I always feel like something is watchin' me, and I have no privacy
–
Privacy Calculus and Data-Tracking as Determinants of IoT-Acceptance

Von der Fakultät für Ingenieurwissenschaften
Abteilung Informatik und Angewandte Kognitionswissenschaft
der Universität Duisburg-Essen

zur Erlangung des akademischen Grades

Doktor der Philosophie (Dr. phil.)

genehmigte Dissertation

von

Evgenia Princi
aus
Moskau, Russland

1. Gutachterin: Prof. Dr. Nicole Krämer
2. Gutachter: Prof. Dr. Torben Weis

Datum der mündlichen Prüfung: 9. Dezember 2020

“Neither privacy nor publicity is dead,
but technology will continue to make a mess of both.”

- Danah Boyd

ACKNOWLEDGEMENTS

The path towards this dissertation has been inspiring and challenging, broadening my horizon in so many ways. Its completion is an achievement that was accomplished with the help of wonderful people who have supported and encouraged me from the beginning and to whom I would like to express my deepest gratitude.

I would like to thank Prof. Dr. Nicole Krämer for her support and for the most constructive and valuable feedback, always aimed at moving me forward. Thank you for your encouragement and trust, which fundamentally strengthened my self-confidence as a researcher.

I want to thank Prof. Dr. Torben Weis for his kind words and for many inspiring technological insights at our project meetings. I am already looking forward to further collaboration.

I wish to thank all the people from the best team in the world whose support was a milestone in the completion of this project. I appreciate all of our conference trips, afterwork drinks and (unintended) train journeys. Most of all, I would like to thank Judith Meinert and Johanna Schäwel for reading this thesis and giving me thorough and helpful feedback. Thanks to Aike Horstmann, Jessica Szczuka, Filipa Stoyanova, Elias Kyewski and Jan Kluck. Sharing thoughts, successes and challenges with you made work a pleasure every day. I want to thank Yannic Meier for being a great colleague and an amazing fried. Thank you for all the inspiring conversations, the exhilarating punk concerts and tons of adventures that will stay in my memory for a lifetime.

Thanks to my sister, Marianna. Your great expectations of me always kept me motivated and I am grateful for your confidence and for teaching me that you never know what you can do until you try.

I am incredibly grateful for the endless love and devotion of my mother, Maria. Thank you for always being proud of me. I have only come this far because you have made this life possible and it was all of your difficult decisions that finally led to this success. It is as much your merit as it is mine.

Above all, I would like to recognize the invaluable role of my husband, Giuliano Princi. Grazie per il tuo amore incondizionato, la tua comprensione e la tua incrollabile fiducia in me. Con il tuo sostegno posso superare ogni sfida e diventare la migliore versione di me stessa. Uno per uno, mi aiuti a realizzare tutti i miei sogni d'infanzia. Questo lavoro non sarebbe stato possibile senza di te. Team Princi est. 2004.

I dedicate this work to my wonderful children, Vittorio and Valentino.
Thank you for your patience and for showing me what really matters.
I love you to the moon and back.

ANNOTATION OF THE PAPERS INCLUDED IN THE CUMULUS

Research Paper 1:

Princi, E., & Krämer, N.C. (2020, January). I Spy with my Little Sensor Eye – Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology. In *Proceedings of the 53rd Hawaii International Conference on System Sciences,* 1391-1400. https://doi.org/10.24251/HICSS.2020.171

Research Paper 2:

Princi, E., & Krämer, N. C. (2020). Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices. *Frontiers in Psychology.* https://doi.org/10.3389/fpsyg.2020.582054

Research Paper 3:

Princi, E., & Krämer, N. C. (2019). Acceptance of Smart Electronic Monitoring at Work as a Result of a Privacy Calculus Decision. *Informatics, 6*(3), 40-59. https://doi.org/10.3390/informatics6030040

ABSTRACT

The growing deployment of interconnected technology from the Internet of Thins (IoT) is increasingly challenging the common understanding of privacy. The interdependencies between users' psychological mechanisms, technical dynamics of IoT and context-specific factors require a profound evaluation of privacy-related perceptions and behaviors under consideration of user-centric and system-based perspectives. The present dissertation contributes to the burgeoning research on privacy in the framework of IoT and aims at providing valuable insights regarding the acceptance of interconnected technologies. For this purpose, the thesis first reflects on relevant theoretical foundations including the privacy calculus theory, privacy concerns and the selective control of information from the socio-psychological perspective. Additionally, a new differentiation of the human and the technological levels of privacy is suggested in this work as a result of a combinatory approach from existing privacy theories. Against the background of privacy-related characteristics in IoT environments, particular challenges of empirical investigations of IoT are addressed. The present cumulus comprises three empirical studies, which provide results on the investigation of privacy calculus in three different fields of IoT application – smart home, healthcare and workplace. The examination of IoT in different contexts confirms that privacy calculus can be transferred as a theoretical basis for investigations of IoT as people weigh perceived risks against anticipated gratifications prior to their decision to use and accept a particular IoT device. However, given the limited possibilities of IoT users to control data collection, data processing or inferencing of information from sensor data, it is assumed that the outcome of privacy calculus in the framework of interconnected technologies changes towards a binary decision: to accept or reject a particular IoT device. Furthermore, the contextual perspective contributes to the identification of situation-specific factors of IoT deployment. The overarching discussion addresses the growing debate around privacy threatening technologies and, in addition to a critical reflection of the privacy calculus, elaborates on extensions of current privacy theories as a result of the adoption of IoT technology. Following theoretical considerations and the results of the three scientific articles, which constitute the present thesis, practical implications are provided with the aim to strengthen informational self-determination of individuals through legislation or a more profound consideration of user privacy in the development process of IoT products and services. Moreover, ethical implications suggest different approaches on how to deal with issues regarding discrimination or injustice as possible consequences of IoT dissemination. Finally, an outlook for future research on privacy in the framework of IoT is provided.

ZUSAMMENFASSUNG

Der wachsende Einsatz vernetzter Technologien aus dem Internet der Dinge (IoT) stellt das generelle Verständnis von Privatheit zunehmend in Frage. Die Wechselwirkungen zwischen den psychologischen Mechanismen der Nutzenden, den technologiebedingten Dynamiken von IoT sowie den kontextspezifischen Faktoren erfordern eine tiefgreifende Auseinandersetzung mit den Wahrnehmungen und Verhaltensweisen von Individuen in Bezug auf die Privatheit, unter Berücksichtigung nutzerzentrierter und systembasierter Perspektiven. Die vorliegende Dissertation trägt zur aufkeimenden Privatheitsforschung im Rahmen von IoT bei und soll einen wesentlichen Einblick hinsichtlich der Akzeptanz gegenüber vernetzten Technologien ermöglichen. Zu diesem Zweck werden zunächst relevante theoretische Grundlagen aus sozialpsychologischer Perspektive reflektiert, darunter die Privacy Calculus Theorie, Privatheitsbedenken sowie die selektive Kontrolle von Informationen. Darüber hinaus wird in dieser Arbeit eine neue Differenzierung der menschlichen und der technologischen Ebenen der Privatheit vorgeschlagen, als Ergebnis eines kombinatorischen Ansatzes in Bezug auf bestehende Privatheitstheorien. Des Weiteren werden besondere Herausforderungen empirischer Untersuchungen von IoT, vor dem Hintergrund privatheitsbezogener IoT-Charakteristika, erörtert. Der vorliegende Kumulus umfasst drei empirische Studien, welche Ergebnisse bezüglich der Anwendung des Privacy Calculus in drei unterschiedlichen Einsatzfeldern von IoT liefern - Smart Home, Gesundheitswesen und Arbeitsplatz. Die Untersuchung von IoT in verschiedenen Anwendungskontexten bestätigt, dass der Privacy Calculus als theoretische Grundlage auf die weitere IoT-Erforschung transferiert werden kann, da Menschen vor ihrer Entscheidung hinsichtlich der Nutzung und der Akzeptanz eines bestimmten IoT-Gerätes wahrgenommene Risiken gegen zu erwartende Gratifikationen abwägen. Angesichts der für den Nutzer eingeschränkten Kontrollmöglichkeiten der Datenerfassung, -verarbeitung und Schlussfolgerung aus Sensordaten wird jedoch angenommen, dass sich das Ergebnis der Privacy Calculus-Analyse im Rahmen vernetzter Technologien auf eine binäre Entscheidung reduziert – die Nutzung eines bestimmten IoT-Gerätes zu akzeptieren oder abzulehnen. Darüber hinaus trägt die kontextbezogene Perspektive zur Identifizierung von situationsspezifischen Faktoren der IoT-Nutzung bei. Die übergreifende Diskussion befasst sich mit der wachsenden Debatte bezüglich privatheitsbedrohender Technologien und arbeitet, zusätzlich zur kritischen Reflexion des Privacy Calculus, notwendige Erweiterungen für bestehende Privatheitstheorien, als Folge der Einführung von IoT-Technologien, heraus. Im Anschluss an theoretische Überlegungen und die Ergebnisse der

drei wissenschaftlichen Artikel, die Bestandteil der vorliegenden Arbeit sind, werden praktische Implikationen aufgezeigt mit dem Ziel, die informationelle Selbstbestimmung des Individuums durch Gesetzgebung oder eine umfassendere Berücksichtigung der Privatheit der Nutzenden im Entwicklungsprozess von IoT-Produkten und -Services zu stärken. Ferner legen die ethischen Implikationen verschiedene Ansätze nahe, wie Fragen der Diskriminierung oder Ungerechtigkeit, als mögliche Folge der Verbreitung von IoT, begegnen werden kann. Schließlich wird ein Ausblick auf die zukünftige Privatheitsforschung im Rahmen von IoT vorgestellt.

TABLE OF CONTENTS

LIST OF FIGURES

I INTRODUCTION

The increasing technologization of our everyday lives constantly confronts people with the fact that their personal data is collected, analyzed and used as a basis for the development of new products and services. In the course of the digital change, a significant contribution can be attributed to the Internet of Things (IoT). IoT represents a technological revolution striving at a global network of interconnected devices and applications, which gather and exchange various data providing so-called smart solutions in order to support people in their routine (Gudymenko et al., 2011). Smart voice controller, learning thermostats, fitness-trackers, smart locks, air quality monitors, app- and voice-controlled lighting systems or smart security solutions are all increasingly affordable and enjoy growing popularity. The implementation of IoT is particularly attractive for consumers, as this innovative technology promises the greatest possible comfort, e.g., in terms of personalized services tailored to users' preferences (Zheng et al., 2018).

However, this comfort comes at a price. The basis for personalized services and various other functions of IoT are person-related data captured by sensors, which are embedded in household appliances, wearables and other connected devices (Kröger, 2019). This means that the deployment of IoT enables an unprecedented accessibility of an individual's behavioral and environmental information due to its unobtrusive mode of operation. Consequently, IoT poses a significant challenge for privacy. Given the lack of predefined standards regarding data extraction, ownership, storage and intended use, it is often unclear, what data is collected, how it is managed and who has access to it (Zheng et al., 2018). Consequently, uncertainties associated with privacy implications of IoT raise concerns among users (Zheng et al., 2018). The investigation of individuals' privacy concerns in relation to IoT usage is of utmost importance, not only to illuminate the impact of networked everyday objects on informational self-determination but also to explain psychological mechanisms underlying the perception of privacy risks and the acceptance of privacy threatening technology.

Empirical research on user privacy, which addresses questions regarding the impact of IoT that is increasingly surrounding us has to date been strongly limited to technically focused scientific disciplines (Pötter & Sztajnberg, 2016; Rizal et al., 2018; Scarpato et al., 2017; van Kranenburg & Bassi, 2012; Zhou et al., 2019). However, scholars comprehensively explored the relationship of privacy and the usage of Internet applications in the framework of online communication (Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2010) or electronic commerce (e-commerce; Dinev & Hart, 2006). The initially established *privacy paradox*

(Barnes, 2006), which characterizes the contradictory behavior of people expressing privacy concerns but nevertheless sharing their private data online, is increasingly considered obsolete as newer research approaches aim to open the black box behind the seemingly paradoxical behavior (Krämer & Schäwel, 2020). A well-established and prominent approach is the *privacy calculus theory*, which states that the decision to disclose private data is dependent on a careful balancing of perceived privacy risks and anticipated gratifications (Culnan & Armstrong, 1999). Previous studies mostly investigated privacy calculus in the context of social networking sites (SNS) or other websites. The present dissertation contributes to the burgeoning literature on the topic of privacy in relation to interconnected technologies by applying the well-studied privacy calculus approach to the IoT context in order to address the tension that arises between the rapidly expanding usage of connected, data-tracking devices and individual privacy. Simultaneously, one of the main goals of this work is to elaborate on the privacy calculus concept as privacy decisions in the context of IoT are not always rational as proposed by this theory (Acquisti et al., 2016; Masur, 2018).

In the second chapter of this thesis the theoretical background is outlined, which forms the basis for the empirical studies included in the cumulus and serves as an argumentative framework for the following discussion. This chapter examines how the fundamental understanding of privacy evolves in the context of IoT. This includes the consideration of established privacy theories and the elaboration of relevant factors that facilitate or inhibit IoT acceptance with respect to privacy. As the main theoretical contribution, I propose an integrative approach towards the differentiation of the privacy construct into two different levels to meet the specifications of the interplay between technology and individual. Furthermore, particular IoT characteristics are introduced in order to shape a fundamental understanding of the functionality of this innovative technology as a necessary prerequisite for a holistic view of its thematic intersection with privacy. The last sections of the second chapter address the challenges of empirical investigations of IoT from the socio-psychological perspective including the ethical debate around IoT, the heterogeneity of connected devices and the various contexts of its application.

The third chapter introduces three published research articles, which constitute this cumulative dissertation. In this chapter, the research objectives of the current thesis are articulated, followed by brief descriptions of each manuscript. To provide a differentiated picture of the acceptance of IoT, the empirical studies focus on three different areas: the private use of smart household appliances, the implementation of networked monitoring technology at the workplace and the use of a fitness device in the context of healthcare. In addition, the studies differ in the investigation of context-specific factors, which are intended to provide deeper insight into the perceptual processes of IoT users in the respective situation. Thus, the cumulus contributes to (1) discuss theoretical approaches attempting to explain psychological mechanisms behind the usage of IoT with a specific focus on the privacy calculus, (2) provide valuable insight on the privacy threatening potential of IoT regarding person-related data and the challenges of its empirical investigations, and (3) presents results of quantitative investigations of IoT in three different contexts: smart home, healthcare and workplace.

The last chapter reflects on the findings of the empirical studies conducted in the context of this thesis against the background of the elaborated theoretical considerations. The resulting theoretical, practical and ethical implementations are intended to motivate better design practices and regulations regarding the development of IoT applications and products to protect individual's privacy and maintain informational self-determination without entirely shifting the responsibility to the user.

II THEORETICAL BACKGROUND

2.1 Privacy in the Digital Age

Since one of the first legal attempts to define privacy as “the right to be let alone“ (Warren & Brandeis, 1890, p. 193), scholars in different scientific fields contributed to the conceptualization of privacy, particularly emphasizing its relevance for the individual as well as its societal significance (Kokolakis, 2017; Trepte et al., 2017). For the purpose of this thesis, the psychological understanding of privacy is examined in more detail. This understanding is substantially shaped by the privacy pioneer and legal researcher Alan Westin (1967), stating that “privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (p. 5). Against the background of progressive technological advancements, privacy is increasingly compromised, as it is often impossible for users to regulate, when and what information is tracked by which technology with which purpose. This can be exemplified by Westin’s (1967) definition. When deploying IoT, individuals cannot always determine for themselves, *when* information about them is communicated to others. While some devices only capture data during their activity, others are permanently connected including transmission of extracted information. Additionally, information might be accessed at all times, if devices store it online (Shen et al., 2019). Individuals also cannot always determine *how* information about themselves is accessed: are only those data affected that users provide voluntarily and intentionally (e.g., specifying age and weight when using the fitness tracker) or is information involved that is tracked without user awareness or consent (e.g., sleep cycles, Eibl & Engel, 2015)? Neither can individuals necessarily determine, *to what extent* information about themselves is accessed as IoT applications can collect single, unrelated data or merge various user information via data linkage from multiple sources in order to infer new information (e.g., behavioral predictions or preferences) by means of algorithms (Feng et al., 2018). Lastly, individuals cannot always determine, *to whom* information about themselves is communicated. Does only the user have access (e.g., in the case of locally stored data), is the data utilized by manufacturers to improve algorithms, sold for advertising purposes or even shared with employers or authorities (Chinaei et al., 2020)? These foibles also reappear in Petronio’s (2002) *Communication Privacy Management Theory* (CPM), which posits that people consciously determine privacy rules and hence control the ownership of their data. Principally, this can only be achieved, if all parameters of data collection and processing are available. Otherwise, individuals will fail due to the substantial number of uncertainties in IoT environments.

With the inclusion of Irwin Altman's (1975) definition of privacy “as the selective control of access to the self or to one’s group” (p. 18), the socio-psychological perspective considers privacy as a controllable and dynamic construct. This means that the need for privacy varies between individuals and depends on the situational context. With regard to IoT, these factors seem insufficient when describing the need for privacy. Additionally, the kind of provided data and its handling must be taken into account as the need for privacy might depend on the sensitivity of certain information and whether it is permanently stored or forwarded to third parties. Judee Burgoon (1982) takes up the aspect of controllability and moreover, expands on the concept of privacy by introducing a multidimensional angle. The interrelated dimensions include *informational privacy* (i.e. identifiable data), *social privacy* (i.e. relationships or personal encounters), *physical privacy* (i.e. personal space) and *psychological privacy* (i.e. one’s thoughts, feelings and values). Accordingly, privacy could be regarded as a metaphorical regulator between complete withdrawal and social interaction, which can be gradually shifted depending on the individual need for privacy and the situational conditions.

Atlam and Wills (2020) suggest a more contemporary approach when defining privacy in the IoT framework. More precisely, they postulate that privacy is constituted by four components: *information*, *communication*, *body* and *territory*. At first sight, this perspective intersects with the interpretation of Burgoon (1982). Similar to the dimensions of privacy, “Information privacy is related to various types of personal data collected and processed by an organization, such as financial and medical information, while the privacy of communication is concerned with protecting data sent between two communicating nodes using any communication medium” (Atlam & Wills, 2020, p. 138). Thus, the authors’ understanding of the communication component shows parallels to the social dimension of privacy, by addressing the aspect of information exchange. A closer look, however, reveals that the focus is on the technologically mediated dissemination of information between connected entities, rather than on information about social interactions. Furthermore, the authors specify two different components, which correspond to Burgoon’s (1982) physical dimension of privacy, that are body (individual’s physical integrity) and territory (physical environment, e.g., home or public places). In this way, they ascribe particular significance to the ability of IoT to access physical data outside the online environment. However, it should be mentioned that the newer approach by Atlam and Wills (2020) seems to completely neglect the fact that IoT is capable of mood detection (Chacko & Bharati, 2018) or inferences regarding personal preferences

(Ziegeldorf et al., 2014), which corresponds to the psychological privacy dimension of Burgoon (1982).

These elaborations exemplify that privacy is essential to autonomy, freedom and personal well-being. However, it becomes obvious that theoretical implications of privacy are mostly related to offline communication describing face-to-face interaction in the pre-Internet era. With absence of data tracking technology, a possibility of early privacy management was "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" (Westin, 1967, p. 7). Online communication (especially through SNS) shifts privacy boundaries and at the same time expands the possibilities of self-disclosure by allowing users not only to actively reveal their data to a broader audience (e.g., comments and location; Kazai et al., 2016) but also to have data collected by the system (likes or time spent on particular posts; e.g., Matz et al., 2020). However, given the ubiquity and unobtrusiveness of IoT and its entanglement in diverse areas of life (e.g., work, health, transportation), it is becoming increasingly difficult for individuals to shield themselves from data collection. Referring to Burgoon's (1982) privacy dimensions, the user becomes more transparent than ever before. The reason for this is that while previous research on online communication primarily addressed informational privacy (e.g., Dienlin & Metzger, 2016), the application of IoT, however, also encompasses the other three dimensions when it comes to potential privacy threats (Schomakers et al., 2020). Nevertheless, people continue to use IoT and thereby grant access to sensitive, private data. In order to provide a better understanding of the underlying psychological mechanisms of users' privacy decisions, the following chapters discuss well-studied theoretical privacy perspectives that have been investigated in the context of online communication and transfer their applicability to the field of IoT.

2.1.1 A Balancing Process: The Privacy Calculus

Barnes (2006) was one of the first scholars to draw scientific interest towards the paradoxical behavior of individuals when using online services. In her study, she showed that users of social networking sites are concerned about privacy, but at the same time appear generous when it comes to disclosing personal data indicating discrepancies between privacy attitudes and behavior (Norberg et al., 2007). This *privacy paradox* is increasingly considered obsolete, as a growing body of literature made attempts to explore the mental processes behind people's paradoxical privacy behavior. One of the most popular approaches explaining the privacy paradox is the *privacy calculus theory*. Based on considerations from Laufer and Wolfe (1977), suggesting that people, prior to engaging in certain behaviors, evaluate its positive and negative outcomes, the theory represents a privacy decision-making process. More precisely, the model postulates that individuals weigh potential privacy risks against anticipated benefits in order to decide whether to provide personal data or not (Culnan & Armstrong, 1999). This assumption follows the theory of reasoned action (Ajzen & Fishbein, 1980) and the theory of planned behavior (Ajzen, 1991), which assume that individual perceptions have a significant influence on behavioral intentions. In this regard, Dinev and Hart (2006) state that privacy risks and expected gratifications of self-disclosure, as contrary beliefs, play a crucial role for the intention to disclose personal information. Looking closer at individuals' calculation of beliefs, the authors argue that "The influence of one belief might override another to the extent that the resulting probability favors one behavioral intention over another" (p. 62). Concretely, this means that if the expected benefits override privacy threats, individuals share their data, which leads to the ostensibly paradoxical behavior. Privacy calculus is widely applied as a theoretical framework for studies on online communication (Bol et al., 2018; Chen, 2018; Dienlin & Metzger, 2016) and e-commerce (Dinev & Hart, 2006). Krasnova and colleagues (2010) found that users of social networking sites disclose personal information in order to maintain relationships or because they enjoy using these platforms. In contrast, perceived privacy risks, such as data misuse or identity theft, are negatively related to self-disclosure (Krasnova et al., 2010). Dienlin and Metzger (2016) extended the privacy calculus model demonstrating that expected benefits are a determinant for self-disclosure on SNS whereas self-efficacy poses an influencing factor for self-withdrawal. Trepte and colleagues (2017) moreover revealed the impact of cultural differences on the trade-off between anticipated gratifications and privacy risks.

Shifting the focus to IoT, the benefits of providing personal data seem even more diverse. For example, smart thermostats offer economic and environmental advantages (Lu et al., 2010) while fitness trackers help improving one's health through self-quantification (Gilmore, 2016). A recent study demonstrated privacy calculus as an underlying decision-process prior to adoption of mobile health technologies, however, emphasizing that the risk-benefit trade-off is skewed due to the overestimation of benefits and the underestimation of privacy risks (Fox, 2020). Findings from Zheng and colleagues (2018) indicate that a distinctive reason for IoT adoption is convenience (e.g., central control of deployed devices) and that people even tend to disregard privacy threats in order to profit from convenient IoT features. This lends further support to the privacy calculus and corroborates previous research regarding the stronger impact of anticipated benefits (Lee et al., 2018; Wang et al., 2016; Zheng et al., 2018). Nevertheless, privacy threats are particularly severe, as the amount and heterogeneity of gathered data within the usage of IoT surpasses personal information that is solely tracked in online environments (e.g., on SNS or websites; Shahraki & Haugen, 2018). In addition to uncertainties regarding purpose of data collection and its handling by different stakeholders, data synchronization within one's IoT ecosystem might enable access to any sensitive information including inferences about home-occupancy up to the possibility of external control of devices by unauthorized parties in case of a hacker attack (Kröger, 2019; Rizal et al., 2018).

These considerations point out that both the advantages and the privacy risks of IoT are quite manifold. Following the principles of privacy calculus, all of them must be taken into account when deciding to deploy IoT and provide personal information. Thus, taken in absolute terms, privacy calculus assumptions are grounded on the rationally acting individual with full agency (Dinev & Hart, 2006). Many scholars regard this concept as controversial. First, not all privacy-relevant information is accessible for users, leading to asymmetrical decision requirements (Masur, 2018). Acquisti and colleagues (2016) further express substantial criticism regarding the reasoned individual due to bounded rationality of users. More precisely, they state that "both the inability to calculate probabilities and amounts for risks and related costs for the various possible individual strategies, but also […] the inability to process all the uncertain and stochastic information related to information security costs and benefits" (Acquisti & Grossklags, 2006, p. 9) inhibit an effectively rational decision. In other words, even if detailed information is available, e.g., by provision of privacy policies, privacy decision processes seem to be conditioned by limited cognitive resources of individuals (Simon, 1982).

Another aspect is stressed by more recent literature, which attributes the disproportionate weighing of risks and benefits to deeply rooted cognitive biases (Adjerid et al., 2013; Krämer & Schäwel, 2020; Matz et al., 2020). Biases are oftentimes a result of heuristic thinking, which represents timesaving and habituated mental shortcuts in case of uncertainties (Tversky & Kahneman, 1974). Waldman (2020) argues that technology companies manipulatively exploit users' cognitive barriers in order to persuade them into sharing more data and specifies the five most pervasive biases potentially leading to suboptimal privacy decisions: *anchoring* defines the tendency to base a decision on a certain reference (e.g., provide more data, when others do, too; Acquisti et al., 2012). *Framing* puts aspects in a positive or a negative context, which in turn may impact a decision (positively framing disclosing behavior while diminishing privacy risks; Adjerid et al., 2013). *Hyperbolic discounting* concerns inter-temporal choices and implies that immediate gratification may outweigh privacy risks expected in the future (Acquisti & Grossklags, 2005; Wang et al., 2011). *Overchoice* refers to the numerous privacy options IoT users are faced with (Waldman, 2020). Yet, it is not the actual choice but the quantity of privacy choices which might overwhelm the user (Hartzog, 2018). Finally, *metacognitive processes* may lead people, who recognize privacy decisions as particularly difficult, to not engage in privacy protection in the first place (Waldman, 2020).

Hence, diverse cognitive barriers to a certain degree might decrease the effectiveness of the rational choice model, which is particularly challenging for users of IoT. Given that device manufacturers and service providers strongly rely on extensive user data, they might systematically leverage users' cognitive limitations and biases in order to get access to personal data (Calo, 2014; Mathur et al., 2019), thus skewing the balancing process of privacy calculus in their favor.

In addition to the criticized foibles of privacy calculus, Masur (2018) emphasizes the role of situational context, which most studies do not take into account, "Consequently, these findings can only be regarded as an aggregated representation of several situationally varying decision processes that involved a privacy calculus" (Masur, 2018, p. 115). Context-specific characteristics of IoT is a major challenge when it comes to investigations of this technology and will be discussed in more detail in Chapter 2.3.3 (Context-specific dynamics of IoT). Still, privacy calculus is an adequate basis for understanding users' motivation to provide personal data, as privacy-related decision might "seem irrational to an external observer, but at the same time fairly rational to the decision maker" (Gerber et al., 2018, p. 6). Consequently, the individual concept of privacy along with the subsequent decisions, either to provide or to withhold information, seems to be substantially shaped by subjective perceptions of users in terms of potential risks, benefits and its control. In the following, the latter is discussed in more detail.

2.1.2 Selective Control of Information

Individual control of personal information is considered an inherent element of the socio-psychological understanding of privacy (Altman, 1976; Petronio, 2002). Fried (1984) points out that these two concepts, control and privacy, cannot be examined in isolation, by stating that "Privacy is not simply an absence of information about us in the minds of others, rather it is the *control* we have over information about ourselves" (p. 209). Building on this, Masur, Teutsch and Trepte (2017) postulate that people engage in optimization processes by selectively controlling whether they provide distinct information, and that these processes are substantially challenged with regard to digitalization. Already in the early days of the Internet, Tavani and Moor (2001) noted that "As a practical matter we cannot possibly control vast amounts of information about us that circulates through myriads of computer networks and databases. The current globalization of these information processes exacerbates the problem" (p. 6). In their explanations, the authors refer mainly to informational privacy. IoT technology, however, also comprises social, psychological and physical privacy (Burgoon, 1982), which poses an even greater threat to privacy as more diverse information is made accessible. Moreover, given the enhanced capabilities of IoT to automatically collect and process data or use algorithms in order to generate inferences (Feng et al., 2018, Kröger, 2019), maintaining control of personal data becomes more and more complex. Nevertheless, the proposal of Tavani and Moor (2001) for a more sophisticated privacy protection seems to be transferable to the context of IoT. To be more precise, the authors argue that in addition to individual control over the dissemination of personal information, external control is required, for example in the form of privacy-enhancing technologies (PETs; such as privacy policies). In this regard, literature distinguishes between actual and perceived control (Hajli & Lin, 2016; Skinner, 1996). Actual control correspond to external control suggested by Tavani and Moor (2001) and represents general possibilities for individuals to control who receives access to what information, regardless of individual's awareness of these options. As for IoT, controlling mechanisms are mostly provided by technological means, such as privacy settings. This means that data, which a device is allowed to collect, and the purpose of its use can be determined either by default or through active changes of privacy settings by the user. However, it is often difficult to measure a person's objective level of control in a situation. Therefore, Ajzen (2005) proposes the concept of perceived control. In contrast to actual control, perceived control resembles Tavani and Moor's (2001) understanding of individual control and describes the extent, to which an individual feels to be in control over a situation or person (Ajzen, 2005). In socio-psychological privacy research, perceived control poses a more prominent approach due to its greater effect on privacy behavior than actual control (Averill, 1973; Burger, 1989; Skinner, 1996). Perceived control has been found to predict users' willingness to provide personal, even identifiable, information (Brandimarte et al., 2013; Gerber et al., 2018). Furthermore, perceived control strongly correlates with privacy concerns (Hajli & Lin, 2016; Malhotra et al., 2004; Xu, 2007). To be more specific, Krasnova and colleagues (2010) demonstrated that users of SNS indicate reduced privacy concerns and a higher level of security when they perceive to be in control of their personal information. Also Gerber and colleagues (2018) confirmed that perceived control, as a situation-specific factor, negatively affects privacy concerns. However, the relation between control and privacy concerns might be grounded on a misconception of individuals regarding the possibilities to control their information. In the study by Brandimarte and colleagues (2013) people indicated to have less privacy concerns and a higher willingness to share sensitive information, when they were provided with control over the publication of these data. At the same time, the more relevant control over both the access to personal information and its usage by others, was not significant to individuals, which the authors refer to as the control paradox. Less control over information publication, in contrast, led to higher privacy concerns, even when access to and usage of private information was unlikely. As privacy concerns has been found to diminish individual's willingness to provide personal information or to engage in online transactions (Dinev & Hart, 2006; Van Slyke et al., 2006), the next chapter takes a closer look on this construct in order to elaborate on the role of individuals' privacy concerns against the background of IoT.

2.1.3 Privacy Concerns

In the digitalized world, the wide accessibility and dissemination of personal data through the use of websites, smartphones and other tracking technologies, such as IoT, gives cause for substantial privacy concerns. Compared to 71% in 2017, two years later only 59% of respondents indicated that they might protect themselves sufficiently against misuse of their personal data or identity theft (European Commission, 2020). While numerous studies on privacy concerns in the context of online communication and SNS usage provide inconclusive results (Baruh et al., 2017), there are comparatively few studies investigating privacy concerns of IoT users, despite its relevance within this field. With regard to the role of privacy concerns in IoT research, Apthorpe and colleagues (2017) state that "IoT devices for smart homes are becoming increasingly pervasive; however, the privacy concerns of owning many Internet connected devices with always-on environmental sensors remain insufficiently addressed" (p. 5). In their study on technologies, which use location based services (LBS; i.e. services depending on users' geographic data), Xu and Teo (2004) demonstrate that individuals worry about privacy violation in connection to disclosure of their location. Moreover, the authors show a negative effect of privacy concerns on the willingness to use LBS and conclude that privacy concerns might consequently hinder LBS adoption (Xu & Teo, 2004). Kowatsch and Maass (2012) also confirm the negative impact of privacy concerns on the adoption of IoT services, however, in their research model, privacy concerns are significantly alleviated by the perceived usefulness of a particular IoT service and individual's personal interest in using it. In addition to perceived control (Gerber et al., 2018; Krasnova et al., 2010), familiarity with legislation and privacy knowledge were also identified as factors that have a reducing effect on privacy concerns (Hong et al., 2019).

Facing inconsistent theoretical and methodological approaches with regard to scientific investigations of privacy concerns (Li, 2012; Masur, 2018), van Zoonen (2016) develops a two-dimensional framework of this construct. More precisely, the author examines whether and how IoT technologies in smart cities can raise privacy concerns. For this purpose, she specifies, which kind of data is involved, ranging from personal to impersonal data, and the purpose of data usage "which can move from improving the livability and services in a city to advancing surveillance and keeping citizens in control" (p. 473). As a result, van Zoonen (2016) provides a tool for local governments to determine potential privacy concerns of citizens with regard to certain technologies.

At this point a distinction must be made between the dissemination of data regarding horizontal (peers and friends) and vertical (providers, governments or institutions) axes of privacy (Bartsch & Dienlin, 2016). Effectively, horizontal and vertical privacy may intersect, as it is the case with SNS such as Facebook or the Chinese video platform TikTok, which enable interactive communication between members (horizontal) but also shares extensively tracked data such as contact details, technical and behavioral information, with third parties and advertisers (vertical; Neyaz et al., 2020). Considering the deployment of IoT devices and services, examples for horizontal privacy are automated data sharing from fitness trackers with a community, smart home data access from multiple members of the household but also attacks from hackers. In contrast, examples for vertical privacy in IoT are cloud-based processing of merged user data by manufacturers in order to fine-tune algorithms or the trade of personal data for customized services (e.g., insurance companies monitor driver behavior and vehicle use data to offer discounts; Karapiperis et al., 2015). Zhou and colleagues (2019) state that "The sensitive data collected by IoT devices are shared with cloud-based service providers. Driven by profit, these providers usually keep this data forever and even share these data with other advertising agency without the user's consent, which increases the risk of privacy leak" (p. 1610). In a recent survey by Beales and Muris (2019), participants reported privacy concerns regarding the access of their private data by internet service providers, but most of all, they were worried concerning possible privacy infringements on the part of the government. The technical development in combination with inscrutable data access by third parties raises uncertainties, potentially leading to further privacy concerns. Thus, scientific interest needs to address both horizontal and vertical privacy in the exploration of privacy concerns.

The next chapter discusses another specification that can be explicitly assigned to the IoT field with reference to the level of privacy.

2.1.4 Technological and Human Levels of Privacy

When reviewing the relevant definitions of scholars regarding privacy, it becomes evident that the classical understanding of privacy is associated with social interactions. Altman (1990) presumes that privacy is inherently a social strategy including “the interplay of people, their social world, the physical environment, and the temporal nature of social phenomena” (Margulis, 2011, p. 11). Likewise, Burgoon's (1982) elaboration of privacy is placed in the context of interpersonal communication. Masur (2018), furthermore, states that “No individual desires privacy all the time because the desire to be sociable and to interact with others, to open oneself and to take part in social exchanges is equally important“ (p. 49). The underlying assumption is that people share their information with other individuals or groups and can determine the degree of privacy by controlling the disclosed information. This can be achieved by self-withdrawal or by different self-disclosure strategies regarding the communication with different people. However, when the existence of a human counterpart no longer applies, and instead, is replaced by automated processes or bots, the privacy seems to be detached from the social component. Thus, privacy in the application of IoT requires a separate category oriented towards the interplay between technology and individual. Therefore, I propose the division into the human and the technological levels of privacy, under consideration of Burgoon's (1982) dimensional privacy perspective and the privacy components suggested by Atlam and Wills (2020). This new integrative approach towards the differentiation of the privacy construct into two different levels with regard to technological advances represents a major theoretical contribution of the doctoral thesis and, in the following, will be explained in more detail.

While the traditional comprehension of privacy described above would refer to the *human level* in terms of social interactions, within the *technological level* the system acts autonomously by extending user profiles through information linkage, making decisions based on algorithms with only conditional control by the user (Abu Waraga et al., 2020). To be more precise, the human level refers to the communication with other people, through which an individual explicitly reveals personal data, enabling access to his or her informational privacy. Disclosing behavior on this level means that a person engages in social interaction. Personal information is primarily controllable by the individual. However, other people might make assumptions regarding one’s social or psychological information, basing on the provided information or due to their observations of a person. Thus, the human level can also implicitly encompass one’s social and psychological privacy.

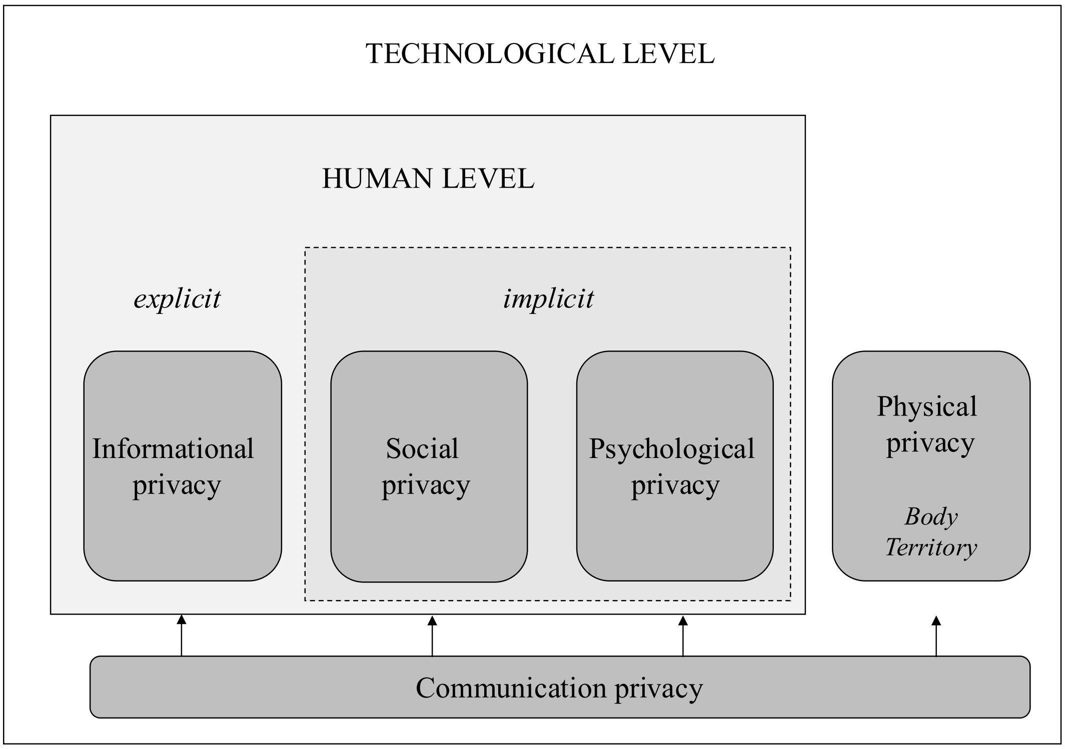

Figure 1. Technological and human levels of privacy

The technological level comprises the three dimensions of the human level and additionally encompasses physical privacy due to the sophisticated data collection and analysis capability of IoT (Schomakers et al., 2020). Physical privacy includes information about an individual's body (physiological data) and territory (location, environmental data). Communication privacy refers to the process of information exchange by means of IoT-based technology. Thus, on the technological level, every information about an individual can be accessed and linked or communicated within a network. There is no social interaction, and controllability of information by the individual is limited to possible privacy settings of the IoT application. To obtain a more differentiated view, Figure 1 demonstrates the human and technological levels of privacy related to the four privacy dimensions of Burgoon (1982) and the components of Atlam and Wills (2020). However, users are often unaware of the fact that, especially at the technological level, they provide data about themselves and that this data can be automatically tracked and processed by diverse IoT devices (Mikusz et al., 2018), as illustrated in the next chapter.

2.1.5 Privacy Knowledge and Risk Awareness

Studies have shown that the ability of individuals to make privacy-relevant decisions and thus to protect their privacy, crucially depend on one's privacy knowledge (Bartsch & Dienlin, 2016; Baruh et al., 2017; Debatin, 2011; Trepte et al., 2017). Trepte and colleagues (2015) postulate that privacy knowledge is essential for self-determined evaluation and usage of online services. The authors interpret the term as a two-dimensional construct, combining *factual knowledge,* i.e. information about privacy risks, legal policies or institutional practices and *procedural knowledge,* i.e. the ability to use privacy-protecting tools or strategies. Brough and Martin (2020) extend this characterization by a third dimension, namely *experiential knowledge* "including general familiarity with using online technology and firsthand experience with privacy violations" (p. 12). Although privacy knowledge was confirmed as a predictor for privacy protecting behavior (Debatin, 2011; Park & Jang, 2014), numerous studies report that individuals generally indicate an insufficient level of knowledge (e.g., Brough & Martin, 2020), particularly when it comes to technologies that utilize unobtrusive tracking techniques (Matz et al., 2020). On the one hand, this might be explained by users' inability to actively inform themselves, for example, by reading privacy policies (Golbeck & Mauriello, 2016), as they are often considered incomprehensible or too time-consuming (Meier et al., 2020; Rao et al., 2019). On the other hand, users potentially have obsolete ideas about data tracking, which leads to the fact that "while IoT is changing the pervasiveness and granularity of in-home data collection, users are still relying on outdated, pre-IoT models of entities in the IoT ecosystem to make purchasing, privacy, and security-related decisions" (Zheng et al., 2018, p. 10). Additionally, the users' misconception of data tracking mechanisms might be grounded in the complex nature of algorithms (DeVito, 2017). Therefore, even if basic technological knowledge is available, sophisticated, IoT-specific concepts may not be well understood by users, leading to an insufficient privacy knowledge.

A similar picture emerges with regard to individuals' awareness of privacy risks. In their study, Perera and colleagues (2015) refer to a survey by the privacy compliance company TRUSTe (2014), which reveals that barely more than half of the respondents are aware of the fact that IoT is able to collect user data. Zheng and colleagues (2018) further demonstrate that IoT users are unaware of possible inferences that can be retrieved from non-audio/non-visual technology (devices without camera and microphone, such as a smart toothbrush) and comprise sensitive information e.g., home-occupancy. The significant lack of awareness in IoT users might be traced back to the fact that IoT capabilities of data collection and processing are not restricted to the online environment but also extended to the physical world in an unobtrusive manner, invisible for users of this technology (Kröger, 2019). This not only includes that people are unaware of tracking capabilities of devices they deploy (Mikusz et al., 2018) but also with regard to the amount of gathered data, access from third parties and purpose of data collection. Thus, IoT users, who are unaware of the explicit capabilities and methods of IoT technology, passively and unconsciously provide their data by deploying IoT devices, challenging the principle of intentionality regarding self-disclosure and privacy regulation as proclaimed by the privacy calculus.

To better understand the underlying principles of tracking methods and potential privacy threats with regard to specific IoT functionality, the following chapters elaborate distinctive features of this technology and describe its mode of operation.

2.2 Privacy-related Characteristics of IoT

The underlying principle of how IoT works is, as already mentioned, the interconnectedness of devices and applications together with the provision of services resulting from the exchange of information. However, a substantial amount of data is required for this purpose. Alongside sensory measurements of, for example, traffic flows in cities, IoT devices have access to private, in some cases highly sensitive data, especially when used by individuals (Celik et al., 2018) compared to smart cities or logistics. Therefore, the following chapters are dedicated to privacy-relevant aspects and the changing ways of dealing with privacy implications regarding the increasing use of IoT.

2.2.1 IoT: An Overview

IoT technology is an indispensable part of the digitalized society and has become an integral aspect of our everyday life. IoT is a comprehensive term coined by Kevin Ashton in 1999 for a variety of physical and virtual electronic systems that are interconnected (e.g., smartphones, wearables, vehicles). For this purpose, these systems use the infrastructure of the Internet in order to exchange data by means of information and communication technologies (Chen & Lien, 2014). The principal objective of IoT is to support people in their everyday lives and to enhance the efficiency and convenience of processes in several fields including health, transit or sustainability (Kröger, 2019). Examples are networked household appliances that are able to operate remotely or systems that are equipped with a certain level of intelligence, i.e. they can retrieve data, such as consumer habits, and act autonomously on the basis of this data (Atlam & Wills, 2020). For this reason, IoT is also referred to as ‘smart’ technology. The user numbers of fitness trackers, networked cars and people living in smart homes are constantly increasing (Statista, 2016). IoT is also being implemented more and more frequently in industrial and public environments. However, its broad application brings about new challenges. First of all, given the heterogeneous technologies, IoT is vulnerable in terms of cyber threats, such as hacker attacks (Frustaci et al., 2018). Infected applications might be remotely controlled, or their mode of operation might be manipulated. Second, large amounts of data generated or gathered by IoT applications need to be analyzed, interpreted and processed. For this purpose, reliable processing structures are necessary, which allow to draw valid inferences from the data (de Matos et al., 2020). This in turn means that data and contextual information are stored and forwarded posing a greater challenge for data privacy. In order to better understand how personal data enters the Internet and how sensitive private information can be derived from it, in the following, the general functioning of IoT will be briefly outlined.

2.2.2 Data Everywhere – Digitalization and Technical Properties of IoT

The growing use of IoT in different areas of life (e.g., private homes, smart cities, health or industry) increasingly permits accessibility to private data about users, their environments, preferences etc. For this purpose, behavioral and environmental data of individual users are captured by a magnitude of sensors (e.g., microphones, accelerometers or GPS systems) and digitalized (Kröger, 2019). Given the permanent connectivity of IoT to various networks, a flood of collected data is emerging, and with the implementation of algorithms and machine learning methods, the focus is shifted from the type of data collected to the purpose of the data gathering (Matz et al., 2020). This enables IoT to analyze masses of data automatically, merge it with other data by means of data linkage and utilize it for different purposes (Kröger, 2019). Thus, many IoT applications can draw inferences, suggest efficient problem solutions or even act self-contained and goal oriented. Given the automated to autonomous functioning of such devices, which means that systems can either execute predefined commands or learn and adapt to environment, a certain degree of intelligence is attributed to this technology (Zhou et al., 2018). Hence, IoT enables a unique insight into the individual and his or her environment reaching even deeper into one's private live. Fitness trackers, for example, can provide information about the health status and movement profiles of the user, smart vacuum cleaners precisely map the apartment and reveal when the residents are out of the house. Depending on the objective of the data evaluation, complex correlations can be generated with regard to behavioral patterns and differentiated user profiles (Peppet, 2014; Kröger, 2019). These, among other things, serve commercial purposes (Zhou & Piramuthu, 2015). In this way, new business models and digital services, such as personalized advertising, are established, which base on private, potentially sensitive user data. But how do users perceive the increasing numbers in smart technologies as physical entities or smart applications that is constantly surrounding them? To this end, the next chapter aims to illuminate the user perspective and to discuss the perception and acceptance of IoT in more detail.

2.2.3 IoT Acceptance

The latest forecast by Transforma Insights (2020) expects that the number of IoT devices, which was about 7.6 billion in 2019, will rise to 24.1 billion in 2030 with the consumer sector as the dominating category accounting for 65% of all connected devices. It is further assumed that revenue will more than triple from USD465 billion to USD1.5 trillion. These astronomical figures substantiate the steadily increasing interest in and the popularity of IoT. The ubiquitous Deployment of IoT mainly occurs in three major domains: personal, business and public (Economides, 2017). In order to shed more light on the user perspective, specifically the personal domain will be addressed in this description. Within this domain, benefits for the users are manifold. These include the monitoring of one's health for example by transmitting health data to physicians, enabling remote treatment (Devi & Muthuselvi, 2016), increasing fitness e.g., by recommendations of wearable devices tracking one's physical data (Naslund et al., 2016) or through the consideration of individual preferences within one's own four walls by smart home systems such as the adjustment of light according to the user's mood (Chacko & Bharati, 2018). However, the mere existence of a technology that promises to improve nearly every aspect of everyday life does not guarantee it's adoption by consumers. Thus, the question arises, what are the driving factors behind individual's usage and acceptance of IoT embedded in their private environment? To answer this question, researchers from various disciplines have drawn on different theoretical foundations. To name a few frequently used theories in connection with IoT acceptance, there are privacy calculus (which represents the main focus of this dissertation; see Lee et al., 2018; Kim et al., 2019) and Davis' (1989) *Technology Acceptance Model* (TAM; see Kim et al., 2017; Patil, 2017), which postulates that the intention to use certain technologies depends on perceived usefulness and perceived ease-of-use of the technology. Furthermore, scholars (e.g., Almetere et al., 2020; Su et al., 2013) focus on the *Unified Theory of Acceptance and Use of Technology* (UTAUT), elaborated by Venkatesh and colleagues (2003). The UTAUT originates from the TAM and extends it by the factors *social influence* and *facilitating conditions* (i.e. environmental factors, which might simplify a task).

Also, Rogers' (1983) *Innovation Diffusion Theory* (IDT) is considered in the framework of IoT (see Ammirato et al., 2019; Saheb, 2020). IDT assumes that the acceptance of technologies or innovations is a result of a five-stage adoption process and describes how a certain technology spreads within different categories of adopters over time. Additionally, studies examine integrative research models comprising components from several theories (Kowatsch & Maass, 2012) or the effect of particular factors, such as enjoyment or personalization, on the intention to use IoT (Economides, 2017). Due to the partly contradicting results, to date, there is no consensus among scientists regarding a model, which offers the most suitable framework to investigate IoT acceptance. This might be due to fundamental challenges associated with IoT research, discussed in more depth in the next chapter.

2.3 Challenges of Empirical Investigations on IoT

Scientific investigations in the field of IoT are not new and are widely discussed from a variety of perspectives such as computer sciences (Brown et al., 2013), psychology (AlHogail, 2018) or communication sciences (van Kranenburg & Bassi, 2012). In the course of IoT research by different scientific disciplines, distinctive challenges of empirical investigations of networked technologies have been identified. Among the most prominent are ethical and moral considerations (e.g., van den Hoven, 2017), heterogeneity of IoT applications (Bedhief et al., 2016) and context-specific dynamics of IoT (Apthorpe et al., 2018), which in the following will be referred to in more detail.

2.3.1 Ethical Perspective on IoT

The adaptation of emerging technologies within a society often requires social, organizational and political adjustments, e.g., in terms of user acceptance, legal amendments or burgeoning political debates. At the same time, new technological developments, in turn, have the potential to change a society for example by altering moral principles such as privacy, equity, responsibility or justice (van den Hoven, 2017). Thus, there are several perspectives with regard to ethical issues. One is based on peculiarities in the course of empirical research on the use of IoT. Due to social inequality, field studies with methods such as ambulant assessment (i.e. behavior monitoring in daily life settings; Fahrenberg et al., 2007), might provide distorted outcomes, as low-income households potentially own fewer IoT devices and therefore, do not meet the requirements of the focus groups of some studies. At the same time, even if devices are provided to subjects in the context of empirical studies, digital divide, which refers to individuals' varying skills and literacy regarding the handling of digital technologies (van Deursen & Mossberger, 2018) might lead to large differences in the usage of IoT and especially in the protection of privacy.

The other perspective with regard to ethical issues focuses on ethical challenges in the development and application of IoT. In this context, scholars agree upon the fact that privacy-related constraints rank among essential challenges (Porambage et al., 2016; Zheng et al., 2018) and arouse great interest in the scientific community. Weber (2015) states that "In particular the ability of an individual to consent to privacy infringements as a way of allowing the service provisioning poses a question of accountability and power abuse" (p. 234) and criticizes the insufficient legal allocation of responsibility regarding the management of private data to providers. With no legal certainty, also, employers operate in a grey area, for example when they use algorithms to analyze online available information about candidates, basing on candidate data from CVs (Weber, 2015). Furthermore, Leong and Chen (2020) emphasize a particular (commercial) interest of insuring institutions in private customer data and the subsequent increasing utilization of IoT by life, health and automobile insurance companies. Accordingly, these companies might receive customer data with regard to driving behavior, physical activities or drinking and cigarette smoking habits (Kröger, 2019). From an ethical point of view, this is highly controversial. On the one hand, new business models emerge, which offer fair tariffs to customers (Leong & Chen, 2020), for example discounts for non-smokers, due to the fact that they cause less costs than smokers (also referenced as nudging, Handel, 2013). On the other hand, behavioral profiling, which describes the consolidation of user data and the inferencing of preferences and behavior (Ziegeldorf et al., 2014) can lead to a different treatment of people (Kröger, 2019). Thus, societal morality and the solidarity principle of equality are called into question, which particularly protect people from discrimination.

The explanations underline the urgency and necessity to consider ethical aspects and moral concerns in the context of IoT. Research already reflects on this field for instance, with attempts of scholars to implement moral values into design requirements, also referred to as *Value-Sensitive Design* (VSD, Mcmillan, 2019), "where the needs and values of human users, as citizens, or patients, are considered in their own right and not simply as a side constraint on successful implementation" (p. 67) as formulated by van den Hoven (2017). However, given the wide spectrum of the most diverse IoT products and services, there is rarely an all-fits-one solution. Rather, the specific circumstances of different IoT applications, which are illustrated below, must be taken into account.

2.3.2 Heterogeneity in the IoT Environment

IoT is a comprehensive term for numerous networked technologies that differ in regard to several criteria such as types of devices, system operation, communication methods, amount of tracked data, etc. (Canedo & Skjellum, 2016; Atlam & Wills, 2020). Concerning the diversity of IoT applications, Bassi and Lange (2013) argue that "the solutions developed are usually non-interoperable, and while successful, they do not produce a common abstract infrastructure capable of marking significant progress in the whole field" (p. 14). The authors see a plausible reason for the heterogeneity of IoT in the fact that different fields of application of IoT (e.g., smart cities and entertainment) have specific requirements, and therefore, IoT based solutions develop in different directions (Bassi & Lange, 2013).

The field of application is a significant determinant of how certain IoT devices are deployed. While the deployment of IoT in smart home environments is primarily designed to meet individual customer preferences, such as convenience (Zheng et al., 2018), the focus in logistics lies on efficiency (Tu, 2018). Devices can also vary regarding the mobility of a certain technology (Kröger, 2019). A device can be stationary (e.g., smart refrigerator), movable (e.g., smart vacuum cleaner), wearable (e.g., clothes equipped with sensors) or even implantable (e.g., smart pacemaker). Moreover, there are devices that can be operated by the user (e.g., smart heating system) or only serve as an autonomous part of the smart home (e.g., smart carbon dioxide detector). As manufacturers can develop IoT devices according to their own specifications, substantial differences exist between the same devices from different manufacturers (Bai et al., 2017). One example is the varying storage location of collected data, as data can be stored locally on the device or on a server abroad (Bokefode et al., 2016). Equally, the number and capability of data-collecting sensors is highly variable depending on device, purpose or manufacturer (Bai et al., 2017). This, in turn, might affect perceived privacy risks, since an integrated microphone is considered more privacy intrusive than, for example, an accelerometer (Kröger, 2019). Additionally, manufacturers differ with regard to protection of deployed sensors. This was demonstrated by Bai and colleagues (2017), showing that apps on the mobile platform Android had access to data from 25 built-in sensors while iOS apps only had access to six sensors in order to retrieve data.

Together, these are factors that significantly influence user's perception of IoT. People's attitude towards IoT might therefore differ depending on the purpose of the device. According to this, a smart light bulb would be less worrying with regard to data privacy, because it is primarily intended to provide certain lighting conditions making data tracking seem unlikely to customers. However, an interaction device, such as the personal assistant Alexa from Amazon, purchased specifically for controlling the smart home and retrieving information, might rather be associated with data tracking as it is possibly more salient to the user. In addition, the fact that IoT can be used for a wide range of different tasks with partially overlapping capabilities makes it difficult for users to assess this technology. For example, users who confidently deployed a smart TV for years can still be quite skeptical about a personal assistant, as their mental model may differ greatly depending on the different device categories and types of collected data. Tabassum and colleagues (2019) cite numerous studies, which found that individuals mostly worry about their private data when it comes to videos, photos and biometric data (e.g., Lee & Kobsa, 2017; Lee et al., 2017). This also means that they are less concerned about other data, which is potentially just as privacy violating (Kröger, 2019). Therefore, empirical studies on the holistic concept of IoT prove to be very complex and statements regarding the general attitude towards and use of IoT are hardly indicative. Different scientific disciplines, especially computer science, strive to elaborate unified concepts in order to obtain a common framework that standardizes processes, terms and architecture to enhance the development and deployment of IoT (Pötter & Sztajnberg, 2016). From a socio-psychological perspective, however, to date there is no consensus regarding the methodology of IoT research. For this reason, previous studies mostly explore specific devices or device categories as case studies (Apthorpe et al., 2018; Emami-Naeini et al., 2019).

The studies included in the present cumulus each investigate a particular IoT device in order to derive specific statements about the respective device category, illuminate different areas of application and identify parallels with regard to privacy-related factors.

2.3.3 Context-specific Dynamics of IoT

Scholars argue that perceived control as well as perceived privacy are situation-specific factors (Gerber et al., 2018; Masur, 2018). Moreover, in his *theory of situational privacy and self-disclosure*, Masur (2018) concludes that privacy-related behavior (i.e., to disclose or withhold private information) can be induced by different circumstances prevailing in a particular situation. Consequently, an individual's privacy-related decision strongly depends on the context in which the decision is taken. This poses a further challenge for empirical investigations of IoT, especially, because the context of IoT usage can refer to several perspectives. First of all, there is the question of the application context. In other words, in which sector is IoT applied? To address this question in the best possible way, studies investigate IoT adoption and influencing factors of IoT usage with focus on particular sectors, such as logistics (Tu, 2018), smart cities (van Zoonen, 2016), health (Leong & Chen, 2020) or smart homes (Zheng et al., 2018). To date, there are relatively few studies comparing IoT adoption in different application contexts. However, we can assume that the differences might be fundamental. Investigations on IoT adoption within the workplace show that individuals are concerned regarding the misuse of their data, particularly with regard to sensitive information (Yildirim & Ali-Eldin, 2019). At the same time, parents of a diabetes-suffering child would most likely be willing to give up much of their privacy in favor of preventing diabetes-related complications by using an IoT healthcare device (i.e. smart glucose monitoring system). Thus, in certain situations, perceived risks and benefits vary to a large extent and should therefore be specifically addressed by research. For example, Markos and colleagues (2018) found that individual's perception of information sensitivity might vary in certain situations, depending on who receives the information, "challenging the notion that individuals uniformly perceive certain types of information to be inherently more sensitive" (Brough & Martin, 2020, p. 12).

The voluntariness of IoT usage could be understood as another context-specific perspective. This means, that while a person buys an IoT household device and, according to privacy calculus, puts anticipated benefits above perceived risks, other household members are involuntarily exposed to the tracking device, thus, potentially having a different usage intention (Hargreaves et al., 2018).

Apthorpe and colleagues (2018), in turn, rely on *contextual integrity* as a theoretical basis, which describes privacy norms of information dissemination in different contexts. In their study, the authors point out the relevance of situational context by investigating individual's acceptability of 3,840 information flows under varying conditions, such as different IoT devices, information types or data recipients, hence, demonstrating the diversity of contextual factors.

Furthermore, situational cues can also be responsible for how individuals perceive IoT. Thus, contextual factors, such as personalized advertising (Kim et al., 2019) or a notification of being monitored (Noah et al., 2018) might negatively affect people's attitude towards IoT by causing privacy concerns.

For this reason, in addition to the heterogeneity of IoT applications, the cumulus also considers the application context. Hence, the included empirical studies investigate the use of IoT in the field of smart home environment, workplace and health.

III RESEARCH OBJECTIVES

The previous chapters provide an in-depth elaboration of the theoretical framework for the studies conducted in the course of this dissertation. The introduced theories and concepts form the necessary foundation in order to understand the motivation of the present doctoral thesis and to discuss the results of the accomplished studies before their background comprehensively.

The aforementioned considerations indicate that IoT technology, through its extensive application in almost all areas of everyday life and through the use of tracking techniques or information linkage methods, challenges the current understanding of the privacy concept in research. However, the profound examination of privacy-related issues raised in connection to IoT application is still in its infancy. Existing research models such as TAM (Davis, 1989), UTAUT (Venkatesh, 2003) or IDT (Rogers, 1983), which comprise the acceptance and adoption of IoT, neglect privacy-relevant aspects. The aim of this cumulative dissertation is, therefore, not to suggest a new theoretical approach, but to apply the well-studied privacy calculus as a decision-making basis for IoT acceptance, accordingly, transferring this theory to the IoT context. A further research on IoT and privacy not only sheds light on the current topic of human-computer interaction, but also expands our knowledge about psychological mechanisms in regard to privacy decisions of potential IoT users. This is crucial in the investigation of the influence our perception of privacy has on the use of networked technologies and might open the possibility to examine the impact of the inexorable digital revolution on our conceptualization of privacy.

The overarching goal of this thesis is to contribute to privacy literature by extending the privacy calculus theory through its application in IoT. As outlined in detail in Chapter 2.1.1 (A Balancing Process: The Privacy Calculus), the application of this technology affects privacy to a considerably greater extent than the use of SNS and other websites. The extension of privacy calculus, therefore, refers to its adoption as a theoretical grounding outside of already well documented online communication channels (Bol et al., 2018; Dienlin & Metzger, 2016; Trepte et al., 2017). In particular, there is a need to identify specifications which, given the affordances of IoT, have to be considered when privacy calculus serves as a theoretical basis. The studies introduced in the following chapters initially rely on the assumption of the rational thinking individual prior to discussing the above-mentioned limitations of this theory (see Chapter 2.1.1) in more depth in order to derive theoretical implications.

Under consideration of elaborations on the heterogeneity of IoT (see Chapter 2.3.2), the empirical studies are focused on three different areas. This involves the private use of smart household appliances, the use of a fitness device from the electronic healthcare (eHealth) sector and the implementation of a networked monitoring technology at the workplace. In addition to the investigation of IoT usage against the background of privacy calculus, the impact of other domain-specific factors is examined in these different areas in order to provide a comprehensive insight into the respective field of application and the perceptual processes of individuals.

Figure 2 illustrates the overarching research model of the present dissertation. For a better overview, the tested constructs are summarized with regard to the respective study. Thus, Study I examined the usage intention of an IoT household device, dependent on its convenience, amount of tracking and participants' attitude towards data collection. Study II analyzed whether the intention to use an IoT fitness tracker is affected by moral considerations and technology commitment of participants and assessed the impact of actual and perceived control of private data. Finally, Study III investigated, whether employees accept an IoT emergency detection system at their workplace in dependence of their trust in the employer and the system's tracking ability and rescue value. All three empirical studies tested the privacy calculus and assessed individuals' privacy concerns. The results are intended to address the following questions, raised on a meta-level:

- Is privacy calculus a suitable theory for the investigation of IoT and how does its application evolve within this framework?
- Which psychological mechanisms are involved in the risk-benefit tradeoff with regard to the situational context?
- What changes in the theoretical concept of privacy are necessary against the background of IoT dissemination?

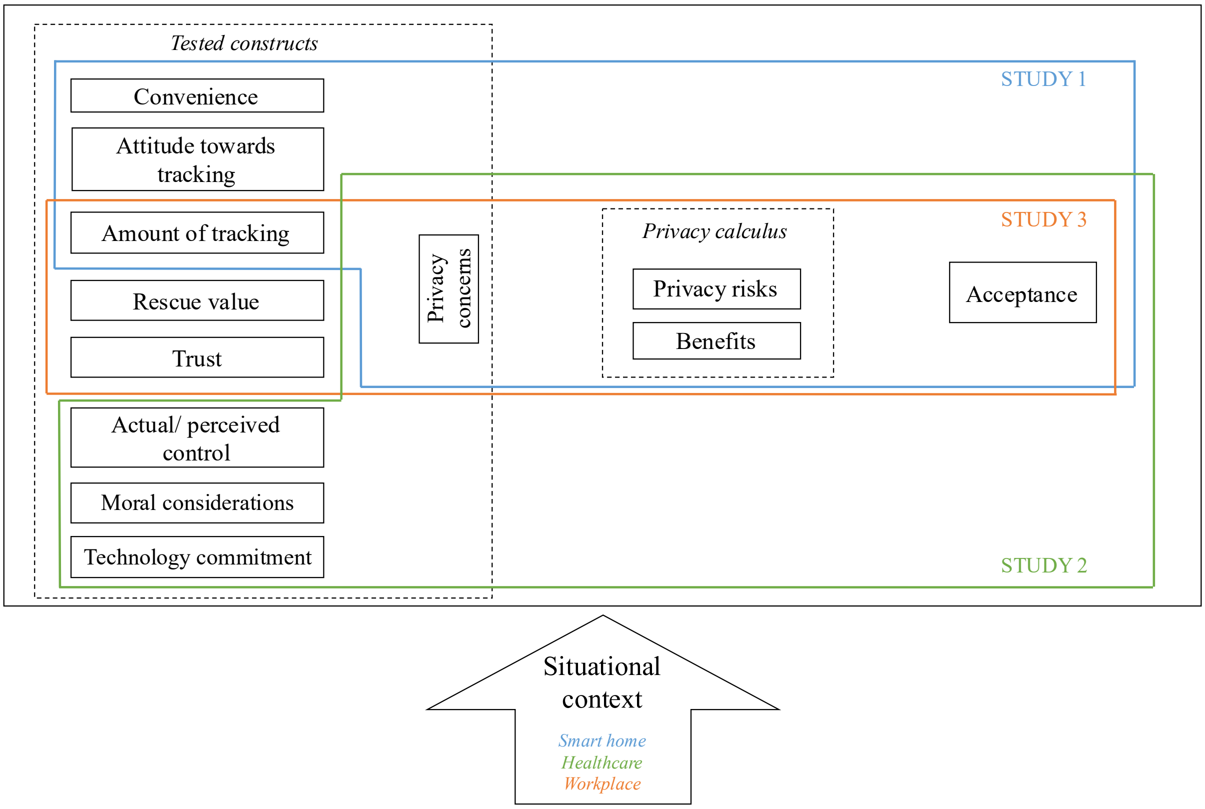

Figure 2. Overarching research model of the cumulus

To answer these questions, two empirical vignette studies and a laboratory experiment were conducted. All three studies investigate the effect of data tracking on the acceptance of an IoT device or the willingness to use it. At the same time, the studies explore whether the balancing of risks and benefits takes place in order to confirm privacy calculus as an underlying theory within the framework of IoT usage. To meet the requirements of heterogeneity, every study considers a different IoT devices allowing more specific conclusions with regard to the respective device category. Furthermore, the studies each take place in a different field of application, namely smart home, healthcare and workplace, to reflect on the situational context. In contrast to the field-specific variables (e.g., trust in the employer within the workplace context) privacy concerns are part of all three empirical studies. To get a more detailed picture of the impact of privacy concerns in the framework of IoT usage, both regression and moderation effects of this construct are analyzed.

3.1 Synopsis of the Research Papers Included in the Cumulus

Following the explanation of the relevant theoretical constructs and the specification of the research objectives, the subsequent chapters provide a detailed overview of the empirical studies conducted within the framework of the present dissertation. The ethics committee of the University of Duisburg-Essen authorized the conduction of all three studies included in the cumulus, which comply with the ethical standards of the American Psychological Association (Smith, 2003).

3.1.1 I Spy with my Little Sensor Eye - Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology (Research Paper 1; Princi & Krämer, 2020)

With the increasing number of interconnected IoT devices and the promise of this technology to facilitate, accelerate or even autonomously perform a wide range of everyday tasks, the number of people who want to benefit from this promise is also continuously growing. Accordingly, more and more private households are equipped with various IoT applications (Zheng et al., 2018). These include smart baby monitors, learning thermostats or smart assistants, which respond to user requests and are able to control the entire smart home environment on command or on their own, in accordance to user preferences. On the one hand, these applications offer enormous potential. For example, one's home can be automatically heated and ventilated in a cost-efficient way, either on the basis of fixed schedules, home occupancy detected by sensors or personalized settings. On the other hand, IoT technologies represent a serious violation of privacy, because private user data that is collected, uploaded within the network or shared with third parties creates an essential basis for the functionality of many networked devices. Especially in one's own home, conversations might be recorded, behavior might be observed, or habits might be identified. Consequently, information is made accessible that used to be hidden from the outside world. Individuals are therefore faced with the decision, whether they are willing to give up their privacy to a certain extent to get the expected advantages of particular technologies.

The aim of Study I was to examine whether individuals weigh the benefits of using an IoT home device against possible privacy risks and thus apply privacy calculus in their decision making. Moreover, the moderating role of privacy concerns was investigated, as studies have shown that tracking methods and even personalized services are likely to be perceived as privacy-invasive (Aguirre et al., 2015) raising worries about one's privacy (Ketelaar & van Balen, 2018). As individuals also differ in their attitude towards tracking (Ketelaar & van Balen, 2018), it was explored whether the attitude towards data collecting methods moderates the relationship between the tracking capability of an IoT device and the willingness to use it (see Figure 3). For this purpose, an online study with 209 participants was conducted. First, a pretest was used to determine a suitable smart household appliance for the vignettes of the main study. The two defined criteria for the pretest included perceived convenience and perceived privacy risk of IoT devices from different smart home categories (e.g., smart TV, smart assistant, smart Thermostat etc.). The choice fell on smart household appliances as devices from this category were perceived as very convenient with a moderate privacy risk. For the main study, which constituted a 2 x 2 design, four scenarios were created varying with regard to provided convenience and the devise's ability to track information about the user. Since a between-subjects design was chosen, participants had to evaluate the respective device and indicate their intention to use it for the randomly presented scenario. Afterwards, they were asked to provide information on perceived convenience, their attitude towards tracking and their privacy concerns.

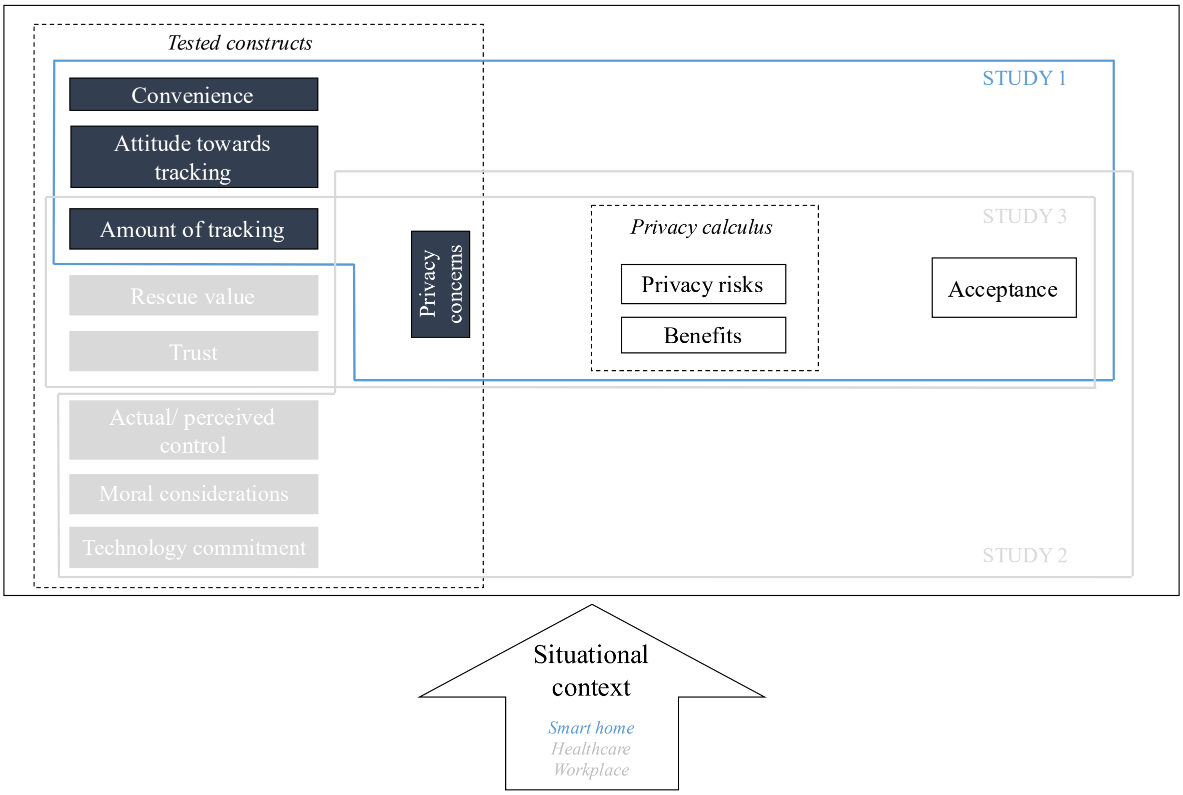

Figure 3. Research model of Study I

The results showed that convenience of a smart household device significantly raises individual's intention to use it. Interestingly, the actual ability of the device to track personal data does not have an effect on usage intention. However, this relationship is moderated by both privacy concerns and the attitude towards tracking. When participants have a positive attitude towards collection of their data, their willingness to deploy a device with an intense tracking ability is increased. On the contrary, when individuals indicate to be concerned about their privacy, their willingness to use a tracking device is rather low. This underlines the fact that the image people construct with respect to a certain IoT device (e.g., the expected performance) seems to be more decisive for the intended use than the actual technical characteristics, such as the ability of the device to collect user data.

The juxtaposition of device convenience as a specific benefit of the device and privacy concerns as perceived risks illustrates two key findings: firstly, people consider both the risks and benefits of using a device and take them into account when making their decision to use it. Therefore, Study I allows the assumption that the cognitive process behind the decision whether to deploy an IoT household device can be attributed to the privacy calculus. Second, the tendency to prefer benefits over risks is confirmed (Lee et al., 2018).

3.1.2 Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices (Research Paper 2; Princi & Krämer, 2020)

The results of Study I of this dissertation empirically indicate that people do not seem to care whether technology that they deploy in their private homes is able to track, analyze and share their personal data. To a certain extent, individuals worry about their privacy but are still willing to use IoT as a tool for their household due to its promising effect of convenience. But how does an individual's evaluation of IoT change if we shift the focus to another field of application with potentially even more sensitive data? To answer this question, Study II was conducted in the context of IoT deployment in healthcare.

In this sector, IoT is increasingly applied for medical purposes such as the remote monitoring of vital signs by physicians or the use of innovative implantable medical devices (e.g., a smart pacemaker; Ibrahim et al., 2020). This underlines the enormous potential of IoT to improve the living conditions of patients with certain disorders, for instance, by means of remote medical treatment (Catarinucci et al., 2015). This means that the necessity of hospitalization might be no longer required due to IoT applications. However, the use of IoT in healthcare is particularly controversial. On the one hand, these technologies offer a new level of attack opportunities with regard to physical privacy that hackers can exploit to manipulate or even control targeted devices, with potentially life-threatening consequences, especially, when it comes to implantable devices (Alblooshi et al., 2019). On the other hand, Laplante and Laplante (2016) state that the use of IoT in healthcare poses the greatest threat to privacy compared to other sectors, because device sensors from eHealth products can not only record environmental information, as for example in the smart home area, but also internal physical measurements such as physical activity, blood pressure or insulin levels, allowing inferences regarding the health status of an individual.

These elaborations illuminate the particular relevance of IoT in healthcare and, at the same time, present the contrasting substantial risks of its application in this sector. The aim of Study II was, therefore, to explore how individuals integrate their evaluation of eHealth device benefits and perceived privacy risks into their decision process regarding the adoption of these devices and, thereby, to verify privacy calculus as theoretical framework for IoT in the healthcare context (see Figure 4). As so-called fitness trackers (wearable IoT devices equipped with multiple sensors) can collect and analyze sensitive physical data (e.g., location or heart rate) and at the same time, rank among the most common and adopted IoT devices (Kao et al., 2019), a wearable, IoT-based fitness tracker was used for the case study.

Usually, individuals deploy wearable devices in order to quantify their fitness, sleep and other health-related values. However, studies have shown that data captured by various sensors of fitness-trackers can be used to recognize drinking and smoking patterns (Parate, 2014; Tang et al., 2014) or draw inferences on driving behavior (Júnior et al., 2017). This might be particularly problematic given that insurance companies are highly interested in customer data and are therefore constantly developing new business models to access these data (Karapiperis et al., 2015), e.g., by offering IoT devices to members, aiming to access their data in return. If health insurance companies with high accuracy can classify their patients into risk groups based on behavioral data, there is reason to assume that this information might be used with particular financial interest in the sense of data economy (i.e. with commercial purposes). This in turn might lead to price discrimination and inequality towards certain groups (Mittelstadt, 2017) posing a particular ethical challenge for IoT in healthcare. For this reason, another focus of the current study was to examine, whether individuals' moral considerations have an impact on their intention to use an eHealth device.

As described in detail in Chapter 2.1.2 (Selective control of information), control of private information can be interpreted as an inherent part of the privacy concept (Altman, 1976) and individuals strive to optimize disclosing processes by selectively controlling what information they want to disclose or to keep private (Masur et al., 2017). However, against the background of the increasing complexity of smart technologies users are exposed to technological challenges or might lack necessary knowledge of how to protect their privacy (see Chapter 2.1.5., Privacy Knowledge and Risk Awareness). Since scholars distinguish between objective control, actually provided by a certain IoT device (e.g., by means of privacy settings) and individually perceived control by the user, Study II investigated both actual and perceived control of information as determinants for the willingness to use an IoT healthcare device.

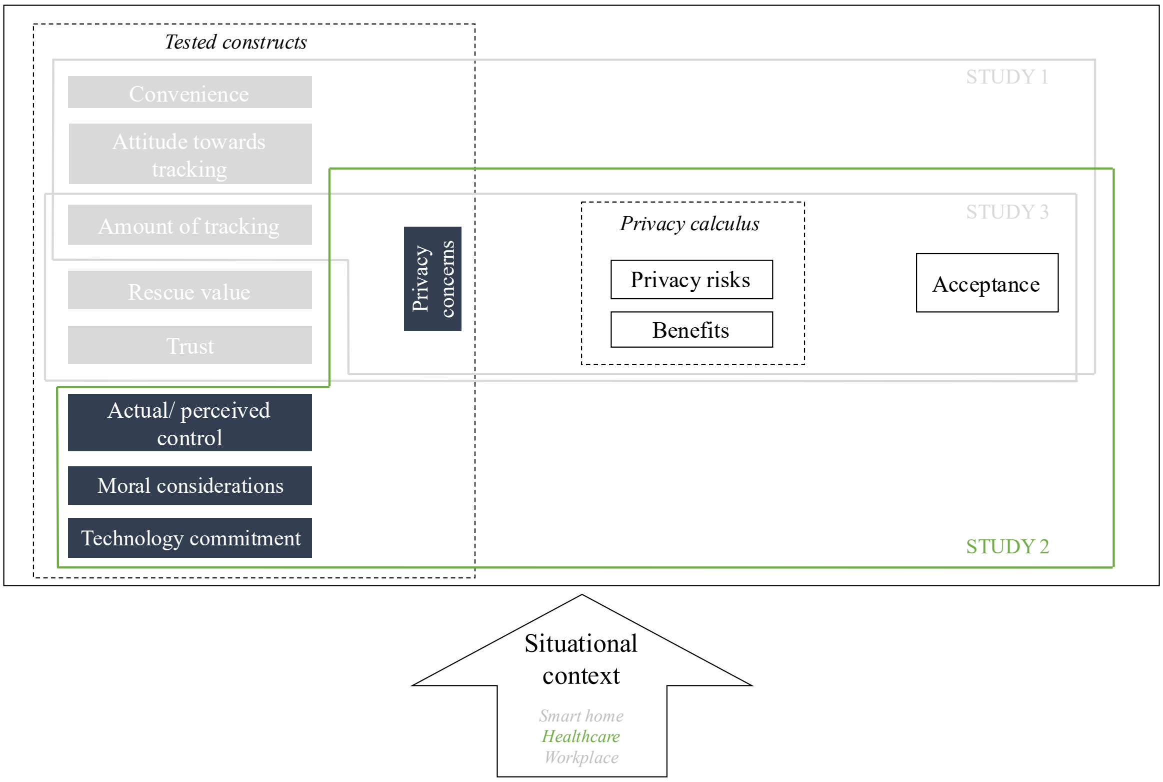

Figure 4. Research model of Study II

Prior to the main study a pretest was conducted in order to determine an eHealth device, which corresponds to the categories such as innovativeness, usefulness or trustworthiness, in order to ensure basic interest of participants. For the main study, volunteers were invited to the laboratory and asked to test the corresponding wearable fitness device under real conditions. The 209 participants were told a cover story about a program of a health insurance company to provide customers with smart eHealth devices with the purpose of increasing their fitness. Afterwards, they were randomly presented one of the three descriptions of the respective device, which varied with regard to data control possibilities and the amount of private data the device was able of tracking. They were then asked, whether they would participate in the program following by questionnaires in order to assess their perceptions of control, risks and benefits as well as their moral considerations, privacy concerns and technology commitment.

The results revealed that individuals weigh risks and benefits prior to their decision to deploy an eHealth device, lending further support for privacy calculus in the healthcare context. Although there is no significant effect of actual control, perceived control positively affects participants' intention to use the device as well as their perception of the device's benefits, at the same time decreasing individual's perception of risks. The findings also replicate the control paradox (Brandimarte et al., 2013) as actual control, which is more relevant for privacy protection, was not significant compared to perceived control. When participants indicate moral considerations with regard to the device, their willingness to use it is rather low. However, neither technology commitment nor privacy concerns have any effect on the usage intention.

Compared to the deployment of smart devices in one's private home, individuals seem to be more concerned about personal data tracking in healthcare. This might be due to possible worries of patients regarding negative consequences, if sensitive healthcare data is forwarded, for instance, to insurance companies or employers. However, notwithstanding the fact that health-related information is classified as sensitive according to EU data protection legislation (Regulation (EU) 2016/679), it should be noted that people might differ in their individual perception of data-sensitivity. Furthermore, Study II indicates that the calculation of risks and benefits should not be considered in isolation, as external variables, such as perceived control in this case, may have an influence on this mechanism. This finding underlines the relevance of providing IoT users in healthcare with control over their data, either by means of privacy-protecting device features or governmental regulations. Moreover, data indicates that benefits of IoT in eHealth have a stronger effect than privacy risks, which might be explained by positive expectations (Hajli & Lin, 2016) and novelty (Hirschman, 1980) of the technology leading to a trivialization of risks. Finally, individuals in the healthcare context seem to have expectations of institutions regarding their moral responsibility as a prerequisite for the adoption of IoT-based technology (van den Hoven, 2017).

With regard to technology commitment and privacy concerns, neither of these constructs had an impact on usage intention. Henze and colleagues (2016) argue that the ubiquitous application of IoT leads to a fundamental skepticism towards this technology. This means that individuals generally indicate high levels of privacy concerns and at the same time vary in their perceptions of privacy risks related to a certain eHealth device, which in turn determines their intention to use the respective device.

3.1.3 Acceptance of Smart Electronic Monitoring at Work as a Result of a Privacy Calculus Decision (Research Paper 3; Princi & Krämer, 2019)

The first two studies of the current thesis examined the intention to use IoT in two different contexts: private home and healthcare. Study III was intended to extend the research scope by a further field of application, namely the workplace. In the course of global digitalization, companies from all branches have to adapt in order to remain competitive. Against the background of the efficiency and expansion of IoT, it is therefore inevitable that employers increasingly opt for the use of networked technologies to enhance transparency and effectiveness (Greengard, 2015). More specifically, IoT at the workplace can be used to automate work processes (e.g., logistic workflows, Karakostas, 2017) or to impart new skills to employees with the help of wearable technology and augmented reality (Kravčík et al., 2017). Another reason for the use of IoT at the workplace is the monitoring of employees (Mähler & Westergren, 2018). Monitoring systems can serve various purposes, such as employee safety (Wu et al., 2019), assessment of their productivity (Mähler & Westergren, 2018) or their energy consumption, in order to nudge them into a more energy-saving behavior (Kotsopoulos et al., 2017). However, personal and behavioral data captured at the workplace, among other things, can reveal information about social relationships or the health status of employees (by means of wearables), as well as identify work patterns (Mähler & Westergren, 2018). Consequently, employee monitoring poses a severe privacy threat, especially given the invasive nature of interconnected IoT. One particular aspect at this point is that the decision to implement IoT is usually taken by the employer, manifesting the distorted power-relations in this sector. Picking up the privacy definitions by Westin (1967) and Altman (1975; see Chapter 2.1 - Privacy in the Digital Age) draws attention to the fact that the decision on the deployment of IoT at the workplace is largely one-sided, and individual privacy, hence, becomes strongly restricted. To be more precise, in this context it seems no longer possible for individuals to decide when, how and what information is gathered and who is getting access to it. Moreover, "selective control of access to the self" (Altman, 1975, p. 18) also seems to be no longer available when employees are being monitored. Therefore, the aim of Study III was to explore individuals' privacy concerns and perceived advantages of an IoT system under the described conditions with the focus on whether employees still perform a risk-benefit trade-off prior to IoT acceptance, potentially modifying the privacy calculus. Even though employees often have no decision-making power with regard to the implementation and use of IoT at the workplace, it is crucial to investigate their acceptance towards this technology. Therefore, additionally to privacy calculus, communication privacy management theory (CPM; Petronio, 2010) was chosen as a theoretical framework. With this theory, Petronio (2010) argues that individuals define iterative rules regarding the management of their private data with internal conflicts as a result of rule violation.

Missing approval of IoT at the workplace might lead to technological stress (feeling to be overwhelmed by technology) and perceived loss of privacy (Stieglitz et al., 2017) as well as anxiety, e.g., with regard to job loss. In this respect, research has identified trust in the employer as a key factor (Ball, 2010; Jøsang et al., 2007). Especially, in relation to employee monitoring, trust is of utmost importance as individuals usually do not know which data are processed in which way and for which purpose and, therefore, have to rely on the employer to manage personal data in a responsible way (Korczynski, 2000).

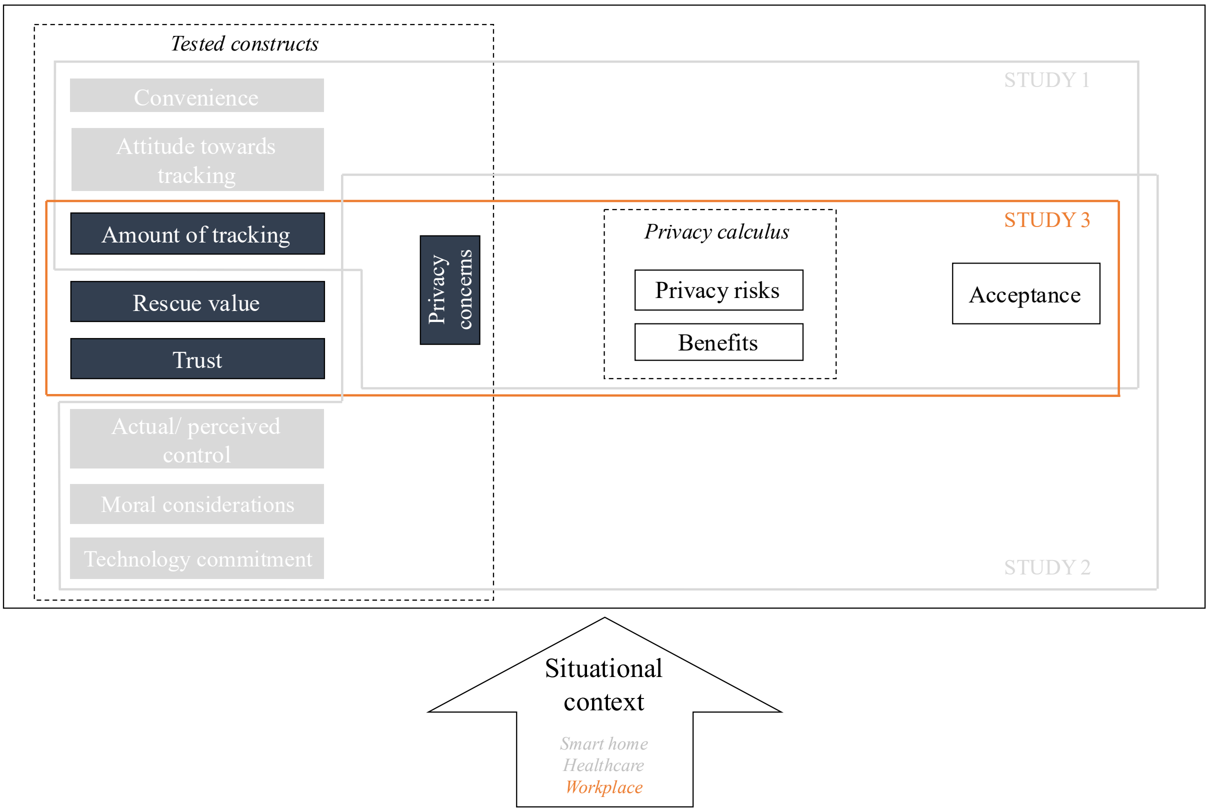

Figure 5. Research model of Study III

In order to provide context-specific conclusions, Study III comprised a representative sample of 661 employees. The 2 x 2 design includes four scenarios with descriptions of a smart emergency detection system. Participants were told that the purpose of the IoT-based system was to monitor employees and the work environment in order to detect anomalies that indicate an emergency and initiate rescue measures. Depending on the scenario, the IoT system offered either a high or a low rescue value and was equipped with privacy-preserving or privacy-invading tracking capability. The study was conducted online. After filling in the questionnaire about their trust towards the employer, participants were randomly presented one of the four scenarios and asked whether they would accept the respective system when implemented at their workplace. Additionally, perceived risks, benefits and privacy concerns were assessed (see Figure 5).

The results of Study III reveal that the acceptance of an IoT-based monitoring system at the workplace depends on the amount of collected data, trust in the employer and perceived benefits. The more data the system is capable of tracking, the more risks individuals perceive regarding their privacy and the lower is their perception of benefits and their acceptance of the system. At the same time, the system's rescue value does not impact its acceptance. One explanation is that the rescue value only counts as a benefit in an emergency and is therefore underestimated by employees (the benefits of the monitoring system in the study were accordingly perceived as rather low).

Although privacy concerns increased the perception of privacy risks, neither of the two constructs affected the system's acceptance. This is a very interesting finding, as the high perception of privacy risks in the study demonstrates that employees acknowledge both risks and benefits but obviously only take the latter into account regarding IoT acceptance. This might be specific for the work-related context due to the unbalanced power-relations between employer and staff. Employees usually have no choice but to accept the decision of the employer to deploy IoT, regardless of the perceived disadvantages. Thus, the perspective of privacy calculus shifts from risks and benefits of a particular IoT system to a meta-level, focusing on the factors privacy loss versus job security. This means that, due to the limited possibilities for employees' actions in the context of work, privacy calculus relates to the trade-off of factors on which employees can decide (such as continuation of the employment) rather than to the risk-benefit evaluation of a particular IoT system. This, in particular, distinguishes the applicability of privacy calculus at the workplace from the sectors private home and health.

With regard to CPM, findings suggest that the maintenance of individual privacy rules depends on the tracking capability of an IoT-based system. Thus, a privacy-preserving mode of operation allows to comply even with strict privacy rules, as for example, data are not recorded or forwarded. However, a privacy-invading monitoring system is not likely to be compatible with a regulatory privacy management of employees. Study III, therefore, illustrates that different IoT-based solutions can be applied at the workplace, which may differ with regard to their privacy-related settings. Therefore, it is necessary to continue examining particular devices and systems and to consider the application context in order to classify them within the privacy framework.

IV DISCUSSION

The present doctoral thesis aimed at extending the current knowledge about the decision-making process regarding the deployment of IoT technology in terms of privacy-related elaborations of individuals. For this purpose, three empirical studies investigated, whether privacy calculus provides a suitable theoretical framework in order to examine IoT acceptance. With respect to the heterogeneity of IoT (see Chapter 2.3.2), different devices were selected on the basis of results of preliminary studies, which were then tested in the respective main study. Furthermore, the three studies were conducted in different fields of application – smart home, healthcare and workplace – in order to consider specific characteristics of the situational context of IoT usage (see Chapter 2.3.3). In addition to the impact of the IoT device on the intention to use it, particular intrapersonal and environmental factors were tested for their influence on IoT adoption within the respective application context.

The following chapters deal with the overarching research questions of this dissertation (see Chapter III) raised on a meta-level:

- Is privacy calculus a suitable theory for the investigation of IoT and how does its application evolve within this framework?
- Which psychological mechanisms are involved in the risk-benefit tradeoff with regard to the situational context?
- What changes in the theoretical concept of privacy are necessary against the background of IoT dissemination?

To answer these questions, the discussion is built on considerations provided in the theoretical background (see Chapter II), which also include a new conceptualization of the levels of privacy introduced in Chapter 2.1.4, as well as the results of the empirical studies constituting the cumulus (see Chapter 3.1). On this basis, theoretical, practical and ethical implications are provided. In addition to the limitations of this work, future research is discussed against the background of the challenges of empirical investigations of IoT (see Chapter 2.3).

4.1 Privacy Calculus in the Framework of IoT

The privacy calculus theory (Culnan & Armstrong, 1999) formed the basis for all three empirical studies conducted in the context of the present doctoral thesis. This theory postulates that people weigh perceived risks against expected gratifications, when they have to take privacy-related decisions, such as whether to disclose personal data or not. This theory has been established particularly in the field of online communication (Bol et al., 2018; Chen, 2018; Dienlin & Metzger, 2016; Trepte et al., 2017). The aim of this dissertation was to extend the field of application of the privacy calculus theory to the framework of IoT deployment by investigating the effect of perceived privacy risks and expected benefits of a particular IoT device on its acceptance and whether individual's usage intention is grounded on the weighing of these two factors.

4.1.1 IoT Acceptance as a Binary Decision

Study I investigated the usage intention of an IoT household device depending on the device's convenience and tracking ability. In this study, participants had no possibility to adjust privacy setting of the smart household device. Nevertheless, the findings show that people evaluate both perceived risks and benefits of the device prior to their decision regarding the intention to use it. Furthermore, convenience positively affects the usage intention of the device. This means that people agree to extensive data tracking even without the option of any control over their data in order to benefit from the most convenient features. Similar results are provided by Study III, which examined employees' acceptance of an IoT emergency detection system at the workplace, depending on perceived risks and benefits. Findings from Study III reveal that although employees perceive privacy risks regarding the deployment of an IoT monitoring system at their workplace (e.g., collection and forwarding of person-related data), these risks do not affect the system's acceptance. In other words, people seem to tolerate or even to suppress perceived risks when they believe that they can benefit from IoT or, as it is the case at the workplace, that they can avoid negative consequences, such as job loss. Users of IoT have very limited if any autonomy in deciding what information they provide, since they do not actively share this information, but it is collected and aggregated by device sensors in a way that is not transparent to the user (Kröger, 2019). This fundamentally differs from the application of privacy calculus, for example, in the context of SNS. Although personal data (e.g., likes or the number of friends) can also be tracked on such platforms (Matz et al., 2020), SNS users, in principle, can actively decide whether and what information, such as status updates or pictures, they want to disclose. Moreover, most SNS offer the possibility to gradually adjust privacy settings, for instance who has access to personal information, and thus to regulate how much of their privacy individuals want to trade in order to use a network. According to these results in connection to particular characteristics of IoT, such as the lack of possibilities to control data collection, the decision concerning the deployment of IoT seems to be limited to the options either to accept a device or not. This means that the outcome of the privacy calculus associated with IoT usage is binary. Since the binary decision does not offer the possibility to only reveal little data in order to get at least some benefits, but instead follows the all or nothing principle, users must provide access to all the required data in order to benefit from the advantages of an IoT device. This is particularly evident in Study II, which investigated the usage intention of an eHealth device. Especially in order to benefit from health-related services, IoT applications in healthcare usually require (very) sensitive data, which users must provide in order to receive tailored services. Consequently, the binary outcome of the privacy calculus in relation to users' preference of benefits might be even more critical for user privacy.

4.1.2 Critical Reflection of the Privacy Calculus

Against the background of the interpretation of the privacy calculus as a binary decision and due to specific characteristics of IoT functionality, the critical reflection of privacy calculus (Acquisti, et al., 2015; Krämer & Schäwel, 2020; Masur, 2018), which has already been elaborated in earlier chapters, needs to be discussed again in more detail.

Study I reveals that although people indicate concerns regarding their privacy, they do not seem to care whether they deploy an IoT device capable of sophisticated tracking techniques. Although participants were informed in detail about the collection and processing of their data by the IoT household device, cognitive limitations (Acquisti et al., 2015) in connection to advanced technological properties of IoT, such as algorithms (DeVito, 2017), might be the reason that "the possibilities and implications of data linkage and pattern recognition are not well-understood by the average consumer" (Kröger, 2019, p. 155), even if sufficient information is provided. This means that participants read the descriptions of the respective scenario but potentially were not able to conclude, to what extent the tracking capability of the device might threaten their privacy. These results particularly stress that even if users are provided with all privacy-relevant information, as demanded by many scholars as a prerequisite for a rational decision (e.g., Masur, 2018), the mere access to information does not imperatively enforce rationality. This might be explained by a lack of awareness regarding the permanent tracking of everyday IoT devices, which is a crucial factor for the underestimation of privacy risks (Kröger, 2019). In other words, despite of having a certain degree of privacy knowledge, IoT users might just not recognize that their data is being recorded and processed, for instance due to the unobtrusive mode of operation of an IoT device. An example would be a person who has decided not to use IoT for privacy reasons and does not notice that his or her behavior is nevertheless captured by IoT devices of colleagues or family members.

Study II, which examined the usage intention of an eHealth device depending on actual and perceived control, demonstrates that perceived control significantly affects the willingness to apply the device. However, actual control enabled by technological means does not have any influence on this consideration. Thus, individuals do not seem to associate the control actually provided by the device with their estimation of control possibilities. This corroborates the results of Brough and Martin (2020), who showed that although privacy knowledge has been identified as a crucial determinant for privacy-relevant decisions (Bartsch & Dienlin, 2016; Baruh et al., 2017; Debatin, 2011; Trepte et al., 2017), the factual, procedural and experiential knowledge and hence the basis for thorough decision-making seems to be limited. Moreover, as perceived benefits had a stronger impact on the participation in the healthcare program than perceived risks, Study II points out that users might give priority to immediate gratification and thus, base their decision in favor of the IoT usage on a skewed balancing process of risks and benefits. These findings highlight the aspect of cognitive biases as they correspond to the hyperbolic discounting heuristic (Waldman, 2020), which states that immediate gratifications might outweigh future privacy risks due to individuals' inter-temporal choices. Additionally, the findings confirm results from previous studies regarding the fact that benefits might override risks (Metzger & Suh, 2017; Zheng et al., 2018).

In the workplace context, Study III found that notwithstanding the fact that employees reported a high perception of both privacy risks and privacy concerns, neither of these constructs affected the acceptance of an IoT monitoring system for emergency detection. Especially at the workplace, the implementation of tracking IoT technology is problematic as the refusal of this technology might lead to a job loss. Therefore, basing on the results of Study III, it can be assumed that employees resign on their privacy and accept IoT in order to retain the employment. In this regard, recent scientific investigations increasingly provide evidence that the complexity of privacy-related decisions, which accompany surveillance capitalism (Zuboff, 2019) or data capitalism (West, 2019), might result in privacy cynicism (Hoffmann et al., 2016). Privacy cynicism states that it is not realistic for users to act rationally as they "can no longer meaningfully participate in society without paying with their personal data as a kind of entrance fee" (Lutz et al., 2020, p.1169). As a consequence of uncertainty and powerlessness, people ignore potential privacy risks (Hoffmann et al., 2016), which reflects the findings from Study III. In other words, digital infrastructures of modern society inherently include the extraction of personal data leading to resignation of individuals regarding their privacy protection. For the theoretical development of privacy rationales this means that in addition to the consideration of privacy risks and benefits, specific characteristics of digital technologies such as permanent tracking or information inferencing and their effect on the individual must be addressed in order to provide more substantiated statements regarding privacy-related decisions. Still, the findings of the empirical studies included in this work confirm the impact of the risk-benefit trade-off on the acceptance of and the willingness to use a certain IoT device, strengthening privacy calculus as the most prominent approach to explain the paradoxical usage of data-requiring technology despite of perceived privacy concerns.

4.2 Situational Context and Factors of IoT Acceptance

The empirical studies presented in this work were conducted in three different fields of IoT application to shed light on potential contextual differences. In his theory of situational privacy and self-disclosure, Masur (2018) argues that different circumstances prevailing in a particular situation can determine the behavior and the perceptions of individual privacy. To be more precise, depending on the situational context, a person might experience different levels of privacy and have a high or a low willingness to provide personal data. Additionally it can be distinguished between personal factors, which comprise personality characteristics (Floyd et al., 2000), attitudes (Ajzen, 1991) or perceived states of privacy (Dienlin, 2014) and environmental factors, which remain stable across different situations but might still be perceived differently depending on the context. However, the studies of the cumulus have less of a comparative character and should be considered separately with regard to the respective situation. This is due to the varying design of the studies and the assessment of situation-specific factors, which not necessarily allow generalizing assumptions regarding the context. Therefore, in the following, specific aspects of each field of application are discussed and common tendencies are elaborated.

4.2.1 Characteristics of IoT Deployment in the Smart Home

When people deploy IoT in their private homes, they might have a stronger perception of privacy compared to other sectors of IoT application. This could be explained by mechanisms of environmental privacy specified by Altman (1975), such as the possibilities to obtain more privacy through physical distance to other people or territorial demarcation (e.g., fences and closed doors) and therefore to be less concerned about private data. In this respect, Study I demonstrated that the tracking ability of IoT devices, which are applied in private homes does not seem to be critical for the users. However, with regard to the technological level of privacy (see Chapter 2.1.4), it can be assumed that the territorial delineation does not lead to a stronger privacy protection, since IoT applications, even without active information disclosure of users, can access personal data within delineated areas or even the body. Hence, surrounded by networked data tracking technology, users are increasingly becoming transparent despite closed doors and raised fences. Thus, perceived privacy, which people might experience at home, potentially stems from a misconception because data in this field of application is as accessible as in public space by means of IoT technology. Nevertheless, the number of privately used IoT devices increases (Statista, 2016), which might be particularly attributed to the convenience of smart products and services (Zheng et al., 2018), also confirmed by the results of Study I.

Additionally, in the smart home context the moderating effect of privacy concerns and the attitude towards tracking were examined. The selection of these two constructs bases on the assumption that, contrary to the implementation of IoT for example at the workplace, the decision to deploy IoT in private homes, is mostly voluntary and personal attitudes therefore play a role in the implementation of IoT. Against this background, findings from Study I reveal moderating effects of both privacy concerns and the attitude towards tracking. Thus, the willingness to use a data-collecting IoT household device decreases, when the user is worried about his or her privacy or has a negative attitude towards tracking of personal information.

4.2.2 Characteristics of IoT Deployment in Healthcare

Switching the focus to the healthcare context, the use of IoT, especially in this sector, creates a strong tension between the enormous potential for the health of individuals, in terms of digitalized treatment and monitoring capabilities (Catarinucci et al., 2015), and the potentially negative consequences if collected and aggregated highly sensitive data is forwarded on a vertical axis of privacy (i.e. among providers, governments or institutions). Therefore, Study II investigated which factors have an effect in this ambiguity on the decision of individuals to use IoT. Control was assessed as both environmental (i.e. actual control) and personal factor (i.e. perceived control). Interestingly, the findings did not indicate any significant effect of actual control as an environmental factor on the intention to use an IoT fitness tracker. At the same time, perceived control as a personal factor affected both the usage intention and the risk-benefit trade-off. On the one hand, it can be concluded that individuals might have a different perception of environmental factors despite the fact that these factors are stable and do not change within a given situation. More concretely, in relation to situational control, this means that in addition to providing users of IoT healthcare devices with actual possibilities to control personal data, the challenge is to explain or communicate this possibility to the users. On the other hand, it becomes clear that while the usage decision is based on the privacy calculus, i.e. the weighing of perceived risks and benefits, these in turn can be influenced by other factors. Privacy calculus, therefore, seems to be a regulatable mechanism. Thus, predicting variables of perceived risks and benefits need to be identified for a better understanding of the black box behind the balancing process.

Another specific factor with regard to IoT deployment in healthcare are individuals' moral considerations. As the continuous collection and commercial use of health-related data, e.g., by health insurance companies, might have potential disadvantages not only on an individual level but also on a societal level (e.g., price discrimination, Mittelstadt, 2017), the sense of social responsibility and an individual's belief in a solidary community might be a hindering factor of IoT adoption (van den Hoven, 2017). This assumption is supported in Study II. People with a higher level of moral considerations indicate to have a lower intention to use IoT in healthcare. Conversely, this means that people expect technology to be shaped in a way that corresponds to moral values and ethical standards prevailing in a society.

4.2.3 Characteristics of IoT Deployment at the Workplace

With the application of IoT in the work context, an essential factor is the very limited or even non-existent decision-making power of employees with regard to the implementation of IoT systems. This means that contrary to the use of IoT in their private homes, employees must rely on the employer to take their interests into account when planning the introduction of IoT. Consequently, trust in the employer is a decisive factor in the acceptance of IoT at the workplace. Findings from Study III showed a direct effect of trust on the acceptance of IoT, however, there was no significant impact of trust on perceived privacy risks. Hence, employees reported a high perception of risks independent of a trusting relationship with the employer. Although worries of employees about being monitored at the workplace are not new (e.g., Severson, 1997; Zuboff, 1988), the enormous tracking potential of IoT technology reaching even deeper into the privacy of employees needs to be explicitly addressed by research. Given the ability of IoT to intrude all four dimensions of privacy (informational, social, psychological and physical) employees might worry about the monitoring of private conversations among colleagues or the exposure of their health state, for example by wearable IoT, such as work clothes equipped with sensors. Thus, employees might differentiate between their trust in the employer and their trust in the IoT system leading to a higher estimation of risks. Furthermore, as perceived privacy is tightly interwoven with individual control over one's data , the lack of control as it is prevalent at the workplace (Allen et al., 2007), might also contribute to a higher risk perception.

At their workplace, individuals seem to be particularly worried about their privacy. This is not only supported by the high perceptions of privacy concerns and risks in Study III but also by the impact of IoT system's tracking ability both on the acceptance of the system and on the risk-benefit calculation. The most striking result, however, is probably the missing relationship between perceived privacy risks and the system's acceptance. The fact that employees seem to accept IoT albeit their high estimation of privacy risks, demonstrates that particularly at work the options for individuals' actions in terms of privacy protection are restricted. This might lead to the feeling of having to come to terms with the technology in order to keep the employment, corresponding to the idea of privacy cynicism as a consequence of powerlessness (Hoffmann et al., 2016).

4.2.4 Common Tendencies Across the Contexts

The empirical studies that constitute the present dissertation cannot be exposed to a direct comparison as they are not identical in terms of design, and each study additionally examines context-specific factors which are not considered in the other studies. With a certain amount of caution, however, common tendencies can be observed across the contexts. Besides the applicability of the privacy calculus theory in all three contexts, it can be concluded from the results that potential consequences of data tracking for user privacy might differ with respect to the particular situation in which data is collected and that context-specific factors as important elements of the situation must be taken into account when examining IoT acceptance. At this point, however, it should be noted that the participants of all three studies were explicitly informed about the characteristics of the tested IoT device, including the ability of data tracking and processing. Therefore, the evaluation of an IoT device under real circumstances might be much more dependent on situational cues than on system properties, which users are not always aware of (Mikusz et al., 2018). Taken as a whole, the investigation of the three IoT application areas smart home, healthcare and workplace shows that individual's estimation of privacy depends on both personal and environmental factors in a given situation.

4.3 Theoretical Implications

In the course of the present thesis, which investigates privacy-relevant aspects of IoT implementation, this chapter aims to answer the question of how the conceptualization of privacy is changed by the dissemination of this networked technology in different fields of application. Therefore, results of the empirical studies will be discussed against the background of introduced privacy theories and the levels of privacy, which were elaborated in the course of this dissertation. The previously established consensus on the concept of privacy is characterized by well-defined principles and theories (e.g., Burgoon, 1982; Laufer & Wolfe, 1977; Westin, 1967) and differs only in some nuances e.g., in terms of the interrelation of privacy and control (Fried, 1984; Johnson, 1974). However, given the innovative methods of IoT to retrieve personal information, which at the same time are more privacy-intrusive than ever before, the perception and evaluation of privacy might undergo fundamental changes. This digital revolution, comprising privacy in the framework of IoT in recent years, has aroused broad scientific interest and established a new field of research, to which findings from this work aim to contribute.

4.3.1 Challenges for Prevailing Privacy Theories

Related to the privacy calculus (Dinev & Hart, 2006), findings from the empirical studies included in the cumulus allow the conclusion that perceived risks and benefits are weighed during the decision-making process whether to use an IoT device. However, due to the poor ability to regulate the operation of private data, the outcome of this trade-off seems to be limited to a binary decision: to either accept the deployment of IoT or not (comparatively represented as usage intention in Study I and II). These results challenge the current understanding of the privacy concept, because a binary decision no longer allows individuals to continuously adjust what Altman (1975) describes as the desired level of privacy. The adoption of IoT, furthermore, introduces substantial constraints to the argument of Westin (1967) that privacy can be obtained, if a person withdraws from the public, for example in a protected private space, because as long as an individual or people in the immediate environment use IoT devices, their behavior is permanently observable and data access is available. Moreover, the scenarios from the studies are based on characteristic IoT features, such as data tracking and processing. In this connection, CPM (Petronio, 2002) may also be questioned. If data is collected automatically, to what extent is active management of individuals' privacy still feasible?

At this point, the introduced levels of privacy (see Chapter 2.1.4) emphasize the detachment of IoT from interpersonal communication on which both Petronio (2002) and Burgoon (1982) rely in their definitions of privacy. In contrast to the authors' explanations regarding the communication of private information among human actors (i.e. on a social level), IoT communicates on a technological level, meaning that information is exchanged between connected devices and networks. Thus, it would be useful to complement privacy theories with the distinction of privacy levels to ensure a better understanding of the specific impact of IoT on users' privacy.

Finally, the empirical studies contradict the assumption of Altman (1975) and Burgoon (1982) regarding “the active role played by the seeker of privacy” (Burgoon, 1982, p. 209). After the acceptance of a device, the user rather plays a subordinate role with regard to the maintenance of privacy, as the usage of an IoT product or service might comprise the extraction of personal information about the user, including social encounters and relationships, environmental data and physical data (Kröger, 2019), and moreover, conclusions about the psychological state of the person derived from the collected data, such as mood or the perceived level of stress (Peppet, 2014). This extensive tracking of personal data is not constrained by time or location and is not necessarily connected to an active disclosure of the user. In this regard, the results strengthen Nissenbaum’s (2010) request, who argues that, perhaps with the exception of people completely isolated from society, theoretical considerations of privacy must take its growing limitations into account. With regard to the results of the studies, it seems that users already bear these limitations in mind as they apparently accept restrictions of their privacy for the use of IoT, potentially indicating growing privacy cynicism (Hoffmann et al., 2016).

4.3.2 The Control Paradigm

The previous section thoroughly outlined the extent to which the results of the current thesis broaden the understanding of privacy in the framework of IoT and how existing privacy theories might incorporate these changes. As Fried (1984) argues that privacy and control are two inherently interrelated concepts, as a second paradigm, control over personal information and its connection to the changing concept of privacy has to be also reconsidered in the context of IoT. In this regard, findings from Study II reveal the enormous relevance of perceived control. More concretely, when IoT users believe to be in control over their data, they have a stronger perception of the IoT device’s benefits while their perception of privacy risks decreases. Moreover, they report a higher intention to use the IoT device. Thus, Study II shows that the perception of control in a particular situation has an impact on both perceived risks and benefits of an IoT device, which demonstrates that privacy calculus to a certain degree depends on individuals’ control beliefs and stresses the relevance of the situational context.

Building on that, theoretical approaches should explore what possibilities of control IoT users recognize in order to predict their privacy-related behavior and perceptions. Although Tavani and Moor (2001) postulate that with the dramatically increasing dissemination of private information via computer networks, it is no longer possible to entirely obtain control over this information, the findings further indicate that not the actual control is crucial but rather those control possibilities which the user is aware of. On the one hand, these findings strengthen the differentiation of actual and perceived control (Ajzen, 2005; Skinner, 1996) and replicate the control paradox (Brandimarte et al., 2013). On the other hand, the idea of selective control over the disclosure of distinct information (Masur et al., 2017) is challenged by the potential misconception of actual and perceived control. When people believe to be in control of their data, but the device does not offer actual possibilities, for example, to adjust any privacy settings, they cannot selectively decide, what data they want to provide. Although, particular IoT devices offer at least some controlling mechanisms e.g., by means of privacy settings, such as the restriction of location determination, for the most part it is barely possible to effectively protect one's privacy due to IoT's capability to access all dimensions of privacy (Burgoon, 1982) and the lack of possibilities to withdraw from it. All three studies indicate that as a result, privacy might increasingly be threatened and its relevance might be faded out by IoT users in order to concentrate on the benefits rather than tackling with the risks, because 1) anticipated gratifications (which are potentially more present due to user's biased reasoning in connection to promising advertising campaigns) might constantly undermine perceived risks, 2) people are overwhelmed or have no sufficient knowledge of how to protect their privacy and 3) the constant confrontation with privacy breaches and the recurring need to adjust privacy settings for each device as well as the pressure to disclose data in order to participate in digital life might lead to resignation. As a result, in the future it could become a matter of course that people will be transparent in terms of their personal and behavioral information due to its permanent availability and accessibility by IoT. However, the deployment of privacy-intrusive technologies does not necessarily mean the end of privacy as proclaimed, for example, by Froomkin (2000). From the perspective of the introduced levels of privacy (see Chapter 2.1.4) it is still feasible for users to maintain control over private data on the human level and selectively to manage self-disclosure towards other people. Additionally, Trepte (2016) suggests that, against the background of autonomous data collection, selective control might be compensated by conventions of data use. This means that, on the technological level, privacy might be protected, for instance, by a legal framework in which terms about the nature and purpose of data use are defined in advance to the usage. In this respect, EU's General Data

Protection Regulation (GDPR) is a milestone following a promising approach. However, this legal regulation strengthens static privacy rights, such as the right to be informed about the purpose of the data collection, rather than dynamic perceptions of IoT users. Thus, the GDPR represents an important first step towards privacy protection but is not yet sufficiently refined with regard to individual privacy perception as Study II has shown that for IoT users it is essential to know that control is reassured for instance by the option to independently adjust privacy settings.

Taken together, it can be assumed that the integration of IoT in everyday life will significantly change our understanding and our perception of privacy. Therefore, the findings suggest that research needs to address specific privacy challenges related to control over personal data under consideration of the levels of privacy in order to provide extended sophisticated rationales as a theoretical basis for a better privacy protection.

4.4 Practical Implications

Against the background of the findings from the three empirical studies included in this thesis, the theoretical implications presented in the previous chapters can contribute to suggest possible applications for practice. The results indicate that the acceptance of an IoT device significantly depends on the presented information about the tracking capability of a device (Study III) and that users are rather willing to deploy certain IoT applications when they are informed about possible control options (Study II). Consequently, it is crucial to provide users of IoT with detailed information raising their knowledge as well as their awareness regarding sophisticated data-tracking techniques in order to enable self-determined decision-making in the realm of privacy issues in a best possible manner. This means that explicit information about data collection, data handling and possible inferences from potentially anonymous data must be presented to the users in a most comprehensible way. Thus, if people deliberately agree to make their data available by deploying IoT, this decision should be grounded on the most rational consideration of prevailing circumstances and factors. However, this would require a continuous reflection of the technologies surrounding us, and the willingness of individuals to stay informed about the latest technological advances and their impact on privacy. This effort and the fact that the decision for more privacy is not always in the hands of the users, makes it clear that the protection of privacy must by no means be burdened solely on the users. Instead, there must be regulations that not only require informed consent, such as the GDPR and other data protection laws, but also verify the conditions to ensure this consent. In conjunction with enhanced privacy knowledge, which was identified as a crucial determinant for profound privacy decisions (Bartsch & Dienlin, 2016; Trepte et al., 2015), such legal regulations could again strengthen the relevance of individual privacy and increase the pressure on manufacturers to focus more strongly on the currently insufficient privacy protection measures.

Furthermore, the findings of the empirical studies demonstrate a comparatively high acceptance or usage intention of IoT in all three contexts. This might also be interpreted in such a way that users potentially assume their data to be generally protected by IoT device manufacturers. This is especially reflected in Study I, as participants were willing to use a smart home device regardless of its tracking capability, because they potentially assumed that their data was secure. However, this is usually not the case as privacy-protecting solutions, such as PETs or privacy-by-default, are rarely preset, although their implementation is requested by many scholars (Kröger, 2019; Scarpato et al., 2017; Zheng et al., 2018). Privacy-by-default means that the settings of IoT products and services are, prior to initial usage, configured to collect the minimum amount of required information, to maintain anonymity to the greatest extent possible and hence, to work in a privacy preserving manner (Scarpato et al., 2017). Thus, as another practical implication, in addition to a more specific privacy legislation, from the data of the empirical studies can be derived that device manufacturers should bear a large part of the responsibility for protecting the privacy of consumers, e.g., by implementing privacy-by-default in the IoT development process. This is particularly important in the workplace context, as employees usually cannot modify privacy settings of implemented IoT systems. Study II also suggests that more control options, which IoT users are aware of, would raise the usage intention and should therefore be increasingly available to individuals. However, it remains to be seen whether these settings are sufficient to guarantee a high level of user privacy and whether this approach will be established, since many functions are based on private user data.

The high perception of risks in all three studies also draws attention to possible uncertainties of IoT users regarding their privacy. The findings, therefore, emphasize the necessity for a better privacy protection of consumers. In this context, new business models could evolve, which include new tools and approaches with the explicit purpose of restoring and maintaining consumer privacy. For instance, Gu and colleagues (2020) propose a cryptographic tool, which ensures anonymization by automatically hiding identifying information communicated via IoT networks. Chaabouni and colleagues (2019) provide a review on network intrusion detection systems, which are defense techniques developed to identify and prevent privacy attacks in the context of IoT. As people might be increasingly overwhelmed by the amount of privacy decisions resulting in a complete lack of self-protection potentially caused by overchoice bias (Hartzog, 2018, see Chapter 2.1.1), it would also be conceivable that IoT devices would automatically initiate privacy decisions based on initial identification of users' privacy preferences (which information is perceived as sensitive). As information about potential privacy-violating functions is not always accessible to users (Masur, 2018), another idea would be to print QR codes on the packaging of IoT devices so that consumers can easily obtain information about possible privacy impacts of these devices prior to purchase. Here, however, it would be important to ensure that the provided information is presented in a simple language without undermining the complexity of IoT. Alternatively, labels (that are already familiar from nutrition facts or energy consumption of technological devices) might be placed on packages of IoT devices as a more intuitive, visual method to inform consumers about privacy settings of the respective device (Kelley et al., 2009). For this purpose, certification institutions could be founded that assign the appropriate labels based on their profound technological expertise and support the privacy of consumers with potentially limited knowledge in their purchasing decisions.

Finally, the findings in connection to the increasing IoT usage clearly demonstrate that people are interested in the application of IoT and will continue to use this technology as long as they believe to benefit from it. In the light of this, policy makers could contribute to the strengthening of fundamental privacy rights not only through legislation on privacy protection, but also through enhanced support of research projects, institutions and innovative ideas on privacy protection. In this regard, Kröger (2019) stresses that concerns about potential violations of privacy "need to be addressed before IoT technologies are widely deployed – not only to protect the fundamental right to informational self-determination, but also to foster trust and acceptance among users" (p. 147).

4.5 Ethical Implications

Chapter 2.3.1 already outlined ethical challenges, which indicate that the dissemination of IoT technology increasingly raises issues regarding the responsibility of data handling, moral liability and potential changes of societal principles through digitalization (van den Hoven, 2017). From the contextual perspective, the empirical studies conducted in the course of this dissertation illustrate specific challenges in the respective field of application. Study I revealed that individuals are willing to deploy smart household appliances regardless IoT's tracking ability, hence allowing the technology to reach even deeper into their private lives. This raises the question, whether informed user consent, as demanded by the GDPR, is a valid instrument given the insufficient level of knowledge about extensive tracking of personal data (Brough & Martin, 2020) and the lack of awareness regarding potential privacy threats. As possibilities for potential privacy-intrusion “will continue to grow with further improvements of sensor technologies in terms of size, cost and accuracy, further advances in machine learning methods, and – most importantly – the predicted rapid proliferation of consumer IoT devices” (Kröger, 2019), it is essential that in addition to strengthening individual privacy rights, IoT users' options for active privacy protection are expanded. This is also supported by results of Study II, which show that perceived control over personal data positively affects the usage intention. Accordingly, policy makers must tackle the digital divide to ensure that people are able to stand up for their rights through informational self-determination. Strict legislation, however, may at the same time undermine people's autonomy and encourage them to leave the responsibility for their privacy entirely to the authorities. This is problematic because IoT users all the more need to request more detailed information to deepen their privacy knowledge to be able at least to some extent to estimate, whether legal requirements are enforced and implemented by manufacturers.

With regard to IoT in eHealth, Study II demonstrated that moral considerations negatively affect the usage intention of IoT in healthcare. To be more precise, the intention to use an eHealth device decreases when people worry about unequal medical treatment due to the introduction of IoT or varying insurance rates based on their health data. It is therefore becoming apparent that ethical research in the context of IoT needs to consider global issues beyond privacy. More urgent than the formulation of absolute restrictions is the identification of inequality through IoT. Health insurance companies, therefore, need to be held more accountable to avoid potential discrimination.

In the context of the workplace, findings from Study III reveal that even if employees perceive high privacy risks, they might still accept the implementation of a monitoring IoT system. This poses two fundamental questions: first, to what extent the decision to accept the system and thus to provide private (and sensitive) data is voluntary? And second, does the user still have any decision-making power with respect to deviating (commercial) interests of institutions (Leong & Chen, 2020) and unbalanced power-relations between employer and staff? The workplace can no longer be a legal grey area when it comes to employee privacy, especially, because results provide evidence that employees highly value their privacy and report a decreasing acceptance, the more data is collected by IoT installed at the workplace (Study III). Although, an increasing number of regulations, such as the European Union’s GDPR (which are among the strictest in the world; Matz et al., 2020) or the California Consumer Privacy Act of 2018, focus on better transparency, for example of data collection and processing, in order to strengthen fundamental privacy rights of individuals, particular aspects need to be regulated more strongly. For this purpose, it might be helpful to establish ethical boards specialized in IoT, which develop guidelines for digital applications, monitor their use and recognize potentials for discrimination, which might already be transferred into the technology during the development process, because they may be anchored unreflectively in some people's minds. In this way, a responsible technologization can be supported that is in line with moral values and the prevailing social structures.

4.6 Limitations and Future Research

The present doctoral thesis represents a first attempt to transfer privacy calculus as an underlying theoretical basis from online communication to the framework of IoT. Although limitations of this theory regarding the rational acting user with full agency have been comprehensively discussed in this work, the empirical studies initially follow the assumption of a rational individual. These investigations are thus the starting point for further in-depth research on privacy-relevant factors of IoT deployment. To get a holistic picture, further investigations explicitly need to address bounded rationality of individuals.

More concretely, in all three studies of the cumulus, participants reported a rather high level of perceived risks and piracy concerns when they were presented different IoT devices. However, attention should be paid to the fact that the scenarios of each study design contained explicit information of the device's tracking techniques and capabilities in order to raise participants' awareness. Under real circumstances, it is often not recognizable for the user that data is being recorded (Mikusz et al., 2018), and all the more, which inferences can be retrieved from sensor data (Zheng et al., 2018) potentially leading to an underestimation of privacy risks (Kröger, 2019). Hence, future studies need to focus on user's actual awareness of IoT tracking capability in connection with potential privacy risks. Literature also suggests considering further limitations, such as the impact of cognitive biases (Krämer & Schäwel, 2020). This is particularly relevant because manufacturers might take advantage of users' decision processes based on heuristic thinking in order to persuading them to use IoT or nudge them to provide more personal data (Waldman, 2020).

The empirical studies included in the cumulus, as already mentioned, have less a comparative character but should be considered individually in the situation. In addition to the consideration of context-specific factors, the studies also differ in terms of design. Although conclusions can be drawn regarding the impact of risks and benefits and the acceptance of IoT in the respective field of application, in the future, scientific investigations should also apply the same designs in different contexts in order to be able to make comparisons and identify commonalities as well as fundamental differences in the application of IoT in diverse areas.

A further limitation lies in the methodological approaches used in the empirical studies. Study I and III included a quantitative method with realistic vignettes describing characteristics and tracking capabilities of the tested IoT device, which were thoroughly aligned to latest information available from manufacturer websites. However, a scenario-based approach represents a hypothetical situation, meaning that participants' attitudes, perceptions and behaviors might differ when the study is replicated under real circumstances. Although Study II used a cover story as an instrument and approximated a real situation, in which participants could test the IoT device and confirm their actual willingness to use it, it nevertheless was conducted under laboratory conditions. Therefore, further scientific approaches need to reflect on the IoT usage in everyday life. This requires more subtle methods such as ambulatory assessment, which better represent the realm of IoT users and allow behavioral observation under consideration of actual environmental conditions.

4.7 Conclusion

The present dissertation aimed to expand the understanding regarding the influence of interconnected IoT technology on user privacy and to reflect on intrapersonal and environmental factors which affect IoT acceptance. The empirical studies, which constitute the cumulus, were conducted in three different fields of application – smart home, healthcare and workplace. The main findings illustrate that people optimize their privacy-related decisions whether to use IoT by weighing perceived risks against anticipated gratifications of this technology and provide a valuable foundation for the transfer of privacy calculus theory to the framework of IoT. The contextual perspective of the empirical studies contributes to the identifications of situation-specific factors of IoT acceptance. Study I stresses that convenience is a crucial factor when people consider deploying IoT in their private homes. Study II highlights the relevance of perceived control over private data together with users' moral considerations as determinants for the usage of IoT in healthcare. Finally, Study III confirms that individual's acceptance of IoT at their workplace significantly depends on the tracking ability of the respective IoT system and their trust towards the employer. However, these promising results indicate that the application of privacy calculus as a theoretical basis for investigations of IoT must undergo distinct changes due to system-based characteristics, restricting the outcome of the risk-benefit trade-off to a binary decision: to either accept IoT or not. A further innovativeness of this doctoral thesis is the introduction of the levels of privacy.

The elaboration of the human and the technological level is grounded on a consolidation of existent privacy theories and represents a sophisticated approach, which is specifically tailored to the theoretical investigations of IoT. In the course of these developments, further explorations on the conceptualization of privacy in the context of IoT are provided. Additionally, this work addresses particular challenges of empirical investigation of IoT. Taken together, the present dissertation not only sheds light on the prominent topic of human-computer interaction, but also expands our knowledge regarding the privacy calculus and its effect on the application of networked technologies and proposes extensions to existing privacy theories in the context of IoT.

V References

Abu Waraga, O., Bettayeb, M., Nasir, Q., & Abu Talib, M. (2020). Design and implementation of automated IoT security testbed. *Computers and Security, 88,* 101648. https://doi.org/10.1016/j.cose.2019.101648

Acquisti, A., & Grossklags, J. (2006). Privacy Attitudes and Privacy Behavior. In *Economics of Information Security* (pp. 165-178). Springer, Boston, MA. https://doi.org/10.1007/1-4020-8090-5_13

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*(2), 160-174. https://doi.org/10.1509/jmr.09.0215

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). The Economics of Privacy. *Journal of economic Literature, 54(2), 442-92.* https://doi.org/10.2139/ssrn.2580411

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of privacy: Framing, disclosures, and the limits of transparency. In *SOUPS 2013 - Proceedings of the 9th Symposium on Usable Privacy and Security,* 1-11. https://doi.org/10.1145/2501604.2501613

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour. New Jersey: Prentice-Hall. *Englewood Cliffs*.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2005). *Attitudes, Personality and Behavior* (Second Edition). McGraw-Hill Education (UK). https://doi.org/10.1037/e418632008-001

Alblooshi, M., Salah, K., & Alhammadi, Y. (2019). Blockchain-based Ownership Management for Medical IoT (MIoT) Devices. In *Proceedings of the 13th International Conference on Innovations in Information Technology, IIT 2018*, 151-156. https://doi.org/10.1109/INNOVATIONS.2018.8606032

AlHogail, A. (2018). Improving IoT technology adoption through improving consumer trust.

Technologies, 6(3), 64.

Allen, M. W., Walker, K. L., Coopman, S. J., & Hart, J. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly, 21*(2), 172-200. https://doi.org/10.1177/0893318907306033

Almetere, E. S., Kelana, B. W. Y., & Mansor, N. N. A. (2020). Using UTAUT Model to Determine Factors Affecting Internet of Things Acceptance in Public Universities. *International Journal of Academic Research in Business and Social Sciences, 10*(2). https://doi.org/10.6007/ijarbss/v10-i2/6915

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, California: Brooks/Cole. https://doi.org/10.1177/0013916507304699

Altman, I. (1976). A conceptual analysis. *Environment and behavior*, *8*(1), 7-29.

Altman, I. (1990). Toward a Transactional Perspective. In *Environment and Behavior Studies,* 225-255. Springer, Boston, MA. https://doi.org/10.1007/978-1-4684-7944-7_10

Ammirato, S., Sofo, F., Felicetti, A. M., & Raso, C. (2019). A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context. *European Journal of Innovation Management*. https://doi.org/10.1108/EJIM-03-2018-0058

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805.*

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2* (2), 1-23. https://doi.org/10.1145/3214262

Atlam, H. F., & Wills, G. B. (2020). IoT Security, Privacy, Safety and Ethics. In *Internet of Things* (pp.123-149). Springer, Cham. https://doi.org/10.1007/978-3-030-18732-3_8

Averill, J. R. (1973). Personal control over aversive stimuli and its relationship to stress. *Psychological Bulletin, 80* (4), 286. https://doi.org/10.1037/h0034845

Bai, X., Yin, J., & Wang, Y. P. (2017). Sensor Guardian: prevent privacy inference on Android sensors. *Eurasip Journal on Information Security, 2017*(1), 10. https://doi.org/10.1186/s13635-017-0061-8

Ball, K. (2010). Workplace surveillance: an overview. *Labor History, 51* (1), 87-106.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*. https://doi.org/10.5210/fm.v11i9.1394

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56,* 147-154. https://doi.org/10.1016/j.chb.2015.11.022

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication, 67*(1), 26-53. https://doi.org/10.1111/jcom.12276

Bassi, A., & Lange, S. (2013). The need for a common ground for the IoT: The history and reasoning behind the iot-a project. In *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model,* (pp. 13-16). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40403-0_2

Beales, H., & Muris, T. J. (2019). Privacy and Consumer Control. *George Mason Law & Economics Research Paper,* 19-27. https://doi.org/10.2139/ssrn.3449242

Bedhief, I., Kassar, M., & Aguili, T. (2016). SDN-based architecture challenging the IoT heterogeneity. In *2016 3rd Smart Cloud Networks and Systems, SCNS* (pp 1-3). IEEE. https://doi.org/10.1109/SCNS.2016.7870558

Bokefode, J. D., Bhise, A. S., Satarkar, P. A., & Modani, D. G. (2016). Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption. *Procedia Computer Science*, *89*(2), 43-50. https://doi.org/10.1016/j.procs.2016.06.007

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Brough, A. R., & Martin, K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology, 31,* 11-15. https://doi.org/10.1016/j.copsyc.2019.06.021

Brown, M., Coughlan, T., Lawson, G., Goulden, M., Houghton, R. J., & Mortier, R. (2013). Exploring interpretations of data from the internet of things in the home. *Interacting with Computers*, *25*(3), 204-217. https://doi.org/10.1093/iwc/iws024

Burger, J. M. (1989). Negative Reactions to Increases in Perceived Personal Control. *Journal of Personality and Social Psychology, 56*(2), 246. https://doi.org/10.1037/0022-

3514.56.2.246

Burgoon, J. K. (1982). Privacy and Communication. *Annals of the International Communication Association, 6*(1), 206-249. https://doi.org/10.1080/23808985.1982.11678499

Calo, R. (2014). Digital Market Manipulation. 82 George Washington Law Review 995 (2014); University of Washington School of Law Research Paper No. 2013-27, August 15, 2013. https://doi.org/10.2139/ssrn.2309703

Canedo, J., & Skjellum, A. (2016). Using machine learning to secure IoT systems. In *2016 14th Annual Conference on Privacy, Security and Trust, PST* (pp. 219-222). IEEE. https://doi.org/10.1109/PST.2016.7906930

Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal, 2*(6), 515-526. https://doi.org/10.1109/JIOT.2015.2417684

Celik, Z. B., Babun, L., Sikder, A. K., Aksu, H., Tan, G., McDaniel, P., & Uluagac, A. S. (2018). Sensitive information tracking in commodity IoT. *Proceedings of the 27th USENIX Security Symposium* (pp. 1687-1704).

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys and Tutorials, 21*(3), 2671-2701. https://doi.org/10.1109/COMST.2019.2896380

Chacko, V., & Bharati, V. (2018). Data validation and sensor life prediction layer on cloud for IoT. *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017* (pp. 906-909). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.139

Chen, H. T. (2018). Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist, 62*(10), 1392-1412. https://doi.org/10.1177/0002764218792691

Chen, K. C., & Lien, S. Y. (2014). Machine-to-machine communications: Technologies and challenges. *Ad Hoc Networks, 18,* 3-23. https://doi.org/10.1016/j.adhoc.2013.03.007

Chinaei, M. H., Gharakheili, H. H., & Sivaraman, V. (2020). *Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract.* arXiv. https://arxiv.org/pdf/2007.03330.pdf

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems,* 319-340. https://doi.org/10.2307/249008

de Matos, E., Tiburski, R. T., Moratelli, C. R., Johann Filho, S., Amaral, L. A., Ramachandran, G., Krishnamachari, B., & Hessel, F. (2020). Context information sharing for the Internet of Things: A survey. *Computer Networks, 166,* 106988. https://doi.org/10.1016/j.comnet.2019.106988

Debatin, B. (2011). Ethics, Privacy, and Self-Restraint in Social Networking. In *Privacy Online* (pp. 47-60). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21521-6_5

DeVito, M. A. (2017). From Editors to Algorithms: A values-based approach to understanding story selection in the Facebook news feed. *Digital Journalism*, *5*(6), 753-773. https://doi.org/10.1080/21670811.2016.1178592

Dienlin, T. (2014). The privacy process model. In *Medien und Privatheit [Media and Privacy]*, 105-122.

Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dünnebeil, S., Sunyaev, A., Blohm, I., Leimeister, J. M., & Krcmar, H. (2012). Determinants of physicians' technology acceptance for e-health in ambulatory care. *International Journal of Medical Informatics, 81*(11), 746-760. https://doi.org/10.1016/j.ijmedinf.2012.02.002

Economides, A. A. (2017). User Perceptions of Internet of Things (IoT) Systems. In *International Conference on E-Business and Telecommunications* (pp. 3-20). Springer, Cham. https://doi.org/10.1007/978-3-319-67876-4_1

Eibl, G., & Engel, D. (2015). Influence of data granularity on smart meter privacy. *IEEE Transactions on Smart Grid, 6* (2), 930-939. https://doi.org/10.1109/TSG.2014.2376613

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2019). Privacy expectations and preferences in an IoT world. *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017* (pp. 399-412).

European Commission (2020). *New Eurobarometer shows what EU citizens feel about cybercrime*. European Commission. https://ec.europa.eu/home-affairs/news/20200129_special-eurobarometer-cyber-security_en

Fahrenberg, J., Myrtek, M., Pawlik, K., & Perrez, M. (2007). Ambulatory Assessment - Monitoring Behavior in Daily Life Settings. *European Journal of Psychological Assessment, 23*(4), 206. https://doi.org/10.1027/1015-5759.23.4.206

Feng, X., Li, Q., Wang, H., & Sun, L. (2018). Acquisitional rule-based engine for discovering Internet-of-Thing devices. *Proceedings of the 27th USENIX Security Symposium* (pp. 327-341).

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fox, G. (2020). “To protect my health or to protect my health privacy?” A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology, 71* (9), 1015-1029. https://doi.org/10.1002/asi.24369

Fried, C. (1984). Privacy. *Philosophical dimensions of privacy*, 203-222.

Froomkin, A. M. (2000). The Death of Privacy? *Stanford Law Review, 52,* 1461. https://doi.org/10.2307/1229519

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal, 5*(4), 2483-2495. https://doi.org/10.1109/JIOT.2017.2767291

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gilmore, J. N. (2016). Everywear: The quantified self and wearable fitness technologies. *New Media and Society, 18*(11), 2524-2539. https://doi.org/10.1177/1461444815588768

Golbeck, J., & Mauriello, M. L. (2016). User perception of Facebook app data access: A comparison of methods and privacy concerns. *Future Internet, 8*(2), 9. https://doi.org/10.3390/fi8020009

Greengard, S. (2015). *The internet of things*. MIT press.

Gu, K., Zhang, W., Lim, S. J., Sharma, P. K., Al-Makhadmeh, Z., & Tolba, A. (2020).

Reusable mesh signature scheme for protecting identity privacy of IoT devices. *Sensors, 20*(3), 758. https://doi.org/10.3390/s20030758

Gudymenko, I., Borcea-Pfitzmann, K., & Tietze, K. (2011, November). Privacy implications of the internet of things. In *International Joint Conference on Ambient Intelligence,* 280-286.

Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Handel, B. R. (2013). Adverse selection and inertia in health insurance markets: When nudging hurts. *American Economic Review*, *103*(7), 2643-82. https://doi.org/10.1257/aer.103.7.2643

Hargreaves, T., Wilson, C., & Hauxwell-Baldwin, R. (2018). Learning to live in a smart home. *Building Research and Information*, *46*(1), 127-139. https://doi.org/10.1080/09613218.2017.1286882

Hartzog, W. (2018). *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press. https://doi.org/10.4159/9780674985124

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., & Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems, 56*, 701-718. https://doi.org/10.1016/j.future.2015.09.016

Hirschman, E. C. (1980). Innovativeness, Novelty Seeking, and Consumer Creativity. *Journal of Consumer Research,7*(3), 283-295. https://doi.org/10.1086/208816

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2019). Drivers and Inhibitors of Internet Privacy Concern: A Multidimensional Development Theory Perspective. *Journal of Business Ethics,* 1-26. https://doi.org/10.1007/s10551-019-04237-1

Ibrahim, M., Alsheikh, A., & Matar, A. (2020). Attack graph modeling for implantable pacemaker. *Biosensors, 10*(2), 14. https://doi.org/10.3390/bios10020014

Johnson, C. A. (1974). Privacy as personal control. *Man-environment interactions: evaluations and applications: part*, *2*, 83-100.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618-644. https://doi.org/10.1016/j.dss.2005.05.019

Júnior, J. F., Carvalho, E., Ferreira, B. V., De Souza, C., Suhara, Y., Pentland, A., & Pessin, G. (2017). Driver behavior profiling: An investigation with different smartphone sensors and machine learning. *PLoS one, 12(4), e0174959.* https://doi.org/10.1371/journal.pone.0174959

Kao, Y. S., Nawata, K., & Huang, C. Y. (2019). An exploration and confirmation of the factors influencing adoption of IoT-basedwearable fitness trackers. *International Journal of Environmental Research and Public Health*, *16*(18), 3227. https://doi.org/10.3390/ijerph16183227

Karakostas, B. (2017). Towards autonomous IoT logistics objects. In *The Internet of Things in the Modern Business Environment* (pp. 210-222). IGI Global.

Karapiperis, D., Birnbaum, B., Brandenburg, A., Castagna, S., Greenberg, A., Harbage, R., & Obersteadt, A. (2015). Usage-Based Insurance and Vehicle Telematics: Insurance Market and Regulatory Implications. *National Association of Insurance Commissioners & The Center for Insurance Policy and Research*, *1*, 1-79.

Kazai, G., Yusof, I., & Clarke, D. (2016). Personalised news and blog recommendations based on user location, facebook and twitter user profiling. *SIGIR 2016 - Proceedings of the 39th International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 1129-1132). https://doi.org/10.1145/2911451.2911464

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A “nutrition label” for privacy. *SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security,* 1-12. https://doi.org/10.1145/1572532.1572538

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273-281. https://doi.org/10.1016/j.chb.2018.11.022

Kim, T., Barasz, K., & John, L. K. (2019). Why am i seeing this ad? The effect of ad transparency on ad effectiveness. *Journal of Consumer Research*, *45*(5), 906-932. https://doi.org/10.1093/jcr/ucy039

Kim, Y., Park, Y., & Choi, J. (2017). A study on the adoption of IoT smart home service: using Value-based Adoption Model. *Total Quality Management and Business Excellence*, *28*(9-10), 1149-1165. https://doi.org/10.1080/14783363.2017.1310708

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Korczynski, M. (2000). The political economy of trust. *Journal of Management Studies, 37*(1). https://doi.org/10.1111/1467-6486.00170

Kotsopoulos, D., Bardaki, C., Lounis, S., Papaioannou, T., & Pramatari, K. (2017). Designing an IoT-enabled gamification application for energy conservation at the workplace: Exploring personal and contextual characteristics. *30th Bled EConference: Digital Transformation - From Connecting Things to Transforming Our Lives, BLED 2017* (p. 25). https://doi.org/10.18690/978-961-286-043-1.26

Kowatsch, T., & Maass, W. (2012). Critical privacy factors of internet of things services: An empirical investigation with domain experts. In *Mediterranean Conference on Information Systems* (pp. 200-211). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33244-9_14

Krämer, N. C., & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, *31*, 67-71. https://doi.org/10.1016/j.copsyc.2019.08.003

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Kravčík, M., Ullrich, C., & Igel, C. (2017). Towards industry 4.0: leveraging the internet of things for workplace learning and training. *Proceedings of the Workshop on European TEL for Workplace Learning and Professional Development*.

Kröger, J. (2019). Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. *IFIP Advances in Information and Communication Technology* (pp. 147-159). Springer, Cham. https://doi.org/10.1007/978-3-030-15651-0_13

Laplante, P. A., & Laplante, N. (2016). The Internet of Things in Healthcare: Potential Applications and Challenges. *IT Professional*, *18*(3), 2-4. https://doi.org/10.1109/MITP.2016.42

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22-42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, H., & Kobsa, A. (2017). Understanding user privacy in Internet of Things environments. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016* (pp. 407-412). IEEE.

https://doi.org/10.1109/WF-IoT.2016.7845392

Lee, L., Lee, J., Egelman, S., & Wagner, D. (2017). Information disclosure concerns in the age of wearable computing. In *NDSS Workshop on Usable Security (USEC)* (Vol. 1). https://doi.org/10.14722/usec.2016.23006

Lee, S., Ha, H. R., Oh, J. H., & Park, N. (2018). The Impact of Perceived Privacy Benefit and Risk on Consumers' Desire to Use Internet of Things Technology. In *International Conference on Human Interface and the Management of Information* (pp. 609-619). Springer, Cham. https://doi.org/10.1007/978-3-319-92046-7_50

Leong, Y. Y., & Chen, Y. C. (2020). Cyber risk cost and management in IoT devices-linked health insurance. *Geneva Papers on Risk and Insurance: Issues and Practice,* 1-23. https://doi.org/10.1057/s41288-020-00169-4

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471-481. https://doi.org/10.1016/j.dss.2012.06.010

Lu, J., Sookoor, T., Srinivasan, V., Gao, G., Holben, B., Stankovic, J., Field, E., & Whitehouse, K. (2010). The smart thermostat: Using occupancy sensors to save energy in homes. *SenSys 2010 - Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems* (pp. 211-224). https://doi.org/10.1145/1869983.1870005

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media and Society*, *22*(7), 1168-1187. https://doi.org/10.1177/1461444820912544

Mähler, V., & Westergren, U. H. (2018, September). Working with IoT–A Case Study Detailing Workplace Digitalization Through IoT System Adoption. In *IFIP International Internet of Things Conference* (pp. 178-193). Springer, Cham. https://doi.org/10.1007/978-3-030-15651-0_15

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Margulis, S. T. (2011). Three Theories of Privacy: An Overview. In *Privacy Online* (pp. 9-17). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21521-6_2

Markos, E., Labrecque, L. I., & Milne, G. R. (2018). A New Information Lens: The Self-concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information. *Journal of Interactive Marketing*, *42*, 46-62. https://doi.org/10.1016/j.intmar.2018.01.004

Masur, P. K. (2018). Situational privacy and self-disclosure: Communication processes in online environments. In *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Springer. https://doi.org/10.1007/978-3-319-78884-5

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Online Privacy Literacy Scale (OPLIS). Entwicklung und validierung der online-privatheitskompetenzskala [Development and validation of the Online Privacy Literacy Scale]. *Diagnostica*. https://doi.org/10.1026/0012-1924/a000179

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-32. https://doi.org/10.1145/3359183

Matz, S. C., Appel, R. E., & Kosinski, M. (2020). Privacy in the age of psychological targeting. *Current Opinion in Psychology, 31,* 116-121. https://doi.org/10.1016/j.copsyc.2019.08.010

Mcmillan, C. (2019). Envisioning Value-Rich Design for IoT Wearables. *Textile Intersections, 12-14 September, 2019. London, UK*. https://doi.org/https://doi.org/ 10.17028/rd.lboro.9724637

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication*, *8*(2), 291-301. https://doi.org/10.17645/mac.v8i2.2846

Metzger, M. J., & Suh, J. J. (2017). Comparative Optimism About Privacy Risks on Facebook. *Journal of Communication*, *67*(2), 203-232. https://doi.org/10.1111/jcom.12290

Mikusz, M., Houben, S., Davies, N., Moessner, K., & Langheinrich, M. (2018). *Raisin*g Awareness of IoT Sensor Deployments. *Cybersecurity of the IoT - 2018* https://doi.org/10.1049/cp.2018.0009

Mittelstadt, B. (2017). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology*, *19*(3), 157-175. https://doi.org/10.1007/s10676-017-9426-4

Naslund, J. A., Aschbrenner, K. A., & Bartels, S. J. (2016). Wearable devices and smartphones for activity tracking among people with serious mental illness. *Mental Health and Physical Activity, 10,* 10-17. https://doi.org/10.1016/j.mhpa.2016.02.001

Neyaz, A., Kumar, A., Krishnan, S., Placker, J., & Liu, Q. (2020). Security , Privacy and Steganographic Analysis of FaceApp and TikTok. *International Journal of Computer Science and Security*, *14*(2), 38.

Niranjana Devi, K., & Muthuselvi, R. (2016). Parallel processing of IoT health care applications. *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO* (pp. 1-6). IEEE. https://doi.org/10.1109/ISCO.2016.7727039

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford: Stanford Law Books.

Noah, T., Schul, Y., & Mayo, R. (2018). When both the original study and its failed replication are correct: Feeling observed eliminates the facial-feedback effect. *Journal of Personality and Social Psychology*, *114*(5), 657. https://doi.org/10.1037/pspa0000121

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Parate, A. (2014). *Designing Efficient and Accurate Behavior-Aware Mobile Systems*. Doctoral Dissertations. University of Massachusetts Amherst. https://doi.org/10.7275/bdkd-6796 https://scholarworks.umass.edu/dissertations_2/224

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303. https://doi.org/10.1016/j.chb.2014.05.041

Patil, K. (2017). Retail adoption of Internet of Things: Applying TAM model. *International Conference on Computing, Analytics and Security Trends, CAST* (pp. 404-409). IEEE. https://doi.org/10.1109/CAST.2016.7915003

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, Privacy, Security, And consent. *Texas Law Review, 93*, 85.

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IT Professional*, *17*(3), 32–39. https://doi.org/10.1109/MITP.2015.34

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, *2*(3), 175-196. https://doi.org/10.1111/j.1756-2589.2010.00052.x

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing*, *3*(2), 36–45. https://doi.org/10.1109/MCC.2016.28

Pötter, H. B., & Sztajnberg, A. (2016). Adapting heterogeneous devices into an IoT context-aware infrastructure. *Proceedings - 11th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, SEAMS* (pp. 64-74). https://doi.org/10.1145/2897053.2897072

Rao, A., Schaub, F., Sadeh, N., Acquisti, A., & Kang, R. (2019). Expecting the unexpected: Understanding mismatched privacy expectations online. *SOUPS 2016 - 12th Symposium on Usable Privacy and Security* (pp. 77-96).

Rizal, R., Riadi, I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *7*(4), 382-390.

Rogers, E. M. (1983). *Diffusion of innovations.* Simon and Schuster. https://doi.org/10.1002/chp.4750170109

Saheb, T. (2020). An empirical investigation of the adoption of mobile health applications: integrating big data and social media services. *Health Technology, 10*(5), 1063–1077. https://doi.org/10.1007/s12553-020-00422-9

Scarpato, N., Pieroni, A., Di Nunzio, L., & Fallucchi, F. (2017). E-health-IoT universe: A review. *International Journal on Advanced Science, Engineering and Information Technology*, *21*(44), 46. https://doi.org/10.18517/ijaseit.7.6.4467

Schomakers, E. M., Biermann, H., & Ziefle, M. (2020). Understanding privacy and trust in smart home environments. In *International Conference on Human-Computer Interaction* (pp. 513-532). Springer, Cham. https://doi.org/10.1007/978-3-030-50309-3_34

Severson, R. J. (1997). *The principles of information ethics*. ME Sharpe.

Shahraki, A., & Haugen, O. (2018). Social ethics in Internet of Things: An outline and review. *Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS* (pp. 509-516). IEEE. https://doi.org/10.1109/ICPHYS.2018.8390757

Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE Internet of Things Journal*, *6*(5), 7702-7712. https://doi.org/10.1109/JIOT.2019.2901840

Simon, H. A. (1982). *Models of Bounded Rationality*. MIT Press, Cambridge, Mass.

Skinner, E. A. (1996). A Guide to Constructs of Control. *Journal of Personality and Social Psychology*, *71*(3), 549. https://doi.org/10.1037/0022-3514.71.3.549

Smith, D. (2003). *Five principles for research ethics.* Apa.

https://www.apa.org/monitor/jan03/principles.aspx

Statista (2016). *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*. Statista. https://www.statista.com/statistics/ 471264/iot-number-of-connected-devices-worldwide/

Stieglitz, S., Potthoff, T., & Kißmer, T. (2017). Digital Nudging am Arbeitsplatz: Ein Ansatz zur Steigerung der Technologieakzeptanz [Digital nudging at the workplace: an approach to increase technology acceptance]. *HMD Praxis Der Wirtschaftsinformatik*. https://doi.org/10.1365/s40702-017-0367-5

Su, W., BI, X. H., & Wang, L. (2013). Research on user acceptance model of internet of things based on UTAUT theory. *Information Science*, *5*, 128-132.

Tabassum, M., Kosinski, T., & Lipford, H. R. (2019). " 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)*.

Tang, Q., Vidrine, D. J., Crowder, E., & Intille, S. S. (2014). Automated detection of puffing and smoking with wrist accelerometers. *Proceedings - PERVASIVEHEALTH 2014: 8th International Conference on Pervasive Computing Technologies for Healthcare* (pp. 80-87). https://doi.org/10.4108/icst.pervasivehealth.2014.254978

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM SIGCAS Computers and Society*, *31*(1), 6-11. https://doi.org/10.1145/572277.572278

Transforma Insights (2020). *Global IoT market will grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue.* Transforma. https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030

Trepte, S. (2016). Die Zukunft der informationellen Selbstbestimmung – Kontrolle oder Kommunikation? [The future of information self-determination: Control or communication?] In N. Horn (Ed.), *Die Zukunft der informationellen Selbstbestimmung [The future of informational self-determination]* (pp. 159–170). Berlin: Bundesstiftung für Daten-schutz.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media and Society*, *3*(1). https://doi.org/10.1177/2056305116688035

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale”(OPLIS). In *Reforming European data protection* *law* (pp. 333-365). Springer, Dordrecht.

TRUSTe Research (May, 2014). *Internet of Things Industry Brings Data Explosion, but Growth Could Be Impacted by Consumer Privacy Concerns*. TRUSTe. www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion-but-growth-could-be-impacted-by-consumer-privacy-concerns.

Tu, M. (2018). An exploratory study of internet of things (IoT) adoption intention in logistics and supply chain management a mixed research approach. *International Journal of Logistics Management*. https://doi.org/10.1108/IJLM-11-2016-0274

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124

van den Hoven, J. (2017). Ethics for the digital age: Where are the moral specs? In *Informatics in the Future* (pp. 65-76). Springer, Cham.

van Deursen, A. J. A. M., & Mossberger, K. (2018). Any Thing for Anyone? A New Digital Divide in Internet-of-Things Skills. *Policy and Internet*, *10*(2), 122-140. https://doi.org/10.1002/poi3.171

van Kranenburg, R., & Bassi, A. (2012). IoT Challenges. *Communications in Mobile Computing*, *1*(1), 9. https://doi.org/10.1186/2192-1121-1-9

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 16.

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480. https://doi.org/10.1016/j.giq.2016.06.004

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly: Management Information Systems*, 425-478. https://doi.org/10.2307/30036540

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, *31*, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). "I regretted the minute I pressed share": A qualitative study of regrets on Facebook. *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security* (pp.

1-16). https://doi.org/10.1145/2078827.2078841

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard law review*, 193-220.

Weber, R. H. (2015). The digital future - A challenge for privacy? *Computer Law and Security Review*, *31*(2), 234-242. https://doi.org/10.1016/j.clsr.2015.01.003

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business and Society*, *58*(1), 20-41. https://doi.org/10.1177/0007650317718185

Westin, A. F. (1967). Special report: Legal safeguards to insure privacy in a computer society. *Communications of the ACM*, *10*(9), 533–537. https://doi.org/10.1145/363566.363579

Wu, F., Wu, T., & Yuce, M. R. (2019). An internet-of-things (IoT) network system for connected safety and health monitoring applications. *Sensors, 19*(1), 21. https://doi.org/10.3390/s19010021

Xu, H., & Teo, H. (2004). Alleviating consumer's privacy concern in location-based services: A psychological control perspective. *Proceedings of the Twenty-Fifth International Conference on Information Systems,* 64.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *ICIS 2007 Proceedings - Twenty Eighth International Conference on Information Systems*, 125.

Yildirim, H., & Ali-Eldin, A. M. T. (2019). A model for predicting user intention to use wearable IoT devices at the workplace. *Journal of King Saud University - Computer and Information Sciences*, *31*(4), 497-505. https://doi.org/10.1016/j.jksuci.2018.03.001

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-20. https://doi.org/10.1145/3274469

Zhou, L., Wu, D., Chen, J., & Dong, Z. (2018). When computation hugs intelligence: Content-aware data processing for industrial IoT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2017.2785624

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *5*(3), 1657-1666. https://doi.org/10.1109/JIOT.2018.2847733

Zhou, W., & Piramuthu, S. (2015). Information Relevance Model of Customized Privacy for IoT. *Journal of Business Ethics*, *131*(1), 19-30. https://doi.org/10.1007/s10551-014-2248-y

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things:

Threats and challenges. *Security and Communication Networks*, *7*(12), 2728-2742. https://doi.org/10.1002/sec.795

Zuboff, S. (1988). Dilemmas of transformation in the age of the smart machine. In *In the Age of the Smart Machine: The Future of Work and Power,* 81.

Zuboff, S. (2019). *The Age of Surveillance Capitalism.* Profile Books.

DOI: 10.17185/duepublico/73580
URN: urn:nbn:de:hbz:464-20201218-100059-1