use internet-connected (smart) technology for numerous purposes including housekeeping, entertainment, fitness-tracking, organising, and safe-guarding. We are interested in how households organise the use of 'smart' devices as part of their daily routine. This includes your experience as much as the perspective of all other people in your household.

You might or might not already own 'smart' devices such as your smart phone, a fitness tracker, or a virtual assistant (e.g. Amazon Alexa) and either way is fine. As part of the study, you will be offered a range of devices (e.g. virtual assistants, security cameras, door bells/locks, and others) for use in your home. You may choose any number we offer but at least one device. We will be interest to learn how you start using these devices and ask you to share your perspective in so doing.

The findings of this study will contribute to our efforts into "Informing The Future of Smart Homes". More information about the project is available on our website (http://users.ox.ac.uk/~lina3008/) and can be obtained by contacting the research team named above.

Why have I been invited to take part?

You are invited because you indicated your household would be interested in taking part in the study. You are also expected to be familiar with using internet-connected devices in general including any of smart phone, tablet, or computer. Overall we are inviting 6-8 households to take part in the study.

Do I have to take part?

It is not compulsory to take part, and you can ask questions about the study before deciding whether or not to participate, using the contact details provided. If you agree to take part, we will then ask you and everyone else in your household to sign a consent form. You, as an individual and any other member of your household individually, may **withdraw from the study at any time before or during our last interview**, without giving a reason. If, up to one month after the last interview, you decide that you want us to remove your responses, you can contact us and ask us to delete them.

Given that the study includes up to 8 interviews of ca. 60-90 minutes each over the course of 6 months, we separate the study into four phases. Your *household* will be rewarded at the end of each phase. Withdrawal of the whole household during any phase will not lead to deduction of compensations of prior phases. To receive the reward, at least one household member has to complete each phase.

Phase	Interviews	Topic	Reward
A	*Week 0*	Introduction and existing practices	£40
	Week 2		
B	*Week 4*	Introducing new devices	£40
	Week 6		
C	*Week 12*	Routines	£60
	Week 16		
D	*Week 20*	Problem solving and wrapping up	£60
	Week 24		

What will happen if I take part?

If you agree to take part in the study, then the following will take place:

Pre-survey: Please access our pre-study survey which we use to determine your eligibility for this study.

Subsequent study phases will involve the following visits (each lasting 60-90 minutes):

(A) Introduction and existing practices: We (the researchers) will coordinate a first meeting at your home *or any other place you might prefer* ***with you and all other household members***. We use this meeting to get to know you and your household while taking care of administrative requirements. Our conversation will also touch on existing smart (internet-connected) devices you already own, and we are interested to learn more about your intentions to obtain new devices.

(B) Introducing new devices: We will schedule a convenient date and time for us to visit your home and will bring new smart devices with us. We will leave setup and configuration of these devices to you and your household while we will keep in the background. We will encourage participation of all household members.

(C) Routines: During these visits we will be keen to learn about how you got along with the new

devices, that is how you as a household are using them. We will ask you to share your experiences to this point. The conversation will be casual and informal, unlike other research interviews you might have participated in. We will strongly encourage participation by all household members.

(D) Problem solving and wrapping up: These visits to your home will follow a scheme very similar to *(C) Routines*. Our conversations will be casual and informal. Again, we will want to learn about your experiences with using the devices but also any challenges you might be facing.
We will use our last visit to wrap up the study, and will be happy to address any questions or issues you might have at that point in time.

We will encourage participation of all household members in all interviews. We appreciate this might not always be possible and will be happy to talk to whoever is available. However, we cannot talk to children below the age of 16 without any adult being present.

A number of different types of data will be collected at different stages of the study, including the following:

- The pre-survey (online) will collect some demographic information about you, such as the number of children in your household or the age range of parents/guardians. The survey will ask about information on smart (internet-connected) devices you own already and also ask about more general information on your household.
- At the beginning of the study a physical copy of a participant consent form will be collected.
- During the visits to your household we only collect data through **audio recordings** and **video recordings** (optional). Our research benefits from details, and these details can best be captured using recording. Although we would prefer video recordings over audio recordings, you will have the opportunity to opt-out of video recording. However, we require audio recordings for our work. The recordings are anonymised and transcribed so that we can use them during our analysis. We require a level of detail for the analysis only audio recordings can give us. You may voluntarily share any device logs at the end of the study. If you choose to do so we will support you in screening and redacting them wherever you see fit. – We will **NOT** collect any data from any devices we provide you with during the study.
- At any point during the study, you are invited to share thoughts and comments in form of video or audio recordings with us. We will provide you with information on how to do that in a safe and secure way. We are interested in your and your household's experiences with using the devices. You might want to include other household members in your pictures, comments, and videos. We suggest to be mindful when including your children, limiting the recording where possible. For example, you could show your child using a device without showing their face, and you might want to limit this time-wise.
- We will also ask you to keep some form of diary to log your thoughts, experiences, and feelings when using the devices. To keep the diary, you can use a mobile app we will be offering.

All data collected in the study will be kept on our secure server and confidential as specified below. All audio recordings will be transcribed by an external transcription service (which will have signed a confidentiality agreement) in order to facilitate our data analysis.

What are the possible disadvantages or risks of taking part?

We will have mechanisms in place to ensure that information collected during the study will be made anonymous, and not be disclosed to anyone besides the research team. If any risks become known during the research, you will be informed straight away.

Whatever you choose to do with any of the devices is up to you. You will be asked to setup and configure the devices you choose as you wish. We do not have any requirements for you. You may choose to make any configuration or any other change at any time (including stopping using them). You will be using your own accounts and settings, and you will be managing these devices as a household.

What are the advantages of taking part?

You are given the opportunity to engage with new and innovative internet-connected technology in their homes. Together with others in your household, you can experience and discuss the use of these devices.

At the end of the study, you will also be given the option to keep the device you have been using.

What happens to the results of the study?

The audio files collected in the study will be transcribed using an external transcription service with which we have appropriate data protection agreements in place. All personally identifiable information (such as names or places) will be removed from the transcriptions as they are collected. The recordings will then be destroyed. We use transcripts and video recordings (if video recordings are available) for our analysis. Video recordings will be deleted one year after completion of the project (April 2021) at which point you will be notified.

The resulting anonymised data will be stored on Oxford University's data storage facilities, secured by the IT department. All consent and assent forms obtained for the study will be locked in a secure locker in the university office. Access to these items will be limited to members of the project team directly involved in the study.

The research results will be disseminated as public reports, technical reports, as well as academic publications. We will ask all participants for their permission to use anonymous quotes.

The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, it has established an online archive of research materials. All journal articles and conference papers (in publications with an ISSN) published by Oxford researchers will be deposited in the Oxford University Research Archive (ORA) within three months of acceptance for publication. The archive is openly accessible to every internet user.

Contact information will be deleted one year after the project finishes (in April 2021), unless you have given us consent to contact you for future studies. Demographic information and video recordings will be deleted one year after the project finishes (in April 2021). Audio recordings are deleted immediately after transcription.

As requested by our research funding agency (EPSRC UK), all research data (interview transcripts) will be stored for a minimum retention period of 10 years after publication or public release of the work of the research (until April 2031). Data will only be transferred across the research team through password-protected university systems or the handover of a non-networked encrypted hard drive. The data that we collect from you will NOT be transferred to, and stored or processed at, a destination outside the European

Economic Area ("EEA"). All personally identifiable data will be protected under the General Data Protection Regulation, including post-Brexit.

Data Protection

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study. The University will process your personal data for the purpose of the research outlined above. Research is a task that we perform in the public interest. Further information about your rights with respect to your personal data is available from http://www.admin.ox.ac.uk/councilsec/compliance/gdpr/individualrights/.

Who is conducting this research?

The research project is organised by Prof Flechais of Oxford University, who is an Associate Professor at the Department of Computer Science. The research is funded by an ICO Research Grant and through the EPSRC UK in form of PhD studentships. The project will be carried out by Professors Flechais and Van Kleek, and DPhil students William Seymour and Martin Kraemer. This study has been reviewed by, and received ethics clearance through, the Research Ethics Committee at the Department of Computer Science at the University of Oxford, R59140/RE001.

What if there is a problem?

If you have any concern about any aspect of this project, please speak to the relevant researcher (Martin Kraemer; 01865-986331; martin.kraemer@cs.ox.ac.uk;) or their supervisor (Prof Flechais; ivan.flechais@cs.ox.ac.uk) who will do their best to answer your query. The researcher should acknowledge your concern within 10 working days and give you an indication of how they intend to deal with it. If you remain unhappy or wish to make a formal complaint, please contact the Chair of the Research Ethics Committee at the University of Oxford, who will seek to resolve the matter in a reasonably expeditious manner.

Chair, **Social Sciences & Humanities Inter-Divisional Research Ethics Committee**;
Email: ethics@socsci.ox.ac.uk;
Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD

What should I do next?

If **you and all of** your household are happy to take part in the study, please fill in the enclosed consent form, and an online poll to express your availability. Please remember that you may drop out of the study before or during the last interview, without penalty and without giving a reason, by notifying the researcher. You may also withdraw consent to use your data up to one month after the last interview. If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

Prof Ivan Flechais
Department of Computer Science
University of Oxford
Wolfson Building.
Parks Road. Oxford. OX1 3QD
Email: ivan.flechais@cs.ox.ac.uk

DEPARTMENT OF
COMPUTER
SCIENCE

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD UK

Ethics approval: R59140/RE001

PI: Prof Ivan Flechais – Ivan.flechais@cs.ox.ac.uk
Co-I: Prof Max Van Kleek – max.van.kleek@cs.ox.ac.uk

Informing the Future of Smart Homes

INFORMATION SHEET FOR YOUNG PEOPLE AGED 11 TO 15 YEARS

Ethics Approval Reference: R59140/RE001

We are inviting you to join in a research study. Our names are Martin and Ivan, and we work at the University of Oxford in the Department of Computer Science.
Before you decide if you would like to join in, it's important to understand what the study is about, why we're doing it and what it would involve for you. Please read and think about this leaflet carefully. Please feel free to talk to your family, friends, or the researchers about it if you want.
If anything isn't clear or you have more questions you can ask your parents/carer to give us a call and we can discuss it with you and your parents/carer.

Why are we doing this research?
Imagine your family has a living room where the only television in the house is located. If you wanted to use it, you would need to talk to your parents (and siblings). They might want to use it as well, and you find a compromise that somehow works for all of you.

Finding such a compromise isn't always straight forward and might be different for, let's say, a smart voice assistant to which you can talk and which can search the internet or play music for you. That is what we are interested in. How do you find a compromise for something like Alexa?

Why have I been invited to take part?
We invited your parents to take part in this research, and now we would also like to ask you. In total, we are inviting 8 households to participate.

Do I have to take part?
No - It is up to you. We will ask you to sign a form to say that you agree to take part (an assent form). We will give you a copy of this information sheet and your signed form to keep. You are free to stop taking part at any time during the research without giving a reason, by telling the researcher. If you decide to stop, we will not use the information we have already collected from you. The rest of your family can continue the study even without you.

What will happen to me if I take part?

If you want to take part, we will ask you to join our conversations with your parents. You can comment on your experiences and anything on using these new devices when we come to your home. We are happy to listen to whatever you want to say. We will do this about 8 times over a period of up to 6 months. Each visit would last about 60-90 minutes but you don't need to be there all of the time. We will record and write up what we talk about to use it for our research.
We audio record our conversation and also would like to video record them. Our research benefits from details, and these details can best be captured using recording. The recording will be typed up for our analysis. If you don't want to be video recorded, that's fine. We can do without it. Unfortunately, we cannot work without audio recording.

What happens to the results of the study?
Results for each young person taking part are kept strictly confidential. Only a number will be used to identify you, and all information and results are kept in a secure location in the University.

The research will be written up as part of a student's work. We also aim to publish our findings in scientific journals.

All research data (interview transcripts) will be stored for a minimum retention period of 10 years after publication or public release of the work of the research. Third parties may be given access to research data for monitoring and/or audit of the study, or for data storage purposes.
All other data (demographic information, audio and video recordings) will be deleted within one year after completion of the project (by April 2021).

Will anyone else know I'm doing this?
We will keep your information private. This means we will only tell those who have a need or right to know, such as the research team and your parents/carer. We will only share information that has your name and address removed.

What if I don't want to take part in the research anymore?
Just tell your parents/carer and the people carrying out the research that you don't want to take part. You don't have to give a reason and no one will be annoyed with you. It is YOUR choice. You can let us or them know at any point in time during the study or up to one month after our last interview.

Who is organising and funding the research?
The research is organised by Prof Ivan Flechais of Oxford University, who is a Associate Professor. The study is being paid for by the Information Commissioner's Office (ICO) and EPSRC.

Who has reviewed the study?
Before any research involving people can start, it has to be checked by a Research Ethics Committee to make sure that it is OK for the research to go ahead. This study has been approved by the University of Oxford Central University Research Ethics Committee.

What if there is a problem or something goes wrong?

Please tell us if you are worried about any part of this study, by contacting the researcher (ivan.flechais@cs.ox.ac.uk). You may also talk to your teacher/parent/carer who will let the researcher know. If you are still unhappy or wish to make a complaint, either you or your parent(s) can contact the chair of the Research Ethics Committee at the University of Oxford (Chair, Social Sciences and Humanities Inter-Divisional Research Ethics Committee; Email: ethics@socsci.ox.ac.uk; Address: Research Services, University of Oxford, Wellington Square, Oxford OX1 2JD).

Data Protection

The University of Oxford is the data controller with respect to your personal data, and as such will determine how your personal data is used in the study. The University will process your personal data for the purpose of the research outlined above. Research is a task that we perform in the public interest.
Further information about your rights with respect to your personal data is available from http://www.admin.ox.ac.uk/councilsec/compliance/gdpr/individualrights/.

Contact details

If you would like to discuss the research with someone beforehand (or if you have questions afterwards), please contact:

Prof Ivan Flechais
Department of Computer Science
University of Oxford
Wolfson Building.
Parks Road. Oxford. OX1 3QD
Email: ivan.flechais@cs.ox.ac.uk

Thank you for reading this – please ask any questions if you need to.

DEPARTMENT OF
COMPUTER
SCIENCE

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD UK

Ethics approval: R59140/RE001

PI: Prof Ivan Flechais – Ivan.flechais@cs.ox.ac.uk
Co-I: Prof Max Van Kleek – max.van.kleek@cs.ox.ac.uk

Informing the Future of Smart Homes

INFORMATION SHEET FOR YOUNG CHILDREN

TO BE READ WITH THE CHILD BY A PARENT/CARER

Oxford University's Ethics Approval Reference: R59140/RE001

Hello!

Hello! My name is Martin and I work at the University of Oxford. This spring I am doing some research and would like you and your parent to join in.

We'd like to ask you about something like smartphones or Amazon Alexa or the Roomba vacuum cleaner. Maybe you have heard about them, or you have even used them before?

Together with your parents, you will have the chance to use them. All we would like to know is how you like them 😊

You don’t have to join in if you don’t want to! And you can change your mind whenever you like, and you don’t have to say why.

If you decided to stop,

no one will be upset with you!

What will happen?

1. We will come to your home to meet you and learn about existing devices.

2. We will provide you with some new devices.

3. We will visit you over the next few months to see how you get along with these devices.

Picture are from pexels.com

Things you can do

 talk to your parents about using Alexa (voice assistant) and other devices

 explore how you could use them for yourself

 get an idea of how they can be connected to each other

We will audio record you during our visits only and we would also like to video record you and your family if all of you are happy with this. You may also be asked to video record how the devices are being used. But we don't have any access to the devices we give to you.

We use these recordings to understand how you are using these devices. You can say no to being video recorded!

We hope you will enjoy using the devices and taking part in the study. We hope this will allow us to create some new insights so that we can help other people with their use of technology.

We won't use your name in any of our work. And everything you tell us will be kept in a safe place.
The University we work for has checked everything we're doing is ok. But if something bothers you, or makes you upset, please tell us or your parent/carer and we can do something to make it better.

Contact: Martin Kraemer, 01865-986331

B.7 Researcher Study Dashboard

Informing the Future of Smart Homes

Household 1

today: 28/10/2020
Start: 14/07/2019 | End: 04/01/2020 (expected) – actual: 05/02/2020

phase	week	meeting
(A) Introduction	0	19/07/2019
	2	30/07/2019
	3	09/08/2019
reward #1	4	confirmed (27/09/2019)
(B) New devices	6	29/08/2019
	8	12/09/2019
reward #2	12	authorised (08/10/2019)
	12	11/10/2019
(B) Routines	16	05/11/2019
reward #3	20	authorised (07/01/2020)
(C) Problem solving	20	10/12/2019
(D) Wrapping up	26	19/01/2020, 11am
reward #4	24	authorised (07/01/2020)
Closing	29	05/02/2020, 7pm
FINISHED	29	

Household 2

today: 28/10/2020
Start: 29/07/2019 | End: 18/01/2020 (expected) – actual: 28/01/2020

phase	week	visit
(A) Introduction	0	01/08/2019
	2	13/08/2019
reward #1	4	authorised (25/09/2019)
	5	03/09/2019
(B) New devices	10	10/10/2019
reward #2	12	authorised (06/11/2019)
	14	07/11/2019, 5.30pm
(B) Routines	18	16/12/2019, 5.45pm
reward #3	20	confirmed (20/01/2020)
(C) Problem solving	23	10/01/2020, 5.15pm
reward #4	24	confirmed (20/02/2020)
(D) Wrapping up	26	28/01/2020, 5.20pm
FINISHED	26	

Household 3

today: 28/10/2020
Start: 01/09/2019 | End: 22/02/2020 (expected) – actual: 27/02/2020

phase	week	meeting
(A) Introduction	0	01/09/2019, 10am
	2	14/09/2019, 9.30am
reward #1	4	confirmed (06/11/2019)
	4	05/10/2019, 12pm
(B) New devices	11	23/11/2019, 11am
reward #2	12	authorised (25/11/2019)
	13	14/12/2019, 10am
	18	11/01/2019, 11am
reward #3	20	confirmed (20/02/2020)
(B) Routines -- devices II	20	25/01/2020, 10am
(C) Problem solving (D) Wrapping up	24	27/02/2020, 5.45pm
reward #4	24	authorised (03/03/2020)
FINISHED	24	

Household 4

today: 28/10/2020
Start: 07/10/2019 | End: 28/03/2020 (expected) – actual: 20/04/2020

phase	week	meeting
(A) Introduction	0	07/10/2019
	2	21/10/2019
reward #1	4	authorised (11/11/2019)
	5	11/11/2019 6.30pm
(B) New devices	9	11/12/2019, 7.00pm
reward #2	12	confirmed (20/01/2020)
	14	13/01/2020, 6.30pm
(B) Routines	18	10/02/2020, 6.30pm
reward #3	20	authorised (03/03/2020)
(C) Problem solving	22	16/03/2020, 6.30pm
(D) Wrapping up	26	20/04/2020, 6.30pm
reward #4	24	authorised (16/04/2020)
FINISHED	24	

Household 5

today: 28/10/2020
Start: 06/11/2019 | End: 25/04/2020 (expected) – actual: 11/12/2019

phase	week	meeting
(A) Introduction	0	06/11/2019 5.30pm
	3	27/11/2019 5.30pm
reward #1	4	
	5	11/12/2019, 5.30pm
(B) New devices	7	waiting
	9	
reward #2	12	
	12	
(B) Routines	16	
reward #3	20	
(C) Problem solving	20	
(D) Wrapping up	24	
reward #4	24	
DISCONTINUED	--	

Household 6

today: 28/10/2020
Start: 14/11/2019 | End: 02/05/2020 (expected) – actual: 02/06/2020

phase	week	meeting
(A) Introduction	0	14/11/2019 5.00pm
	2	28/11/2019 6.30pm
reward #1	4	confirmed (20/01/2020)
	5	17/12/2019 7.30pm
(B) New devices	11	26/01/2020, 11am
reward #2	12	confirmed (20/02/2020)
	13	09/02/2020, 11am
	17	03/03/2020, 7pm
reward #3	20	authorised (16/04/2020)
(B) Routines	21	07/04/2020, 7pm
additional COVID	23	21/04/2020, 7pm
reward #4	24	authorised (13/05/2020)
(C) Problem solving	25	12/05/2020, 7pm
(D) Wrapping up	29	02/06/2020
FINISHED	29	

PI: Prof Ivan Flechais – Ivan.flechais@cs.ox.ac.uk
Co-I: Prof Max Van Kleek – max.van.kleek@cs.ox.ac.uk

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD UK
Ethics approval: R59140/RE001

Figure B.4: Screenshot of study dashboard – displays summary of household participation progress

B.8 Planning Workshop

REDACTED

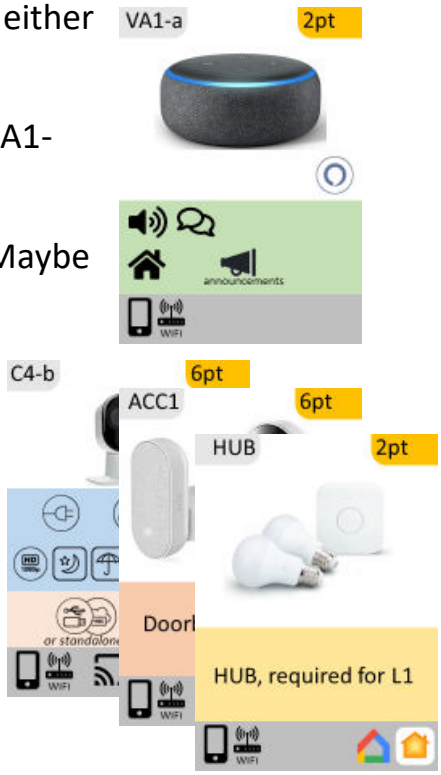
Planning Your Smart Home

Discuss which devices you would like to have in your smart home. Design a **30pt** and a **40pt** smart home by summing up card values.

Steps

Draw a sketch of your home and place the device in their future locations.

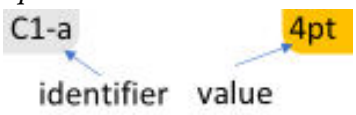
1) Start by choosing a platform (***VA*** cards, green), i.e. either Amazon Alexa (VA1) or Google Home (VA2)
    1) Choose a central control device, i.e. any of VA1-a/b or VA2-a/b/c/d
2) Discuss how you will spend the remaining points. Maybe define priorities for each device category
    - C1/C2/C3/C4 are CCTV cameras (blue) – hint: start discussion with light red section
    - ACC1/ACC2/ACC3 are accessories (red)
    - L1/L2/HUB are light system and accessories (yellow)

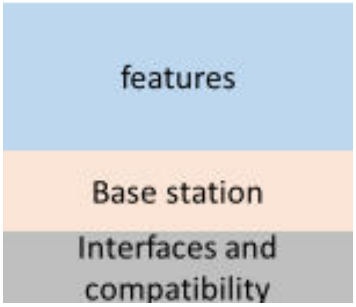


Rules

- You *can* only have one of C1/C2/C3/C4 but you can combine devices listed under C1 and C4
- You *can* use more than one of the same card
- You *cannot* have VA1 and VA2

Take a picture of the two final setups, 30pt and 40pt, and email it to REDACTED!





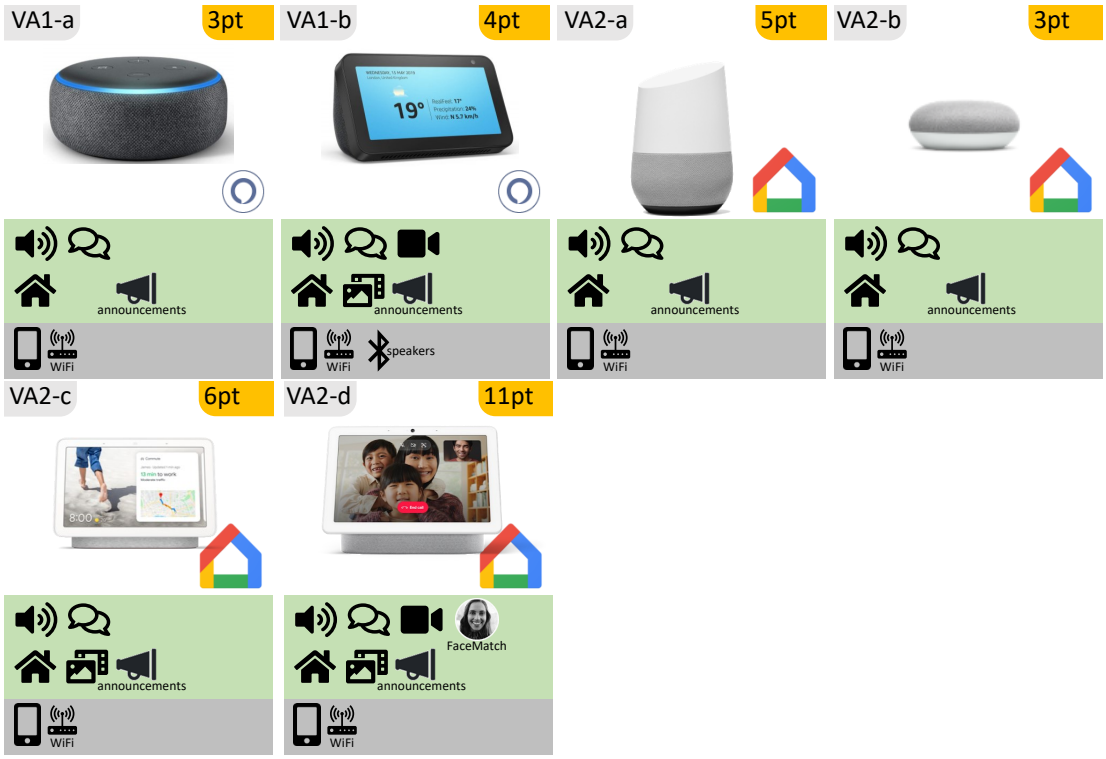
Symbol	Description
	Rechargeable, battery powered
	Can be run with power cord
	No power cord, battery powered
	Plays alarm sound
	Two-way audio communication
	Video quality HD (720p) or HD (1080p)
	Night vision
	Weather resistant IP65
	Camera angle
	Motion detection
	Activity zones with specific triggers
 X days	Automatic cloud backup stored for X number of days
 backup	Local backup, local data storage
 24/7	24/7 recording; permanent video recording
	Skip back for motion detection events
	Mobile app for remote control
	Uses/requires wireless network for operation

	Amazon Alexa enabled
	Google home enabled
	Apple homekit enabled
	Google chromecast enabled
	Sound output
	Smart voice assistant, conversation
	Smart home controller
	Announcement to other connected devices
	Media playback, pictures and videos
	Camera for video chat
	Bluetooth connection
	Smart face recognition

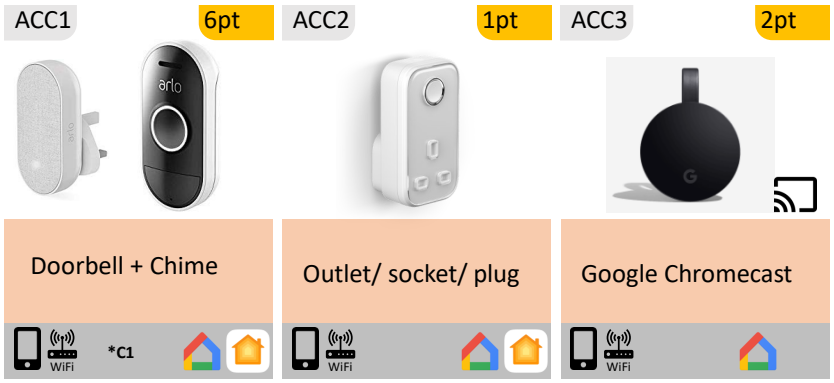
B.8.1 Cameras


C1-a
6pt
30 days
WiFi
audio
video
C1-b
10pt
30 days
backup
C1-c
12pt
30 days
backup
24/7
C1-d
indoor
6pt
30 days
backup
24/7
C3-a
10pt
10 days
C3-b
indoor
9pt
10 days
C4-a
2pt
7 days on base
C4-b
6pt
or standalone
C2
8pt
30 days
audio

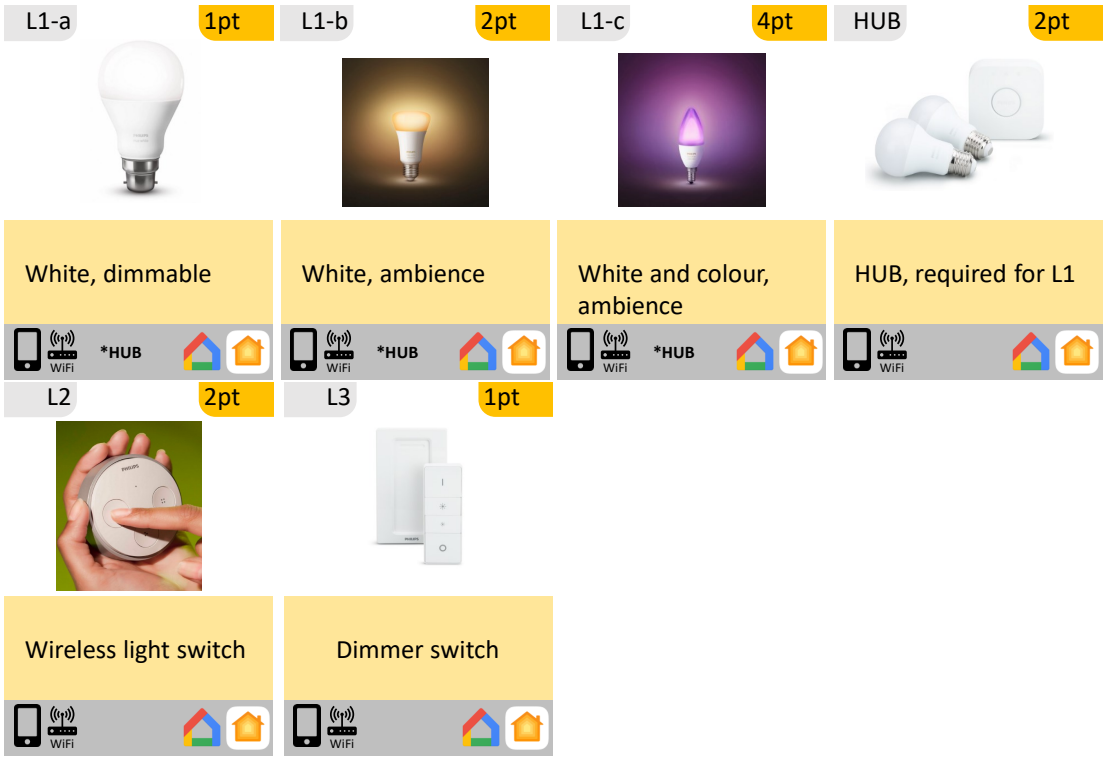
B.8.2 Voice Assistants



B.8.3 Other things



B.8.4 Lighting



B.8.5 Heating

References

[1] Toy Retailers Association. *Toy of the year 2014*. en. 2014. URL: https://www.toyretailersassociation.co.uk/toy-year-2014 (visited on 04/26/2021).

[2] Genesis Toys. *My Friend Cayla*. 2018. URL: https://www.myfriendcayla.com/ (visited on 07/01/2018).

[3] Marc Rotenberg, Claire Gartland, Laura M Moy, and Chris Laughlin. *In the Matter of Genesis Toys and Nuance Communications - Complaint and Request for Investigaton, Injunction, and other Relief to the Federal Trade Commission*. 2016. URL: https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf (visited on 07/01/2018).

[4] Bundesnetzagentur. *Press Release - Bundesnetzagentur removes children's doll "Cayla" from the market*. 2017.

[5] Christine Geeng and Franziska Roesner. "Who's In Control? Interactions In Multi-User Smart Homes". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019, forthcoming.

[6] Hammersley, Tom. *Jealous businessman spied on ex-partner using iPad mounted to kitchen wall*. en. 2018. URL: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/jealous-businessman-spied-ex-partner-14640719 (visited on 04/26/2021).

[7] Karen Levy and Bruce Schneier. "Privacy threats in intimate relationships". In: *Journal of Cybersecurity* 6.1 (2020), tyaa006.

[8] Blase Ur, Jaeyeon Jung, and Stuart Schechter. "Intruders versus intrusiveness". In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '14 Adjunct*. ACM Press, 2014.

[9] Dana McKay and Charlynn Miller. "Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Home Technologies". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, May 8, 2021, forthcoming.

[10] Stroud, Carl. *SPIED ON AT HOME – Creepy electronics expert used £100k 'smart house system' to spy on estranged wife's conversations*. en. 2018. URL: https://www.thesun.co.uk/news/6788205/smart-house-system-electronics-expert-spy-estranged-wife-conversations/ (visited on 04/26/2021).

[11] Statista. *Forecast market size of the global smart home market from 2016 to 2022*. 2017. URL: https://www.statista.com/statistics/682204/global-smart-home-market-size/ (visited on 09/12/2017).

[12] Council of the European Union. *General Data Protection Regulation*. 2016.

[13] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. "Privacy and human behavior in the age of information". In: *Science* 347.6221 (6221 2015), pp. 509–515.

[14] Andy Crabtree, Tom Lodge, James Colley, Chris Greenghalgh, and Richard Mortier. "Accountable internet of things? Outline of the IoT databox model". In: *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2017 IEEE 18th International Symposium on*. IEEE. 2017, pp. 1–6.

[15] Charith Perera, Susan Y.L. Wakenshaw, Tim Baarslag, Hamed Haddadi, Arosha K. Bandara, Richard Mortier, Andy Crabtree, Irene C.L. Ng, Derek McAuley, and Jon Crowcroft. "Valorising the IoT Databox: creating value for everyone". In: *Transactions on Emerging Telecommunications Technologies* 28.1 (1 Nov. 2016), e3125.

[16] Andy Crabtree, Richard Mortier, Tom Rodden, and Peter Tolmie. "Unremarkable networking: the home network as a part of everyday life". In: *Proceedings of the Designing Interactive Systems Conference. ACM.* (2012), pp. 554–563.

[17] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. "User Perceptions of Smart Home IoT Privacy". In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018).

[18] Tom Hargreaves, Charlie Wilson, and Richard Hauxwell-Baldwin. "Learning to live in a smart home". In: *Building Research & Information* 46 (1 2018), pp. 127–139.

[19] Kieron O'Hara. "The Seven Veils of Privacy". In: *IEEE Internet Computing* 20 (2 2016), pp. 86–91.

[20] Louise Barkhuus. "The mismeasurement of privacy". In: *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12* (2012), p. 367.

[21] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

[22] Paul Dourish and Genevieve Bell. "Rethinking Privacy". In: *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing*. Cambridge, Mass.: The MIT Press, Apr. 2011, pp. 137–160.

[23] Julia Slupska and Leonie Maria Tanczer. "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things". In: *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, June 2021, pp. 663–688.

[24] Hanna Schneider, Malin Eiband, Daniel Ullrich, and Andreas Butz. "Empowerment in HCI - A Survey and Framework". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, Apr. 2018, pp. 1–14.

[25] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. "Protection, Productivity and Pleasure in the Smart Home". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19* (2019), pp. 1–13.

[26] A. Lazar, C. Edasis, and A. Piper. "TECHNOLOGY TO EMPOWER OR DISEMPOWER: DESIGN TENSIONS WITHIN THE CONTEXT OF ART THERAPY". In: *The Gerontologist* 56.Suppl_3 (Nov. 2016), pp. 660–660.

[27] Amy Allen. "Feminist Perspectives on Power". In: *The Stanford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. Winter 2021. Metaphysics Research Lab, Stanford University, 2021.

[28] Max Weber. *Economy and society: An outline of interpretive sociology*. Vol. 1. Univ of California Press, 1978.

[29] Robert A. Dahl. “The concept of power”. In: *Behavioral Science* 2.3 (Jan. 2007), pp. 201–215.

[30] Hanna Fenichel Pitkin. *Wittgenstein and justice : on the significance of Ludwig Wittgenstein for social and political thought*. eng. Berkeley ; London: University of California Press, 1972.

[31] Martha Nussbaum and Amartya Sen. *The quality of life*. Clarendon Press, 1993.

[32] Julian Rappapon. “Studies in empowerment: Introduction to the issue”. In: *Prevention in human services* 3.2-3 (1984), pp. 1–7.

[33] Thomas E Wartenberg. *The forms of power : from domination to transformation*. eng. Philadelphia: Temple University Press, 1990.

[34] Radhika Garg and Christopher Moreno. “Understanding Motivators , Constraints , and Practices of Sharing Internet of Things”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3.2 (2 June 2019), pp. 1–21.

[35] William Seymour, Reuben Binns, Petr Slovak, Max Van Kleek, and Nigel Shadbolt. “Strangers in the Room: Unpacking Perceptions of ’Smartness’ and Related Ethical Concerns in the Home”. In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. DIS ’20. Eindhoven, Netherlands: Association for Computing Machinery, 2020, pp. 841–854.

[36] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. “A risk analysis of a smart home automation system”. In: *Future Generation Computer Systems* 56 (2016), pp. 719–733.

[37] Jack Sturgess, Jason R.C. Nurse, and Jun Zhao. “A Capability-oriented Approach to Assessing Privacy Risk in Smart Home Ecosystems”. In: *The PETRAS Conference: Cybersecurity of the IoT*. The Jounral of Engineering, 2018.

[38] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. “Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-Discipline”. In: *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. ITiCSE 2018 Companion. Larnaca, Cyprus: Association for Computing Machinery, 2018, pp. 36–54.

[39] Susan Leigh Star and James R Griesemer. “Institutional ecology,translations’ and boundary objects: Amateurs and professionals in Berkeley’s Museum of Vertebrate Zoology, 1907-39”. In: *Social studies of science* 19.3 (1989), pp. 387–420.

[40] Information Commissioner’s Office. *Principle (b): Purpose limitation*. en. 2021. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (visited on 02/28/2021).

[41] Martin J Kraemer, Ivan Flechais, and Helena Webb. “Exploring Communal Technology Use in the Home”. In: *Proceedings of the Halfway to the Future Symposium 2019*. HTTF 2019. Nottingham, United Kingdom: ACM, Nov. 2019.

[42] Martin Johannes Kraemer, Helena Webb, George Chalhoub, and Ivan Flechais. “"It Becomes More of an Abstract Idea, this Privacy" - Informing the Design for Communal Privacy Experiences in Smart Homes”. In: *SSRN Electronic Journal* (2022), ***under review***.

[43] Kraemer, Martin J., Helena Webb, and Ivan Flechais. “Innovating for Privacy in Communal Use: A Research and Design Framework”. In: (2022), ***under submission***.

[44] M.J. Kraemer and I. Flechais. "Researching Privacy in Smart Homes : A Roadmap of Future Directions and Research Methods". In: *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. Institution of Engineering and Technology, 2018, pp. 1–10.

[45] Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. "Further Exploring Communal Technology Use in Smart Homes: Social Expectations". In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI EA '20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–7.

[46] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. "Informing the Design of Privacy-Empowering Tools for the Connected Home". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI '20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–14.

[47] Martin Kraemer. "Beyond the Individual: Exploring Data Protection by Design in Connected Communal Spaces". In: *2020 USENIX Conference on Privacy Engineering Practice and Respect (PEPR 20)*. USENIX Association, Oct. 2020.

[48] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. ""It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. Yokohama, Japan: Association for Computing Machinery, 2021.

[49] Daniel J. Solove. *Understanding privacy*. eng. Cambridge, Mass. ; London: Harvard University Press, 2008.

[50] Deirdre K. Mulligan, Colin Koopman, and Nick Doty. "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy". In: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374.2083 (Dec. 2016), p. 20160118.

[51] Steve Harrison and Paul Dourish. "Re-Place-Ing Space: The Roles of Place and Space in Collaborative Systems". In: *Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work*. CSCW '96. Boston, Massachusetts, USA: Association for Computing Machinery, 1996, pp. 67–76.

[52] S. Dash, J. I, and J. Ashcroft. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft*. Rutgers University Press, 2004.

[53] Judith A. Swanson. *The Public and the Private in Aristotle's Political Philosophy*. Cornell University Press, 1992.

[54] Judith DeCew and Edward N Zalta. *Privacy*. 2013.

[55] Samuel D Warren and Louis D Brandeis. "The right to privacy". In: *Harvard law review* (1890), pp. 193–220.

[56] Ari Ezra Waldman. "Privacy As Trust: Sharing Personal Information in a Networked World". PhD. Columbia University, 2015.

[57] Kieron O'Hara. *The Seven Veils of Privacy: How Debates About Privacy Conceal Its Nature*. Manchester University Press.

[58] William L. Prosser. "Privacy". In: *California Law Review* 48.3 (1960), pp. 383–423.

[59] Alan F Westin. *Privacy and freedom*. eng. [1st ed.] New York: Atheneum, 1968.

[60] Daniel J Solove. "A brief History of Information Privacy Law". In: *Proskauer on privacy, GW Law Faculty Publication & Other Works, PLI* (2006).

[61] Abraham L. Newman. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Cornell University Press, 2008.

[62] *California Consumer Privacy Act of 2018*. 2018.

[63] Council of the European Union. *General Data Protection Regulation*. 2016. URL: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

[64] K. *Data Protection | European Data Protection Supervisor*. URL: https://edps.europa.eu/data-protection/data-protection_en (visited on 02/01/2020).

[65] Jiahong Chen, Lilian Edwards, Lachlan Urquhart, and Derek McAuley. "Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption". In: *SSRN Electronic Journal* (2019).

[66] Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, and Ellen Nadeau. *An introduction to privacy engineering and risk management in federal systems*. National Institute of Standards and Technology, Jan. 2017.

[67] Hans Peter Gassmann. "OECD guidelines governing the protection of privacy and transborder flows of personal data". In: *Computer Networks (1976)* 5 (2 1981), pp. 127–141.

[68] Ann Cavoukian. *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*. Tech. rep. Information and Privacy Commissioner of Ontario, 2010, p. 10. URL: https://www.ipc.on.ca/images/Resources/gps.pdf.

[69] S. I. Benn and G. F. Gaus. *Public and private in social life*. Croom Helm, 1983.

[70] Erving Goffman. *The presentation of self in everyday life*. eng. Doubleday anchor books ; A174. Garden City, N.Y.: Doubleday, 1959.

[71] Lisa M Austin. "Privacy and Private Law : The Dilemma of Justification". In: *McGill Law Journal* 55 (February 2010), pp. 165–210.

[72] Jeremy Bentham. "The Panopticon Writings". In: *London and New York: Verso* (1995), p. 199.

[73] M Foucault. *Discipline and punish - the birth of prison*. Vintage Books, 1995, p. 342.

[74] Gerald Dworkin. *The theory and practice of autonomy*. Cambridge University Press, 1988.

[75] Charles Fried. "Privacy: A moral analysis". In: *Yale Law Journal 77 (1)* 1 (1984), p. 984.

[76] Ferdinand Schoeman. "Privacy and intimate information". In: *Philosophical Dimensions of Privacy: An Anthology* (1984), pp. 403–418.

[77] Priscilla M Regan. "Legislating Privacy: Technology". In: *Social Values, and Public Policy* 69 (1995).

[78] Roger Clarke. "Introduction to dataveillance and information privacy, and definitions of terms". In: *Roger Clarke's Dataveillance and Information Privacy ...* (1999), pp. 1–17.

[79] Adam D Moore. "Privacy: its meaning and value". In: *American Philosophical Quarterly* 40 (3 2003), pp. 215–227.

[80] Smith, Dinev, and Xu. "Information Privacy Research: An Interdisciplinary Review". In: *MIS Quarterly* 35.4 (2011), p. 989.

[81] Rachel L Finn, David Wright, and Michael Friedewald. "Seven types of privacy". In: *European data protection: coming of age*. Springer, 2013, pp. 3–32.

[82] Alessandro Acquisti, Curtis R Taylor, and Liad Wagman. "The economics of privacy". In: *Journal of Economic Literature* 54(2) (2 2016), pp. 442–492.

[83] Spyros Kokolakis. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". In: *Computers & Security* 64 (2017), pp. 122–134.

[84] Susanne Barth and Menno D.T. de Jong. "The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review". In: *Telematics and Informatics* (2017).

[85] Noura Aleisa and Karen Renaud. "Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)". In: *ArXiv e-prints* (2016), pp. 1–10.

[86] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges". In: *Security and Communication Networks* 7 (12 2014), pp. 2728–2742.

[87] Richard J Hill, Martin Fishbein, and Icek Ajzen. "Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research." In: *Contemporary Sociology* 6 (2 1977), pp. 177–188.

[88] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini. "Privacy cynicism: A new approach to the privacy paradox". In: *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10 (4 2016).

[89] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '14. Toronto, Ontario, Canada: Association for Computing Machinery, 2014, pp. 2347–2356.

[90] Christoph Lutz and Pepe Strathoff. "Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses". In: *SSRN Journal Electronic Journal* (2014).

[91] Marie Caroline Oetzel and Tijana Gonja. "The online privacy paradox: a social representations perspective". In: *CHI'11 Extended Abstracts on Human Factors in Computing Systems*. ACM. 2011, pp. 2107–2112.

[92] Tobias Dienlin and Sabine Trepte. "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors". In: *European Journal of Social Psychology* 45 (3 2015), pp. 285–297.

[93] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. "Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices". In: *Chi'16* (2016), pp. 5228–5239.

[94] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. "Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics". In: *Proceedings of the 2017 SIGCHI Conference on Human Factors in Computing Systems* (2017), pp. 931–936.

[95] I Altman. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co., 1975.

[96] Walter R. Gove. In: *Contemporary Sociology* 7.5 (1978), pp. 638–638.

[97] Leysia Palen and Paul Dourish. “Unpacking "Privacy" for a Networked World”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’03. Ft. Lauderdale, Florida, USA: Association for Computing Machinery, 2003, pp. 129–136.

[98] Stephen T Margulis. “On the status and contribution of Westin’s and Altman’s theories of privacy”. In: *Journal of Social Issues* 59.2 (2003), pp. 411–429.

[99] Finn Brunton and Helen Nissenbaum. *Obfuscation: A User’s Guide for Privacy and Protest*. The MIT Press, 2015.

[100] Sandra Petronio. *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2002.

[101] Shruti Sannon, Brett Stoll, Dominic Difranzo, Malte F. Jung, and Natalya N. Bazarova. ““I just shared your responses”: Extending communication privacy management theory to interactions with conversational agents”. In: *Proceedings of the ACM on Human-Computer Interaction* 4 (GROUP 2020), pp. 1–18.

[102] Sandra Petronio and Rachael Hernandez. “Communication Privacy Management Theory”. In: *Oxford Research Encyclopedia of Communication* (Jan. 2019).

[103] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. “Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2 (2 2018).

[104] Sebastian Benthall, Seda Gürses, and Helen Nissenbaum. “Contextual Integrity through the Lens of Computer Science”. In: *Foundations and Trends® in Privacy and Security* 2 (1 2017), pp. 1–69.

[105] Luke Stark, Jen King, Xinru Page, Airi Lampinen, Jessica Vitak, Pamela Wisniewski, Tara Whalen, and Nathaniel Good. “Bridging the Gap between Privacy by Design and Privacy in Practice”. In: *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA ’16. San Jose, California, USA: Association for Computing Machinery, 2016, pp. 3415–3422.

[106] Yaxing Yao, Richmond Wong, Pardis Emami-Naeini, Nick Merrill, Xinru Page, Yang Wang, and Pamela Wisniewski. “Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms”. In: *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. CSCW ’19. Austin, TX, USA: Association for Computing Machinery, 2019, pp. 533–538.

[107] Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. “Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design”. In: *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*. CSCW ’18. Jersey City, NJ, USA: Association for Computing Machinery, 2018, pp. 425–431.

[108] Xinru Page, Karen Tang, Fred Stutzman, and Airi Lampinen. “Measuring Networked Social Privacy”. In: *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion*. CSCW ’13. San Antonio, Texas, USA: Association for Computing Machinery, 2013, pp. 315–320.

[109] Jessica Vitak, Pamela Wisniewski, Xinru Page, Airi Lampinen, Eden Litt, Ralf De Wolf, Patrick Gage Kelley, and Manya Sleeper. "The Future of Networked Privacy: Challenges and Opportunities". In: *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing*. CSCW'15 Companion. Vancouver, BC, Canada: Association for Computing Machinery, 2015, pp. 267–272.

[110] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. "A Survey on Interdependent Privacy". In: *ACM Comput. Surv.* 52.6 (Oct. 2019).

[111] Edward J Bloustein and Nathaniel J Pallone. *Individual and group privacy*. Routledge, 1978.

[112] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. "Calibrating Noise to Sensitivity in Private Data Analysis". In: *Theory of Cryptography*. Springer Berlin Heidelberg, 2006, pp. 265–284.

[113] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. "Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. CHI '18. Montreal QC, Canada: Association for Computing Machinery, 2018.

[114] Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. "Collective Privacy Management in Social Networks". In: *Proceedings of the 18th International Conference on World Wide Web*. WWW '09. Madrid, Spain: Association for Computing Machinery, 2009, pp. 521–530.

[115] Yunan Chen and Heng Xu. "Privacy Management in Dynamic Groups: Understanding Information Privacy in Medical Practices". In: *Proceedings of the 2013 Conference on Computer Supported Cooperative Work*. CSCW '13. San Antonio, Texas, USA: Association for Computing Machinery, 2013, pp. 541–552.

[116] Alison R. Murphy, Madhu C. Reddy, and Heng Xu. "Privacy practices in collaborative environments: A study of emergency department staff". In: *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW* (2014), pp. 269–282.

[117] D. J. Mir, Y. Shvartzshnaider, and M. Latonero. "It Takes a Village: A Community Based Participatory Framework for Privacy Design". In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. Apr. 2018, pp. 112–115.

[118] Danah Boyd. "Networked Privacy". In: *Surveillance & Society* 10.3/4 (Dec. 2012), pp. 348–350.

[119] Airi M I Lampinen. "Account Sharing in the Context of Networked Hospitality Exchange". In: *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*. CSCW '14. Baltimore, Maryland, USA: Association for Computing Machinery, 2014, pp. 499–504.

[120] Gergely Biczók and Pern Hui Chia. "Interdependent Privacy: Let Me Share Your Data". In: *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013, pp. 338–353.

[121] Priya Kumar and Sarita Schoenebeck. "The modern day baby book: Enacting good mothering and stewarding privacy on facebook". In: *CSCW 2015 - Proceedings of the 2015 ACM International Conference on Computer-Supported Cooperative Work and Social Computing* (2015), pp. 1302–1312.

[122] Murray Goulden, Peter Tolmie, Richard Mortier, Tom Lodge, Anna-Kaisa Pietilainen, and Renata Teixeira. "Living with interpersonal data: Observability and accountability in the age of pervasive ICT". In: *New Media & Society* 20.4 (Apr. 2017), pp. 1580–1599.

[123] Stefania Gnesi, Ilaria Matteucci, Corrado Moiso, Paolo Mori, Marinella Petrocchi, and Michele Vescovi. "My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data". In: *Privacy Technologies and Policy*. Springer International Publishing, 2014, pp. 154–171.

[124] Moses Kim. *The Meaning of Design: What Design Is and Why It's Important*. 2020. URL: https://shakuro.com/blog/the-meaning-of-design-what-design-is-and-why-its-important#the-purpose-of-design (visited on 02/01/2020).

[125] Herbert A Simon. *The sciences of the artificial [electronic resource]*. eng. 3rd ed. Cambridge, Mass.: MIT Press, 1996.

[126] Richmond Y. Wong and Deirdre K. Mulligan. "Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019.

[127] Seda Gürses, Carmela Gradiant Troncoso, and Claudia Diaz. "Engineering privacy by design reloaded". In: *Amsterdam Privacy Conference* (610613 2015), pp. 1–21.

[128] Sarah Spiekermann and Lorrie Faith Cranor. "Engineering Privacy". In: *IEEE Transactions on Software Engineering* 35.1 (2009), pp. 67–82.

[129] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. *Privacy and Data Protection by Design - from policy to engineering*. Vol. abs/1501.0. 2015, pp. 1–72.

[130] Inga Kroener and David Wright. "A Strategy for Operationalizing Privacy by Design". In: *The Information Society* 30.5 (2014), pp. 355–365.

[131] Daniel J Solove. "A Taxonomy of Privacy". In: *University of Pennsylvania Law Review* 154 (3 Jan. 2006), p. 477.

[132] Seda Gürses and Jose M. Del Alamo. "Privacy Engineering: Shaping an Emerging Field of Research and Practice". In: *IEEE Security and Privacy* 14 (2 2016), pp. 40–46.

[133] Steve Harrison, Deborah Tatar, and Phoebe Sengers. "The three paradigms of HCI. alt". In: *Alt. Chi. Session at the SIGCHI Conference on Human Factors in Computing Systems*. San Jose, CA, 2007.

[134] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. "A Design Space for Effective Privacy Notices". In: *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 2015, pp. 365–393.

[135] Fred H. Cate. "The Limits of Notice and Choice". In: *IEEE Security & Privacy Magazine* 8.2 (Mar. 2010), pp. 59–62.

[136] Jonathan A. Obar and Anne Oeldorf-Hirsch. "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services". In: *Information, Communication & Society* 23.1 (July 2018), pp. 128–147.

[137] Ewa Luger, Stuart Moran, and Tom Rodden. "Consent for All: Revealing the Hidden Complexity of Terms and Conditions". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '13. Paris, France: Association for Computing Machinery, 2013, pp. 2687–2696.

[138] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. "Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online". In: *the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (Soups 2016), pp. 77–96.

[139] Donald A. Norman. *The design of everyday things*. eng. Revised and expanded edition. Cambridge, Massachusetts, 2013.

[140] Ewa Luger, Lachlan Urquhart, Tom Rodden, and Michael Golembewski. "Playing the legal card: Using ideation cards to raise data protection issues within the design process". In: *Conference on Human Factors in Computing Systems - Proceedings* 2015-April (2015), pp. 457–466.

[141] M.J. Muller. "Participatory design: The third space in HCI". In: *Human-Computer Interaction Handbook* 4235 (January 2002 2003), pp. 1051–1068.

[142] Katie Shilton, Jeffrey A Burke, Deborah Estrin, Mark Hansen, and Mani Srivastava. *Participatory privacy in urban sensing*. Tech. rep. UCLA: Center for Embedded Network Sensing, 2008. URL: https://escholarship.org/uc/item/90j149pp.

[143] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019), pp. 1–12.

[144] Yaxing Yao, Richmond Wong, Pardis Emami-Naeini, Nick Merrill, Xinru Page, Yang Wang, and Pamela Wisniewski. "Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms". In: *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. CSCW '19. Austin, TX, USA: Association for Computing Machinery, 2019, pp. 533–538.

[145] Andy Crabtree, Peter Tolmie, and Will Knight. "Repacking 'Privacy' for a Networked World". In: *Comput. Supported Coop. Work* 26.4–6 (Dec. 2017), pp. 453–488.

[146] Paul Dourish and Genevieve Bell. *Rethinking Privacy*. 2011.

[147] Shelley Mallett. "Understanding Home: A Critical Review of the Literature". In: *The Sociological Review* 52 (1 2004), pp. 62–89.

[148] Anthony Giddens. *Sociology*. Polity, 1989.

[149] Bryan Turner, Craig J Calhoun, Chris Rojek, and Bryan S Turner. *The Sociology of the Family*. eng. Ed. by Craig J Calhoun, Chris Rojek, and Bryan S Turner. London, 2005.

[150] Samantha Punch, Jeni Harden, Ian Marsh, and Mike Keating. *Sociology : making sense of society*. Fifth. Pearson Education Limited, 2013.

[151] Helen J. Richardson. "A 'smart house' is not a home: The domestication of ICTs". In: *Information Systems Frontiers* 11 (5 2009), pp. 599–608.

[152] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K Dey. "Principles of Smart Home Control". In: *Lncs* 4206 (2006), pp. 19–34.

[153] Andy Crabtree and Tom Rodden. "Domestic routines and design for the home". In: *Computer Supported Cooperative Work: CSCW: An International Journal* 13 (2 2004), pp. 191–220.

[154] John Strain. "Households as morally ordered communities: explorations in the dynamics of domestic life". In: *Inside the Smart Home* (2003), pp. 41–62.

[155] Graham Crow. *community*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007.

[156] Albert O Hirschman. *Shifting involvements : private interest and public action*. eng. 20th-anniversary ed. , with a new foreword by Robert H. Frank. Princeton, N.J.; Oxford: Princeton University Press, 2002.

[157] Joan Aldous, Emile Durkheim, and Ferdinand Tonnies. "An Exchange Between Durkheim and Tonnies on the Nature of Social Relations, with an Introduction by Joan Aldous". In: *American Journal of Sociology* 77.6 (1972), pp. 1191–1200.

[158] Ferdinand Tönnies. *Community and association : (Gemeinschaft und Gesellschaft)*. eng. International library of sociology and social reconstruction (Routledge & Kegan Paul). London: Routledge & Kegan Paul, 1955.

[159] Roger Silverstone, Eric Hirsch, and David Morley. "Information and communication technologies and the moral economy of the household". In: *Consuming technologies : media and information in domestic spaces*. Ed. by Roger Silverstone and Eric Hirsch. 1992.

[160] Jon O'Brien, Tom Rodden, Mark Rouncefield, and John Hughes. "At Home with the Technology : An Ethnographic Study of a Set-Top-Box Trial". In: *ACM Transactions on Computer-Human Interaction* 6 (3 1999), pp. 282–308.

[161] Lauren Langman. *transgression*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007.

[162] Stephan Fuchs. *agency (and intention)*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007.

[163] Harold Garfinkel. "Studies of the Routine Grounds of Everyday Activities". In: *Social Problems* 11.3 (Jan. 1964), pp. 225–250.

[164] Alasdair C MacIntyre. *A short history of ethics : a history of moral philosophy from the Homeric age to the twentieth century*. eng. 2nd ed. Routledge classics. London: Routledge Classics, 2002.

[165] Lena Jayyusi. "Values and moral judgement: Communicative praxis as a moral order". In: *Ethnomethodology and the human sciences*. Ed. by Graham Button. Cambridge University Press, Jan. 1991. Chap. 10, pp. 227–269.

[166] Murray Goulden. "'Delete the family': platform families and the colonisation of the smart home". In: *Information, Communication & Society* (Sept. 2019), pp. 1–18.

[167] Jan Windebank. "Dual-earner couples in Britain and France: Gender divisions of domestic labour and parenting work in different welfare states". In: *Work, Employment and Society* 15 (2 2001), pp. 269–290.

[168] Allison Daminger. "The Cognitive Dimension of Household Labor". In: *Am Sociol Rev* 84.4 (July 2019), pp. 609–633.

[169] Marilyn Manser and Murray Brown. "Marriage and Household Decision-Making: A Bargaining Analysis". In: *International Economic Review* 21 (1 1980), pp. 31–44.

[170] Monica Biernat and Camille B. Wortman. "Sharing of Home Responsibilities Between Professionally Employed Women and Their Husbands". In: *Journal of Personality and Social Psychology* 60 (6 1991), pp. 844–860.

[171] Jacqueline Scott and Elizabeth Clery. "Gender roles An incomplete revolution ?" In: *British Social Attitudes 30* (2012), pp. 115–139.

[172] Gerold Mikula, Heribert H. Freudenthaler, Sigrun Brennacher-Kröll, and Beatrix Brunschko. “Division of labor in student households: Gender inequality, perceived justice, and satisfaction”. In: *Basic and Applied Social Psychology* 19 (3 1997), pp. 275–289.

[173] Audrey Desjardins, Ron Wakkary, and William Odom. “Investigating Genres and Perspectives in HCI Research on the Home”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI ’15* (2015), pp. 3073–3082.

[174] Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. “Smart homes and their users: a systematic analysis and key challenges”. In: *Personal and Ubiquitous Computing* 19 (2 2015), pp. 463–476.

[175] Sarah Mennicken, Jo Vermeulen, and Elaine M Huang. “From Today ’ s Augmented Houses to Tomorrow ’ s Smart Homes : New Directions for Home Automation Research”. In: *UbiComp ’14 Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2014), pp. 105–115.

[176] Alladi Venkatesh. “Computers and Other Interactive Technologies for the Home”. In: *Communications of the ACM* 39.12 (12 Dec. 1996), pp. 47–54.

[177] Younghwa Lee, Kenneth A Kozar, Kai R T Larsen, Y Lee, K A Kozar, and K R T Larsen. “The Technology Acceptance Model: Past, Present, and Future”. In: *Communications of the Association for Information Systems* 12 (50 2003), pp. 752–780.

[178] Thomas Berker, Maren Hartmann, Yves Punie, and Katie Ward. *Introduction*. 2006.

[179] Paul Dourish. “The Appropriation of Interactive Technologies : Some Lessons from Placeless Documents”. In: *Computer Supported Cooperative Work (CSCW)* 12.4 (Dec. 2003), pp. 1–22.

[180] Richard Harper, David Frohlich, Robert Kraut, and Richard Harper. *Inside the Smart Home*. Springer-Verlag, 2003, pp. 127–162.

[181] Harvey Sacks. *Lectures on Conversation*. Wiley-Blackwell, Jan. 1995.

[182] Peter Tolmie, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. “Towards the Unremarkable Computer: Making Technology at Home in Domestic Routine”. In: *Inside the Smart Home*. Ed. by Richard Harper. London: Springer, 2003. Chap. 10, pp. 183–206.

[183] Yolande A.A. Strengers. “Designing eco-feedback systems for everyday life”. In: *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI ’11*. ACM Press, 2011.

[184] Peter Tolmie, Andy Crabtree, Tom Rodden, Chris Greenhalgh, and Steven Benford. “Making the Home Network at Home: Digital Housekeeping”. In: *Proceedings of the Tenth European Conference on Computer Supported Cooperative Work*. 2007, pp. 331–349.

[185] Rebecca E. Grinter, W. Keith Edwards, Marshini Chetty, Erika S. Poole, Ja-Young Sung, Jeonghwa Yang, Andy Crabtree, Peter Tolmie, Tom Rodden, Chris Greenhalgh, and Steve Benford. “The ins and outs of home networking”. In: *ACM Transactions on Computer-Human Interaction* 16.2 (June 2009), pp. 1–28.

[186] Paul Ten Have. “The Notion of Member is the Heart of the Matter: On the Role of Membership Knowledge in Ethnomethodological Inquiry”. In: *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 3.3 (2002).

[187] Peter Tolmie, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. “Unremarkable computing”. In: *Proceedings of the SIGCHI conference on Human factors in computing systems Changing our world, changing ourselves - CHI ’02* (1 2002), p. 399.

[188] Andy Crabtree, Tom Rodden, Peter Tolmie, Richard Mortier, Tom Lodge, Pat Brundell, and Nadia Pantidi. “House rules: the collaborative nature of policy in domestic networks”. In: *Personal and Ubiquitous Computing* 19 (1 2015), pp. 203–215.

[189] Tom Hargreaves, Michael Nye, and Jacquelin Burgess. “Making energy visible: A qualitative field study of how householders interact with feedback from smart energy monitors”. In: *Energy Policy* 38 (10 2010), pp. 6111–6119.

[190] Tom Hargreaves, Michael Nye, and Jacquelin Burgess. “Keeping energy visible? Exploring how householders interact with feedback from smart energy monitors in the longer term”. In: *Energy Policy* 52 (2013), pp. 126–134.

[191] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. “I don’t own the data": End User Perceptions of Smart Home Device Data Practices and Risks”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Apr. 2019.

[192] Sarah Mennicken and Elaine M Huang. “Hacking the natural habitat: An in-the-wild study of smart homes, their development, and the people who live in them”. In: *Pervasive Computing*. Ed. by Judy Kay, Paul Lukowicz, Hideyuki Tokuda, Patrick Olivier, and Antonio Krüger. Vol. 7319 LNCS. Berlin, Heidelberg: Springer, 2012, pp. 143–160.

[193] Eric Zeng, Shrirang Mare, and Franziska Roesner. “End User Security & Privacy Concerns with Smart Homes”. In: *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*. SOUPS’17. Santa Clara, CA, USA: USENIX Association, 2017, pp. 65–80.

[194] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. ““She’ll Just Grab Any Device That’s Closer”: A Study of Everyday Device & Account Sharing in Households”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI ’16. San Jose, California, USA: Association for Computing Machinery, 2016, pp. 5921–5932.

[195] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. “"Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019), pp. 1–24.

[196] Roxanne Leitão. “Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse”. In: *Proceedings of the 2019 on Designing Interactive Systems Conference*. ACM, June 2019.

[197] Xinru Page, Paritosh Bahirat, Muhammad I. Safi, Bart P. Knijnenburg, and Pamela Wisniewski. “The Internet of What?” In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2.4 (Dec. 2018), pp. 1–22.

[198] Yolande Strengers and Larissa Nicholls. “Aesthetic pleasures and gendered tech-work in the 21st-century smart home”. In: *Media International Australia* 166.1 (Nov. 2017), pp. 70–80.

[199] Jennifer A. Rode and Erika Shehan Poole. “Putting the gender back in digital housekeeping”. In: *Proceedings of the 4th Conference on Gender & IT - GenderIT ’18*. ACM Press, 2018.

[200] James Pierce. “Smart Home Security Cameras and Shifting Lines of Creepiness”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI ’19* (2019), pp. 1–14.

[201] Peter Worthy, Ben Matthews, and Stephen Viller. “Trust Me: Doubts and Concerns Living with the Internet of Things”. In: *Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS ’16* (2016), pp. 427–434.

[202] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. “Privacy Expectations and Preferences in an IoT World”. In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, July 2017, pp. 399–412.

[203] Hosub Lee and Alfred Kobsa. “Confident Privacy Decision-Making in IoT Environments”. In: *ACM Transactions on Computer-Human Interaction* 27 (1 Dec. 2019), pp. 1–39.

[204] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. “Exploring How Privacy and Security Factor into IoT Device Purchase Behavior”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, May 2019.

[205] Timo Jakobi, Gunnar Stevens, Nils Vindice, Dave Randall, Peter Tolmie, and Volker Wulf. “Evolving Needs in IoT Control and Accountability : A Longitudinal Study on Smart Home Intelligibility”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2 (4 2018).

[206] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. “I’m All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios”. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI ’20. Honolulu, HI, USA: Association for Computing Machinery, 2020, pp. 1–13.

[207] Andy Crabtree, Richard Mortier, Toni Robertson, and Ina Wagner. “Human Data Interaction: Historical Lessons from Social Studies and CSCW”. In: *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway*. Ed. by Nina Boulus-Rødje, Gunnar Ellingsen, Tone Bratteteig, Margunn Aanestad, and Pernille Bjørn. Springer International Publishing, 2015, pp. 3–21.

[208] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. “Privacy Perceptions and Designs of Bystanders in Smart”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (November Nov. 2019), pp. 1–24.

[209] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. ““You just can’t know about everything”: Privacy Perceptions of Smart Home Visitors”. In: *19th International Conference on Mobile and Ubiquitous Multimedia*. ACM, Nov. 2020.

[210] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. ““I Don’t Know How to Protect Myself”: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments”. In: *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. NordiCHI ’20. Tallinn, Estonia: Association for Computing Machinery, 2020.

[211] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. "Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy". In: *Proceedings of the ACM on Human Computer Interaction* 4.CSCW2 (2020), 116:1–116:28.

[212] Radhika Garg and Jenna Kim. "An Exploratory Study for Understanding Reasons of (Not-)Using Internet of Things". In: *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (2018), pp. 1–6.

[213] Eric Zeng and Franziska Roesner. "Understanding and Improving Security and Privacy in Multi-User Smart Homes : A Design Exploration and In-Home User Study". In: *28th USENIX Security Symposium (2019)* (2019).

[214] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. "Alexa, Are You Listening?" In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (Nov. 2018), pp. 1–31.

[215] Vinay Koshy, Joon Sung Park, Ti-Chung Cheng, and Karrie Karahalios. ""We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, May 8, 2021, p. 16.

[216] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. "Rethinking Access Control and Authentication for the Home Internet of Things (IoT)". In: *Proceedings of the 27th USENIX Conference on Security Symposium* (2018), pp. 255–272.

[217] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. "Smart Home Beyond the Home: A Case for Community-Based Access Control". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2020.

[218] Barry Brown, Alex S. Taylor, Shahram Izadi, Abigail Sellen, Joseph Jofish' Kaye, and Rachel Eardley. "Locating Family Values: A Field Trial of the Whereabouts Clock". In: *UbiComp 2007: Ubiquitous Computing*. Innsbruck: Springer Berlin Heidelberg, 2007, pp. 354–371.

[219] Liam J. Bannon. "From Human Factors to Human Actors: The Role of Psychology and Human-Computer Interaction Studies in System Design". In: *Readings in Human–Computer Interaction*. Elsevier, 1995, pp. 205–214.

[220] J. Grudin. "Three faces of human-computer interaction". In: *IEEE Annals of the History of Computing* 27 (4 2005), pp. 46–62.

[221] Susanne Bødker. "When Second Wave HCI Meets Third Wave Challenges". In: *Proceedings of the 4th Nordic Conference on Human-Computer Interaction: Changing Roles*. NordiCHI '06 (2006), pp. 1–8.

[222] Yvonne Rogers. "HCI Theory: Classical, Modern, and Contemporary". In: *Synthesis Lectures on Human-Centered Informatics* 5.2 (May 2012), pp. 1–129.

[223] Lian J Bannon. "Perspectives on CSCW: From HCI and CMC to CSCW". In: *International Conference on Human-Computer Interaction (EW-HCI'92). St. Petersburg: BCS HICOM electronic conference system*. 1992, pp. 148–158.

[224] Kjeld Schmidt and Liam Bannon. "Constructing CSCW: The First Quarter Century". In: *Computer Supported Cooperative Work (CSCW)* 22.4-6 (Aug. 2013), pp. 345–372.

[225] Thomas S Kuhn. *The structure of scientific revolutions*. University of Chicago press, 2012.

[226] Philip Agre. *Computation and human experience*. Cambridge University Press, 1997.

[227] Paul Dourish. "Implications for Design". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '06. Montréal, Québec, Canada: Association for Computing Machinery, 2006, pp. 541–550.

[228] Andrew Crabtree, Mark Rouncefield, and Peter Tolmie. *Doing Design Ethnography*. Springer, 2012.

[229] Paul M. Aoki and Allison Woodruff. "Making space for stories: ambiguity in the design of personal communication systems". In: *Proceedings of the 2005 Conference on Human Factors in Computing Systems, CHI 2005, Portland, Oregon, USA, April 2-7, 2005*. Ed. by Gerrit C. van der Veer and Carolyn Gale. ACM, 2005, pp. 181–190.

[230] Lucy A. Suchman. *Plans and situated actions - the problem of human-machine communication*. Learning in doing: social,cognitive,and computational perspectives. Cambridge University Press, 1987.

[231] Graham Button and Wes Sharrock. "Studies of Work and the Workplace in HCI: Concepts and Techniques". In: *Synthesis Lectures on Human-Centered Informatics* 2.1 (Jan. 2009), pp. 1–96.

[232] Roy Hutchison. *Chicago School*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007.

[233] Val Mitchell, Kerstin Leder Mackley, Sarah Pink, Carolina Escobar-Tello, Garrath T. Wilson, and Tracy Bhamra. "Situating digital interventions: Mixed methods for HCI research in the home". In: *Interacting with Computers* 27 (1 2015), pp. 3–12.

[234] Martyn Hammersley. *ethnography*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007, pp. 1479–1483.

[235] Robert J. Moore. "Ethnomethodology and Conversation Analysis: Empirical Approaches to the Study of Digital Technology in Action". In: *The SAGE Handbook of Digital Technology Research*. Ed. by Sara Price, Carey Jewitt, and Barry Brown. 2015, pp. 217–235.

[236] Douglas W. Maynard and Steven E. Clayman. "The Diversity of Ethnomethodology". In: *Annual Review of Sociology* 17.1 (Aug. 1991), pp. 385–418.

[237] Dan Shapiro. "The Limits of Ethnography: Combining Social Sciences for CSCW". In: *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work*. CSCW '94. Chapel Hill, North Carolina, USA: Association for Computing Machinery, 1994, pp. 417–428.

[238] John A. Hughes, Jon O'Brien, Tom Rodden, Mark Rouncefield, and Steve Blythin. "Designing with ethnography". In: *Proceedings of the conference on Designing interactive systems processes, practices, methods, and techniques - DIS '97*. ACM Press, 1997.

[239] Graham Button and Paul Dourish. "Technomethodology: Paradoxes and Possibilities". In: *CHI 96 Vancouver, BC Canada* (1996), pp. 19–26.

[240] Andy Crabtree, Tom Rodden, Peter Tolmie, and Graham Button. "Ethnography considered harmful". In: *Proceedings of the 27th International Conference on Human Factors in Computing Systems, CHI 2009, Boston, MA, USA, April 4-9, 2009*. Ed. by Dan R. Olsen Jr., Richard B. Arthur, Ken Hinckley, Meredith Ringel Morris, Scott E. Hudson, and Saul Greenberg. ACM, 2009, pp. 879–888.

[241] Graham Button, Andy Crabtree, Mark Rouncefield, and Peter Tolmie. *Deconstructing Ethnography: Towards a Social Methodology for Ubiquitous Computing and Interactive Systems Design*. Springer Berlin, 2015.

[242] Kathy Charmaz and Richard G. Mitchell. "Grounded Theory in Ethnography". In: *Handbook of Ethnography*. SAGE Publications Ltd, 2001, pp. 160–174.

[243] Kathy Charmaz and Karen Henwood. "Grounded Theory Methods for Qualitative Psychology". In: *The SAGE Handbook of Qualitative Research in Psychology*. Ed. by Carla Willig and Wendy Stainton Rogers. SAGE Publications Ltd, 2017. URL: https://doi.org/10.4135%2F9781526405555.

[244] Barney G Glaser. *Emergence vs forcing : basics of grounded theory analysis*. eng. Mill Valley, CA: Sociology Press, 1992.

[245] Kathy Charmaz. "Constructionism and the grounded theory method". In: *Handbook of constructionist research* (2008), pp. 397–412.

[246] Peter Tolmie and Andy Crabtree. "Deploying research technology in the home". In: *Proceedings of the ACM 2008 conference on Computer supported cooperative work - CSCW '08* (2008), p. 639.

[247] Jacob O. Wobbrock and Julie A. Kientz. "Research contributions in human-computer interaction". In: *Interactions* 23.3 (Apr. 2016), pp. 38–44.

[248] Uwe Flick. *An introduction to qualitative research*. eng. 3rd ed. London: Sage, 2006.

[249] Nigel King and Christine Horrocks. *Interviews in qualitative research*. Sage, 2010.

[250] Genevieve Bell, Mark Blythe, and Phoebe Sengers. "Making by Making Strange: Defamiliarization and the Design of Domestic Technologies". In: *ACM Trans. Comput.-Hum. Interact.* 12.2 (June 2005), pp. 149–173.

[251] Graham Button. "The ethnographic tradition and design". In: *Design Studies* 21.4 (2000), pp. 319–332.

[252] Kirsten Boehner, Janet Vertesi, Phoebe Sengers, and Paul Dourish. "How HCI Interprets the Probes". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '07. San Jose, California, USA: Association for Computing Machinery, 2007, pp. 1077–1086.

[253] Phoebe Sengers, Kirsten Boehner, Shay David, and Joseph 'Jofish' Kaye. "Reflective Design". In: *Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility*. CC '05. Aarhus, Denmark: Association for Computing Machinery, 2005, pp. 49–58.

[254] David Randall, Mark Rouncefield, and Peter Tolmie. "Ethnography, CSCW and Ethnomethodology". In: *Computer Supported Cooperative Work (CSCW)* 30.2 (Nov. 2020), pp. 189–214.

[255] H Garfinkel. *Studies in ethnomethodology*. Prentice-Hall, 1967.

[256] John A. Hughes, David Randall, and Dan Shapiro. "Faltering from Ethnography to Design". In: *Proceedings of the 1992 ACM Conference on Computer-Supported Cooperative Work*. CSCW '92. Toronto, Ontario, Canada: Association for Computing Machinery, 1992, pp. 115–122.

[257] John Hughes, Val King, Tom Rodden, and Hans Andersen. "Moving out from the Control Room: Ethnography in System Design". In: *Proceedings of the 1994 ACM Conference on Computer Supported Cooperative Work*. CSCW '94. Chapel Hill, North Carolina, USA: Association for Computing Machinery, 1994, pp. 429–439.

[258] Andy Crabtree. "Taking technomethodology seriously: hybrid change in the ethnomethodology–design relationship". In: *European Journal of Information Systems* 13.3 (Sept. 2004), pp. 195–209.

[259] Fiona Westin and Sonia Chiasson. ""It's So Difficult to Sever That Connection": The Role of FoMO in Users' Reluctant Privacy Behaviours". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. Yokohama, Japan: Association for Computing Machinery, 2021.

[260] Maryam N. Razavi and Lee Iverson. "A Grounded Theory of Information Sharing Behavior in a Personal Learning Space". In: *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*. CSCW '06. Banff, Alberta, Canada: Association for Computing Machinery, 2006, pp. 459–468.

[261] Tamara Alsheikh, Jennifer A. Rode, and Siân E. Lindley. "(Whose) Value-Sensitive Design: A Study of Long- Distance Relationships in an Arabic Cultural Context". In: *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*. CSCW '11. Hangzhou, China: Association for Computing Machinery, 2011, pp. 75–84.

[262] Kathy Charmaz. *Constructing grounded theory: a practical guide through qualitative analysis*. Vol. 10. 2006, p. 208.

[263] Barney G Glaser. *Theoretical sensitivity : advances in the methodology of grounded theory*. eng. Mill Valley, Calif: Sociology Press, 1978.

[264] Paul Ten Have. *Understanding Qualitative Research and Ethnomethodology*. SAGE Publications Ltd, 2004.

[265] Adele E. Clarke. "Grounded Theory: Critiques, Debates, and Situational Analysis". In: *The SAGE Handbook of Social Science Methodology*. Ed. by William Outhwaite and Stephen P. Turner. SAGE Publications Ltd, 2011, pp. 423–442.

[266] Judith A. Holton and Isabelle Walsh. "Foundational Pillars of Classic Grounded Theory". In: *Classic Grounded Theory: Applications With Qualitative and Quantitative Data*. SAGE Publications, Inc., 2017, pp. 28–45.

[267] Harold Garfinkel. *Ethnomethodology's program: Working out Durkheim's aphorism*. Rowman & Littlefield Publishers, 2002.

[268] Paul Atkinson, Amanda Coffey, and Sara Delamont. *Key themes in qualitative research : continuities and changes*. eng. Walnut Creek, Calif. ; Oxford: AltaMira Press, 2003.

[269] Antony Bryant. "Re-grounding grounded theory". English. In: *JITTA : Journal of Information Technology Theory and Application* 4.1 (2002), pp. 25–42.

[270] Michael Muller. "Curiosity, Creativity, and Surprise as Analytic Tools: Grounded Theory Method". In: *Ways of Knowing in HCI*. Springer New York, 2014, pp. 25–48.

[271] Harold Garfinkel and Harvey Sacks. "On formal structures of practical action". In: *Theoretical Sociology: Perspectives and Developments*. Ed. by John C. McKinney and Edward A. Tiryakian. New York: Appleton-Century-Crofts, 1970. Chap. 13, pp. 338–266.

[272] Paul Dourish and Graham Button. “On "Technomethodology": Foundational Relationships Between Ethnomethodology and System Design”. In: *Human-Computer Interaction* 13.4 (Dec. 1998), pp. 395–432.

[273] Lachlan Urquhart and Jiahong Chen. “On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity”. In: *SSRN Electronic Journal* (June 19, 2020). eprint: 2006.11043 (cs.HC).

[274] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. “Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Aug. 2020, pp. 185–204.

[275] Lachlan Urquhart. “Towards user centric regulation: exploring the interface between information technology law and human computer interaction”. PhD thesis. University of Nottingham, July 2017. URL: http://eprints.nottingham.ac.uk/41787/.

[276] Janice M Morse, Judith E Hupcey, Janice Penrod, Jude A Spiers, Charlotte Pooler, and Carl Mitcham. “Symposium conclusion-issues of validity: Behavioral concepts, their derivation and interpretation”. In: *International Journal of Qualitative Methods* 1.4 (2002), pp. 68–73.

[277] Steve Benford, Gabriella Giannachi, Boriana Koleva, and Tom Rodden. “From interaction to trajectories”. In: *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*. ACM Press, 2009.

[278] Victoria Bellotti, Maribeth Back, W. Keith Edwards, Rebecca E. Grinter, Austin Henderson, and Cristina Lopes. “Making sense of sensing systems”. In: *Proceedings of the SIGCHI conference on Human factors in computing systems Changing our world, changing ourselves - CHI ’02*. ACM Press, 2002.

[279] Thomas Erickson and Wendy A. Kellogg. “Social translucence”. In: *ACM Transactions on Computer-Human Interaction (TOCHI)* 7.1 (Mar. 2000), pp. 59–83.

[280] Karin Niemantsverdriet, Harm Van Essen, Minna Pakanen, and Berry Eggen. “Designing for Awareness in Interactions with Shared Systems”. In: *ACM Transactions on Computer-Human Interaction* 26.6 (Dec. 2019), pp. 1–41.

[281] Yosef Jabareen. “Building a Conceptual Framework: Philosophy, Definitions, and Procedure”. In: *International Journal of Qualitative Methods* 8.4 (Dec. 2009), pp. 49–62.

[282] Egon G Guba and Yvonna S Lincoln. *Effective evaluation: Improving the usefulness of evaluation results through responsive and naturalistic approaches*. Jossey-Bass, 1981.

[283] Egon Guba. “Criteria for assessing the trustworthiness of naturalistic inquiries”. eng. In: *ECTJ* 29.2 (1981), pp. 75–91.

[284] Clifford Geertz et al. “Thick description: Toward an interpretive theory of culture”. In: *Turning points in qualitative research: Tying knots in a handkerchief* 3 (1973), pp. 143–168.

[285] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. “Reliability and Inter-rater Reliability in Qualitative Research”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019), pp. 1–23.

[286] David Sikolia, David Biros, Marlys Mason, and Mark Weiser. “Trustworthiness of Grounded Theory Methodology Research in Information Systems”. In: *MWAIS 2013 Proceedings* (2013).

[287] Kathleen Musante DeWalt and Billie R DeWalt. *Participant observation [electronic resource] : a guide for fieldworkers*. eng. 2nd ed. Ebook central. Lanham, Md.: Rowman & Littlefield, 2011.

[288] Rikke Hagensby Jensen, Yolande Strengers, Jesper Kjeldskov, Larissa Nicholls, and Mikael B. Skov. "Designing the Desirable Smart Home: A Study of Household's Experiences and Energy Consumption Impacts". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. CHI '18. Montreal QC, Canada: Association for Computing Machinery, 2018, pp. 1–14.

[289] Deepika Singh, Ismini Psychoula, Johannes Kropf, Sten Hanke, Andreas Holzinger, M Mokhtari, B Abdulrazak, and H Aloulou. "Users' perceptions and attitudes towards smart home technologies". In: *Smart Homes and Health Telematics, Designing a Better Future: Urban Assisted Living*. Ed. by Mounir Mokhtari, Bessam Abdulrazak, and Hamdi Aloulou. Vol. 10898 LNCS. Cham: Springer International Publishing, 2018, pp. 203–214.

[290] Jodi Forlizzi and Carl DiSalvo. "Service robots in the domestic environment". In: *Proceeding of the 1st ACM SIGCHI/SIGART conference on Human-robot interaction - HRI '06* (2006), p. 258.

[291] Sue Arthur and James Nazroo. "Designing Fieldwork Strategies and Materials". In: *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. Ed. by Jane Ritchie and Jane Lewis. 2003.

[292] John C Flanagan. "The critical incident technique." In: *Psychological bulletin* 51.4 (1954), p. 327.

[293] Rebecca E. Grinter, W. Keith Edwards, Mark W. Newman, and Nicolas Ducheneaut. "The Work to Make a Home Network Work". In: *ECSCW 2005*. Ed. by Hans Gellersen, Kjeld Schmidt, Michel Beaudouin-Lafon, and Wendy Mackay. Dordrecht: Springer Netherlands, 2005, pp. 469–488.

[294] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E. Grinter, and W. Keith Edwards. "Computer Help at Home: Methods and Motivations for Informal Technical Support". In: *27th International Conference on Human Factors in Computing Systems, CHI'09* (2009), p. 739.

[295] Norbert Nthala and Ivan Flechais. "Informal Support Networks: an investigation into Home Data Security Practices". In: *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (2018), pp. 63–82.

[296] Alex Sciuto, Arnita Saini, Jodi Forlizzi, and Jason I Hong. ""Hey Alexa, what's up?": studies of in-home conversational agent usage". In: *Proceedings of the Designing Interactive Systems conference 2018 - DIS '18* (2018), pp. 857–868.

[297] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J. Wisniewski. "Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities". In: *CSCW '20: ACM Conference on Computer Supported Cooperative Work and SocialComputing* (2020).

[298] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Nehar Kumar. "Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults". In: *Proceedings of the ACM on Human-Computer Interaction* (CSCW1 2021), p. 24.

[299] Anselm L Strauss. *Qualitative analysis for social scientists*. eng. Cambridge: Cambridge University Press, 1987.

[300] P. Emami-Naeini, Y. Agarwal, L. Cranor, and H. Hibshi. "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" In: *2020 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, May 2020, pp. 771–788.

[301] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. "The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios". In: *Proc. ACM Hum.-Comput. Interact.* 2.CSCW (Nov. 2018).

[302] Richard A. Hilbert. "Toward an Improved Understanding of "Role"". In: *Theory and Society* 10.2 (1981), pp. 207–226.

[303] Richard A Hilbert. "The status of rules in moral life". eng. In: *The classical roots of ethnomethodology : Durkheim, Weber, and Garfinkel*. Chapel Hill ; London: University of North Carolina Press, 1992, pp. 27–45.

[304] David D. Franks. *role*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007.

[305] Don H Zimmerman. "The practicalities of rule use". In: *Understanding everyday life* (1970), pp. 221–238.

[306] Anselm Strauss. "Work and the Division of Labor". In: *The Sociological Quarterly* 26.1 (1985), pp. 1–19.

[307] Andy Crabtree, Tom Lodge, James Colley, Chris Greenhalgh, and Richard Mortier. "Building Accountability into the Internet of Things". In: *SSRN Electronic Journal* (2016).

[308] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2020.

[309] Karin Niemantsverdriet, Mendel Broekhuijsen, Harm van Essen, and Berry Eggen. "Designing for Multi-User Interaction in the Home Environment". In: *Proceedings of the 2016 ACM Conference on Designing Interactive Systems - DIS '16* (2016), pp. 1303–1314.

[310] Carlos Jensen and Colin Potts. "Privacy policies as decision-making tools". In: *Proceedings of the 2004 conference on Human factors in computing systems - CHI '04*. ACM Press, 2004.

[311] Ewa Luger and Gilad Rosner. "Considering the Privacy Design Issues Arising from Conversation as Platform". en. In: *Data Protection and Privacy: The Age of Intelligent Machines*. 1st ed. Computers, Privacy and Data Protection. Oxford: Hart Publishing, Feb. 2017, pp. 193–212. URL: http://www.bloomsburycollections.com/book/data-protection-and-privacy-the-age-of-intelligent-machines/ch8-considering-the-privacy-design-issues-arising-from-conversation-as-platform/.

[312] E. Luger and T. Rodden. "Terms of Agreement: Rethinking Consent for Pervasive Computing". In: *Interacting with Computers* 25.3 (Feb. 2013), pp. 229–241. eprint: https://academic.oup.com/iwc/article-pdf/25/3/229/2595361/iws017.pdf.

[313] Chris Speed and Ewa Luger. "Sensing Data in the Home". In: *People, Personal Data and the Built Environment*. Ed. by Holger Schnädelbach and David Kirk. Cham: Springer International Publishing, 2019, pp. 123–142. URL: https://doi.org/10.1007/978-3-319-70875-1_6.

[314] Elizabeth Denham. *From facial recognition technology to children online: regulating data protection in 2021*. en. Ed. by Information Commissioner's Office UK. Mar. 2021. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/from-facial-recognition-technology-to-children-online-regulating-data-protection-in-2021/ (visited on 03/05/2021).

[315] Kenneth A. Bamberger and Deirdre K. Mulligan. *Privacy on the ground : driving corporate behavior in the United States and Europe*. eng. Information policy series. Cambridge, Massachusetts, 2015.

[316] Victoria Bellotti and W. Keith Edwards. "Intelligibility and Accountability: Human Considerations in Context-Aware Systems". In: *Hum. Comput. Interact.* 16.2-4 (2001), pp. 193–212.

[317] Anind K. Dey, Gregory D. Abowd, and Daniel Salber. "A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications". In: *Hum. Comput. Interact.* 16.2-4 (2001), pp. 97–166.

[318] Nicola Yuill and Yvonne Rogers. "Mechanisms for Collaboration: A Design and Evaluation Framework for Multi-User Interfaces". In: *ACM Transactions on Computer-Human Interaction* 19.1 (May 2012).

[319] Albert Bandura. "Social cognitive theory: An agentic perspective". In: *Annual review of psychology* 52.1 (2001), pp. 1–26.

[320] Albert Bandura. "Toward a psychology of human agency". In: *Perspectives on psychological science* 1.2 (2006), pp. 164–180.

[321] Albert Bandura. "Selective Moral Disengagement in the Exercise of Moral Agency". In: *Journal of Moral Education* 31.2 (2002), pp. 101–119. eprint: https://doi.org/10.1080/0305724022014322.

[322] Albert Bandura. "Self-Efficacy". In: *Encyclopedia of human behaviour*. Ed. by V. S. Ramachaudran. Vol. 4. Academic Press, 1994, pp. 71–81.

[323] Haiyan Jia, Mu Wu, Eunhwa Jung, Alice Shapiro, and S. Shyam Sundar. "Balancing human agency and object agency". In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*. ACM Press, 2012.

[324] Bjorn Nansen, Michael Victor Arnold, Marcus Carter, Rowan Wilken, Jenny Kennedy, and Martin R. Gibbs. "Proxy Users, Use By Proxy: Mapping Forms of Intermediary Interaction". In: *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction, OZCHI 2015, Parkville, VIC, Australia, December 7-10, 2015*. Ed. by Bernd Ploderer, Marcus Carter, Martin R. Gibbs, Wally Smith, and Frank Vetere. ACM, 2015, pp. 294–298.

[325] Albert Bandura. *Self-efficacy : the exercise of control*. eng. New York: W.H. Freeman, 1997.

[326] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. "Breaking ! A Typology of Security and Privacy News and How It ' s Shared". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI'18* (2018), pp. 1–12.

[327] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. “"We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together”. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Apr. 2020.

[328] James Nicholson, Lynne Coventry, and Pamela Briggs. “"If It’s Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI ’19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019, pp. 1–11.

[329] Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. “Co-Designing for Community Oversight: Helping People Make Privacy and Security Decisions Together”. In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019).

[330] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. “Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse”. In: *Proceedings of the New Security Paradigms Workshop*. NSPW ’19. San Carlos, Costa Rica: Association for Computing Machinery, 2019, pp. 1–15.

[331] Richard Owen. “The UK Engineering and Physical Sciences Research Council’s commitment to a framework for responsible innovation”. In: *Journal of Responsible Innovation* 1.1 (Jan. 2014), pp. 113–117.

[332] Richard Owen, Jack Stilgoe, Phil Macnaghten, Mike Gorman, Erik Fisher, and Dave Guston. “A Framework for Responsible Innovation”. eng. In: *Responsible innovation : managing the responsible emergence of science and innovation in society*. Ed. by Richard Owen, J. R. Bessant, and Maggy Heintz. Chichester: John Wiley & Sons, Ltd., 2013. Chap. 2.

[333] David Collingridge. *The social control of technology*. eng. London: Frances Pinter, 1980.

[334] European Commission. Directorate-General for Research, innovation, and René von Schomberg. *Towards responsible research and innovation in the information and communication technologies and security technologies fields*. Publications Office, 2011.

[335] Timo Jakobi, Sameer Patil, Dave Randall, Gunnar Stevens, and Volker Wulf. “It Is About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering”. In: *ACM Transactions on Computer-Human Interaction* 26.1 (Jan. 2019).

[336] Serena Zheng, Marshini Chetty, and Nick Feamster. “User Perceptions of Privacy in Smart Homes”. In: (2018).

[337] Stuart Reeves. “Envisioning Ubiquitous Computing”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ’12. Austin, Texas, USA: Association for Computing Machinery, 2012, pp. 1573–1582.

[338] Marina Jirotka, Barbara Grimpe, Bernd Stahl, Grace Eden, and Mark Hartswood. “Responsible research and innovation in the digital age”. In: *Communications of the ACM* 60.5 (Apr. 2017), pp. 62–68.

[339] Batya Friedman, Peter H Kahn, and Alan Borning. “Value sensitive design and information systems”. In: *The handbook of information and computer ethics* (2008), pp. 69–101.

[340] Yaxing Yao, Davide Lo Re, and Yang Wang. “Folk Models of Online Behavioral Advertising”. In: CSCW ’17 (2017), pp. 1957–1969.

[341] Joel E. Fischer, Andy Crabtree, Tom Rodden, James A. Colley, Enrico Costanza, Michael O. Jewell, and Sarvapali D. Ramchurn. ""Just whack it on until it gets hot"". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16* (2016), pp. 5933–5944.

[342] Richard Mortier, Hamed Haddadi, Tristan Henderson, Derek McAuley, and Jon Crowcroft. "Human-Data Interaction: The Human Face of the Data-Driven Society". In: *SSRN Electronic Journal* (2014).

[343] Peter Tolmie and Andy Crabtree. "The practical politics of sharing personal data". In: *Personal and Ubiquitous Computing* 22 (2 2018), pp. 293–315.

[344] Peter Tolmie, Andy Crabtree, Tom Rodden, James A Colley, and Ewa A Luger. ""This has to be the cats" - Personal Data Legibility in Networked Sensing Systems". In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16*. ACM Press, 2016.

[345] Andy Crabtree, Lewis Hyland, James Colley, Martin Flintham, Joel E. Fischer, and Hyosun Kwon. "Probing IoT-based consumer services: 'insights' from the connected shower". In: *Personal and Ubiquitous Computing* 24.5 (Sept. 2019), pp. 595–611.

[346] Carol Moser, Sarita Y. Schoenebeck, and Katharina Reinecke. "Technology at the Table". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, May 2016.

[347] Mark S. Ackerman. "The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility". In: *Hum. Comput. Interact.* 15.2-3 (2000), pp. 179–203.

[348] Sauvik Das. "Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity". In: *it - Information Technology* 58.5 (2016), pp. 237–245.

[349] Grazyna Kochanska, Katherine C Coy, and Kathleen T Murray. "The development of self-regulation in the first four years of life". In: *Child development* 72.4 (2001), pp. 1091–1111.

[350] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. "A Typology of Perceived Triggers for End-User Security and Privacy Behaviors". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 97–115.

[351] Fabio Massacci and Viet Hung Nguyen. "Goal-Oriented Access Control Model for Ambient Assisted Living". In: *Privacy and Identity Management for Life - 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7-11, 2009, Revised Selected Papers*. Ed. by Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen, and Ge Zhang. Vol. 320. IFIP Advances in Information and Communication Technology. Springer, 2009, pp. 160–173.

[352] NN Nthala and I Flechais. "Rethinking home network security". In: *Proceedings of EuroUSEC 2018 – The 3rd European Workshop on Usable Security*. Internet Society, 2018.

[353] Lynn Schofield Clark. "Parental mediation theory for the digital age". In: *Communication theory* 21.4 (2011), pp. 323–343.

[354] Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. "Managing expectations: Technology tensions among parents and teens". In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM. 2016, pp. 1390–1401.

[355] Anna L. Cox, Sandy J.J. Gould, Marta E. Cecchinato, Ioanna Iacovides, and Ian Renfree. "Design Frictions for Mindful Interactions: The Case for Microboundaries". In: *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. CHI EA '16. San Jose, California, USA: Association for Computing Machinery, 2016, pp. 1389–1397.

[356] Z.V. Segal, M. Williams, J. Teasdale, and J. Kabat-Zinn. *Mindfulness-Based Cognitive Therapy for Depression, Second Edition*. Guilford Publications, 2018.

[357] BJ Fogg. "A Behavior Model for Persuasive Design". In: *Proceedings of the 4th International Conference on Persuasive Technology*. Persuasive '09. Claremont, California, USA: Association for Computing Machinery, 2009.

[358] Harry C. Triandis and Harry Charalambos Triandis. *Individualism & Collectivism*. New directions in social psychology. Routledge, 2018.

[359] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. "Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia". In: *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*. SOUPS '15. Ottawa, Canada: USENIX Association, 2015, pp. 297–308.

[360] Information Commissioner's Office. *Age appropriate design: a code of practices for online services*. May 6, 2021. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/.

[361] Liz Dowthwaite, Helen Creswick, Virginia Portillo, Jun Zhao, Menisha Patel, Elvira Perez Vallejos, Ansgar Koene, and Marina Jirotka. ""It's Your Private Information. It's Your Life.": Young People's Views of Personal Data Use by Online Technologies". In: *Proceedings of the Interaction Design and Children Conference*. IDC '20. London, United Kingdom: Association for Computing Machinery, 2020, pp. 121–134.

[362] Diogo Marques, Tiago Guerreiro, Luis Carriço, Ivan Beschastnikh, and Konstantin Beznosov. "Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, 2019, pp. 1–13.

[363] Stuart Schechter. "The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button!" In: *Proceedings of the Workshop on Home Usable Privacy and Security (HUPS)*. July 2013.

[364] Jayoung Sung, Henrik I Christensen, and Rebecca E Grinter. "Robots in the Wild: Understanding Long-term Use". In: *Proceedings of the 4th ACM/IEEE international conference on Human robot interaction*. 2009, pp. 45–52.

[365] Eric P.S. Baumer and M. Six Silberman. "When the Implication is Not to Design (Technology)". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '11. Vancouver, BC, Canada: Association for Computing Machinery, 2011, pp. 2271–2274.

[366] William H. Swatos, Jr. *Hawthorne Effect*. In: *The Blackwell Encyclopedia of Sociology*. Ed. by George Ritzer. John Wiley & Sons, Ltd, 2007, pp. 2050–2051.

[367] David Oswald, Fred Sherratt, and Simon Smith. "Handling the Hawthorne effect: The challenges surrounding a participant observer". In: *RoSS* 1.1 (Nov. 2014), pp. 53–74.

[368] Andy Crabtree and Richard Mortier. “Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control”. In: *Ssrn* (2016), pp. 1–20.