“I wonder how, I wonder why”: Supporting users in protecting their digital privacy by increasing risk awareness and knowledge as well as addressing protection obstacles

**Zur Erlangung des Grades eines Doktors der Naturwissenschaften (Dr. rer. nat.)
genehmigte Dissertation von Nina Gerber aus Langen
Tag der Einreichung: 21.10.2019, Tag der Prüfung: 03.03.2020
Darmstadt, Technische Universität Darmstadt**

**1. Gutachten: Prof. Dr. Joachim Vogt
2. Gutachten: Prof. Dr. Sarah Diefenbach**

TECHNISCHE
UNIVERSITÄT
DARMSTADT

**Forschungsgruppe für Arbeits- und Ingenieurpsychologie
Fachbereich Humanwissenschaften**

“I wonder how, I wonder why”: Supporting users in protecting their digital privacy by increasing risk awareness and knowledge as well as addressing protection obstacles

Genehmigte Dissertation von Nina Gerber aus Langen

1. Gutachten: Prof. Dr. Joachim Vogt
2. Gutachten: Prof. Dr. Sarah Diefenbach

Tag der Einreichung: 21.10.2019
Tag der Prüfung: 03.03.2020
Jahr der Veröffentlichung auf TUprints: 2020

Darmstadt, Technische Universität Darmstadt

Erklärung zur Dissertation

Die Dissertation ist von mir mit einem Verzeichnis aller benutzten Quellen versehen. Ich erkläre, dass ich die Arbeit – abgesehen von den in ihr ausdrücklich genannten Hilfen – selbstständig verfasst habe.

Darmstadt, den 21.10.2019

(Nina Gerber)

Abstract

This thesis aims to shed light on the so-called "privacy paradox", which refers to the dichotomy between people's attitude and behavior in the privacy context: Although people often express concerns about their privacy, they rarely take measures to protect their private data and frequently provide private information voluntarily, e.g., by using data-collecting technologies and services. Privacy researchers have investigated this phenomenon for several years, but no exhaustive explanation has been found so far. This thesis addresses this issue by (1) adding to the understanding of users' privacy attitude and behavior, and (2) investigating how users can be supported in their efforts to behave more privacy-friendly. To this aim, this thesis makes three main contributions:

First, I integrate prior research on the privacy paradox by identifying and combining theoretical explanation attempts and empirical findings based on a literature review. This holistic approach leads to new insights on the privacy paradox, and thus allow to gauge the validity of the various explanations that have been proposed for the privacy paradox. The literature review provides strong evidence for the privacy calculus model and the influence of social factors on privacy behavior. The results can further serve as a framework for researchers, who can build on the results to guide the direction of their research, e.g., by allowing them to investigate factors that have been found repeatedly to strongly influence the different facets of user privacy, exclude factors that have been found to be negligible, or choose an appropriate study design based on the sizes of the considered effects.

Second, I explore possibilities to assist users in their privacy protection attempts. Based on the literature review described above, I identify three factors that are important for users' decision to protect their privacy or share their private data, respectively: (1) awareness of privacy issues, (2) knowledge of and ability to use protection solutions, and (3) obstacles for privacy protection, such as benefits associated with data disclosure. I investigate these factors more thoroughly in a combination of qualitative and quantitative studies. Regarding (1), I find that most participants lack awareness of possible privacy risks. I conduct a literature review to identify appropriate risks that can be used for risk communication, e.g., in public risk awareness raising campaigns, exemplarily for the case of smart environments. The results can serve as a basis for activists and researchers who are conducting interventions aiming to raise privacy risk awareness. Regarding (2), I identify a lack of understanding in terms of privacy protection and the application of protection solutions. While I find that it seems to be a reasonable approach to design a dedicated solution for providing privacy knowledge instead of including information material in existing solutions, e.g., the app store, also additional motivational elements should be included in this solution to maximize users' motivation and eventually extend their privacy protection measures to various domains. I outline the development of such motivational elements based on a well-founded theoretical model and empirical findings. These results can inform the design of future privacy protection solutions. To address (3), the study results imply that protection solutions and privacy-friendly alternatives should be easy to use and understand, and should also be used by other people. Further, people use digital technologies and services to accomplish a multiplicity of goals, and strive to feel related, competent, autonomous, and stimulated. The extensive list of these goals presented in this thesis, including an assessment of importance for a broad range of technologies and services, can support product designers or designers of privacy interventions in deciding on product features. As usage motivation is found to be related to the deployment of privacy protection strategies, the results can also guide privacy researchers, e.g., when studying the privacy calculus model by serving as input for the privacy costs.

Third, I outline the development of a privacy protection solution. For this purpose, I describe the development and evaluation of a prototypical app that combines information on privacy topics, an analysis of the installed apps to increase privacy awareness, and gamification elements. I discuss how the findings described above can be considered in the design of this privacy protection solution. This solution can serve

as a base for the development of further interventions, as it is designed as a proof of concept and allows to easily integrate additional information content. Motivating users to gain information on the topic of digital privacy over a period of two weeks, the app can be utilized, e.g., in school classes as part of the curriculum to sensitize children and adolescents to privacy issues.

I hope that this thesis adds to the understanding of the ongoing discussion about the privacy paradox and informs future research by identifying which factors are important and which are negligible, respectively, for people's privacy attitude, intention, or behavior. I further aim to provide actual support for users who aim to better protect their privacy, by investigating factors that can contribute to protection solutions and thus inspiring the design of such solutions, as well as by proposing an own protection solution.

Zusammenfassung

Ziel dieser Dissertation ist es, das sogenannte “Privacy Paradox”, das die Diskrepanz zwischen Einstellung und Verhalten in Bezug auf die Privatsphäre beschreibt, näher zu beleuchten: Obwohl Nutzer häufig Bedenken in Bezug auf ihre Privatsphäre äußern, unternehmen sie selten Anstrengungen, ihre privaten Daten zu schützen und geben häufig Informationen freiwillig preis, z.B. indem sie Technologien und Dienste nutzen, die ihre Daten erfassen und speichern. Privatsphäre-Forscher beschäftigen sich bereits seit einigen Jahren mit diesem Phänomen, konnten allerdings bisher noch keine erschöpfende Erklärung finden. Diese Arbeit befasst sich mit diesem Thema, indem sie (1) zum Verständnis von Privatsphäreeinstellung und -verhalten beträgt und (2) untersucht, wie Nutzer in ihren Bemühungen für ein Privatsphäre-freundliches Verhalten unterstützt werden können. Hierfür leistet diese Arbeit drei primäre Beiträge:

Erstens integriert sie frühere Forschungen zum Privacy Paradox durch die Identifikation und Kombination theoretischer Erklärungsversuche und empirischer Erkenntnisse im Rahmen einer Literaturrecherche. Dieser holistische Ansatz liefert neue Erkenntnisse bzgl. des Privacy Paradox' und ermöglicht eine Einschätzung der Gültigkeit der verschiedenen Erklärungen, die bisher für das Privacy Paradox vorgestellt wurden. Die Ergebnisse der Literaturrecherche sprechen für das “Privacy Calculus”-Model und den Einfluss sozialer Faktoren auf das Privatsphäreverhalten. Des Weiteren können die Ergebnisse als Rahmenwerk für Forscher dienen, welche sich in der Ausrichtung ihrer Forschung an den Ergebnissen orientieren können, beispielsweise durch die Untersuchung von Faktoren, für die wiederholt ein starker Einfluss auf die verschiedenen Facetten der Privatpshäre gezeigt wurde, den Auschluss von Faktoren, die sich als vernachlässigbar erwiesen haben oder indem sie ein Studiendesign wählen, das die Stärke der untersuchten Effekte berücksichtigt.

Zweitens untersucht sie Möglichkeiten, Nutzer in ihren Bemühungen für ein Privatsphäre-freundliches Verhalten zu unterstützen. Basierend auf der oben beschriebenen Literaturrecherche werden drei Faktoren identifiziert, die für die Entscheidung der Nutzer, ihre Privatsphäre zu schützen bzw. ihre privaten Daten zu teilen, wichtig sind: (1) Bewusstsein von Privatsphärephäre-Risiken, (2) Wissen über und Fähigkeit zur Nutzung von Schutzlösungen und (3) Hindernisse für Datenschutz, wie z.B. erlangte Vorteile durch die Datenpreisgabe. Diese Faktoren werden mit einer Kombination von qualitativen und quantitativen Studien genauer betrachtet. In Bezug auf (1) zeigt sich, dass den meisten Studienteilnehmern das Bewusstsein für mögliche Privatsphärephäre-Risiken fehlt. Im Rahmen einer Literaturrecherche werden geeignete Risiken, die für die Risikokommunikation verwendet werden können, z.B. im Zuge von öffentlichen Kampagnen zur Erhöhung des Risikobewusstseins, exemplarisch für den Bereich “Smart Environments” identifiziert. Die Ergebnisse können als Grundlage für Aktivisten und Forscher dienen, die Maßnahmen zur Sensibilisierung für das Thema Privatsphäre ergreifen möchten. In Bezug auf (2) zeigt sich ein mangelndes Verständnis für Privatsphäreschutz und speziell die Anwendung von Schutzlösungen. Einerseits deuten die Ergebnisse darauf hin, dass die Entwicklung einer dedizierten Lösung für die Vermittlung von Wissen bzgl. Privatsphäre im Gegensatz zur Integration von Informationsmaterial in bereits bestehende Lösungen, wie beispielsweise den App Store, einen vielversprechenden Ansatz darstellt. Andererseits sollten zusätzliche motivationale Elemente in diese Lösung aufgenommen werden, um die Motivation der Nutzer zu maximieren, ihre Datenschutzmassnahmen auf verschiedene Anwendungsgebiete auszudehnen. Ich skizziere die Entwicklung solcher motivationalen Elemente auf Grundlage eines fundierten theoretischen Modells sowie empirischer Erkenntnisse. Die Ergebnisse können zur Entwicklung zukünftiger Lösungen für Privatsphäreschutz beitragen. In Bezug auf (3) deuten die Studienergebnisse darauf hin, dass Schutzlösungen und Privatsphäre-freundliche Alternativen leicht zu bedienen und zu verstehen sein, sowie auch von anderen Menschen genutzt werden sollten. Darüber hinaus nutzen Menschen digitale Technologien und Dienstleistungen, um eine Vielzahl von Zielen zu erreichen, und streben dabei danach, sich verbunden, kompetent, autonom und stimuliert zu fühlen. Die umfangreiche Liste dieser Ziele, die in dieser Arbeit vorgestellt wird,

einschließlich einer Bewertung ihrer Wichtigkeit für ein breites Spektrum von Technologien und Dienstleistungen, kann Produktdesigner oder Designer von Interventionen bei der Wahl von Produkteigenschaften unterstützen. Da die Nutzungsmotivation außerdem mit der Anwendung von Schutzstrategien für die Privatsphäre zusammenhängt, können die Ergebnisse zudem Datenschutzforscher leiten, z.B. bei der Untersuchung des "Privacy Calculus"-Modells, indem sie dort als Input für die Kosten von Privatsphäreschutz dienen.

Drittens wird die Entwicklung einer Datenschutzlösung beschrieben. Hierfür wird die Entwicklung und Evaluation einer prototypischen App vorgestellt, welche Informationen zu Themen rund um Privatsphäreschutz, eine Analyse der installierten Apps zur Steigerung des Privatsphäre-Bewusstseins sowie Gamification-Elemente kombiniert. Es wird diskutiert, wie die oben beschriebenen Erkenntnisse bei der Gestaltung dieser Datenschutzlösung berücksichtigt werden können. Diese Lösung kann als Grundlage für die Entwicklung weiterer Maßnahmen dienen, da sie als "Proof of Concept" konzipiert ist und es ermöglicht, zusätzliche Informationsinhalte einfach zu integrieren. Die App motiviert Nutzer, sich über einen Zeitraum von zwei Wochen über das Thema Schutz der digitalen Privatsphäre zu informieren und kann beispielsweise in Schulklassen im Rahmen des Lehrplans eingesetzt werden, um Kinder und Jugendliche für Datenschutzfragen zu sensibilisieren.

Ich hoffe, dass diese Arbeit zum Verständnis der laufenden Diskussion um das Privacy Paradox beiträgt und zukünftige Forschung unterstützt, indem sie untersucht, welche Faktoren wichtig und welche vernachlässigbar für die Privatsphäreeinstellung, -intention oder -verhalten sind. Darüber hinaus möchte ich Nutzer, die ihre Privatsphäre besser schützen möchten, konkret unterstützen, indem ich Faktoren untersuche, die zur Nutzung von Schutzlösungen beitragen können und so die Entwicklung solcher Lösungen anregen, sowie eine eigene Schutzlösung vorschlagen.

Contents

1 Introduction **1**
- 1.1 Goals and Research Questions . . . 1
  - 1.1.1 Goal 1: Identify explanation approaches for the privacy paradox . . . 1
  - 1.1.2 Goal 2: Understand factors that are important for users' decision to protect their digital privacy . . . 2
  - 1.1.3 Goal 3: Investigate how users' awareness of privacy issues can be increased . . . 2
  - 1.1.4 Goal 4: Increase users' privacy protection knowledge and ability . . . 2
  - 1.1.5 Goal 5: Identify reasons for users to keep using privacy- threatening technologies and investigate implications for privacy protection . . . 3
- 1.2 Methodological Approach . . . 4
- 1.3 Structure and Publications . . . 5

2 Explanation Approaches for the Privacy Paradox **6**
- 2.1 Methodology . . . 6
  - 2.1.1 Literature Search . . . 6
  - 2.1.2 Inclusion of Study Results . . . 7
  - 2.1.3 Quality Assessment . . . 8
- 2.2 Theoretical Privacy Paradox Explanation Attempts . . . 8
  - 2.2.1 Privacy Calculus . . . 8
  - 2.2.2 Bounded Rationality & Decision Biases . . . 8
  - 2.2.3 Lack of Personal Experience and Protection Knowledge . . . 9
  - 2.2.4 Social Influence . . . 9
  - 2.2.5 The Risk and Trust Model . . . 10
  - 2.2.6 Quantum Theory . . . 10
  - 2.2.7 Illusion of Control . . . 10
  - 2.2.8 The Privacy Paradox as Methodological Artefact . . . 10
- 2.3 Empirical Privacy Paradox Explanation Attempts . . . 11
  - 2.3.1 Privacy Attitude, Privacy Concerns and Perceived Privacy Risk . . . 11
  - 2.3.2 Privacy Related Behavioral Intention and Willingness . . . 15
  - 2.3.3 Privacy Related Behavior . . . 20
- 2.4 Discussion . . . 26
  - 2.4.1 Main Predictors of Privacy Attitude, Concerns, Perceived Risk, Behavioral Intention and Behavior . . . 27
  - 2.4.2 Predictor Variables for Future Studies . . . 33
  - 2.4.3 Theoretical Implications of the Empirical Study Results . . . 42
  - 2.4.4 Limitations . . . 43
  - 2.4.5 Conclusion . . . 44

3 Factors That are Important for Users' Decision to Protect Their Digital Privacy **45**
- 3.1 Related Work . . . 45
  - 3.1.1 Mental Models of Privacy Consequences . . . 45
  - 3.1.2 Strategies for Protecting One's Privacy . . . 46
  - 3.1.3 Obstacles for Privacy Protection . . . 46
- 3.2 Methodology . . . 47
  - 3.2.1 Research Questions . . . 47
  - 3.2.2 Recruitment and Participants . . . 48
  - 3.2.3 Study Procedure . . . 48
  - 3.2.4 Evaluation Methodology . . . 49

3.2.5 Ethical Considerations . . . 49
3.3 Results . . . 49
3.3.1 Mental Model of Privacy Consequences . . . 49
3.3.2 Protection Strategies . . . 51
3.3.3 Protection Obstacles . . . 52
3.3.4 Common Privacy (Mis)conceptions . . . 53
3.4 Discussion . . . 53
3.4.1 Mental Models of Privacy Consequences . . . 53
3.4.2 Strategies for Protecting One's Privacy . . . 53
3.4.3 Obstacles for Privacy Protection . . . 54
3.4.4 Limitations . . . 54

4 Awareness of Privacy Issues 55
4.1 Identification of Privacy Consequences Associated with Living in Smart Environments . . . 56
4.2 Conclusion . . . 59

5 Privacy Protection Knowledge and Ability 60
5.1 Related Work . . . 60
5.1.1 Smartphone App Permissions . . . 60
5.1.2 Privacy Awareness . . . 61
5.1.3 Privacy Education . . . 62
5.2 The FoxIT App . . . 63
5.2.1 Analysis of Smartphone Settings and App Permissions . . . 63
5.2.2 Privacy lessons . . . 64
5.2.3 Gamification Elements . . . 65
5.3 Field Study . . . 66
5.3.1 Research Questions . . . 66
5.3.2 Recruitment and Participants . . . 66
5.3.3 Study Procedure . . . 67
5.3.4 Questionnaires . . . 67
5.3.5 Ethical Considerations . . . 68
5.3.6 Results . . . 68
5.4 Discussion . . . 69
5.4.1 Limitations . . . 70
5.4.2 Implications . . . 70
5.5 Motivational Elements . . . 71
5.5.1 Ideas for Implementation . . . 73
5.6 Conclusion . . . 74

6 Reasons for Using Privacy-Threatening Technologies and Implications for Privacy Protection 75
6.1 Theoretical Background . . . 75
6.2 Identification of Do-goals and Be-goals – Quantitative Approach . . . 75
6.2.1 Study I . . . 76
6.2.2 Study II . . . 80
6.3 Identification of Do-goals and Be-goals – Qualitative Approach . . . 82
6.3.1 Methodology . . . 91
6.3.2 Results . . . 92
6.3.3 Limitations . . . 93

6.4 Relationship between Needs and Privacy Protection Behavior on Facebook . . . 94
6.4.1 Related Work . . . 94
6.4.2 Methodology . . . 95
6.4.3 Results . . . 98
6.4.4 Discussion . . . 98
6.5 Conclusion . . . 100

7 Discussion **101**
7.1 Goal 1: Identify explanation approaches for the privacy paradox . . . 101
7.1.1 Contribution . . . 102
7.2 Goal 2: Understand factors that are important for users' decision to protect their digital privacy . . . 102
7.2.1 Contribution . . . 103
7.3 Goal 3: Investigate how users' awareness of privacy issues can be increased . . . 103
7.3.1 Contribution . . . 104
7.4 Goal 4: Increase users' privacy protection knowledge and ability . . . 104
7.4.1 Contribution . . . 105
7.5 Goal 5: Identify reasons for users to keep using privacy-threatening technologies and investigate implications for privacy protection . . . 105
7.5.1 Contribution . . . 106
7.6 Limitations . . . 106
7.7 Influence of Culture . . . 107
7.8 Conclusion and Future Work . . . 108

Literature **130**

1 Introduction

Nowadays, digitization is regularly treated as a panacea for numerous issues [42]. However, the spread of digital devices and services, particularly in the area of the "Internet of things" (IoT) [1], also implies the omnipresence of data capturing technologies. Hence, it is not surprising that the majority of users considers the privacy of their data to be an important topic. According to recent surveys, 78% of European Internet users think that "it is very important that personal information on their computer, smartphone or tablet can only be accessed with their permission" [58], and 90% of US-American users state that "controlling what information is collected about them is important" [79]. Yet, more than half of the users, not only in Europe and the US, but also in Africa, Latin America, and the Asian-Pacific states, think that the Internet is eroding their privacy and more than 60% worry about how their personal data is being used by companies [40].

Despite these expressed concerns, users have been found repeatedly to refrain from taking measures to protect their digital privacy and often even give their data away voluntarily for small benefits (e.g., [219, 18]). This dichotomy between expressed attitude and actual behavior is referred to as "privacy paradox" and has gained considerable attention among privacy researchers in the last decade [119, 167, 208, 8, 35]. Popular explanations for this paradoxical behavior include a rational cost-benefit analysis that leads to the decision to share private data in many cases [128, 109, 121, 135, 234, 56], the sharing of private data due to social influence [220, 32, 90, 72, 99], the affection of privacy decisions by cognitive biases and heuristics, as well as bounded rationality [9, 118, 72, 53, 6, 36, 44], and the application of quantum theory, which states that the outcome of a decision is not determined until the actual decision is made and thus surveys asking users about their desired behavior are not reliable [72].

Kokolakis [119] thus concludes that due to the variety of possible explanations, the privacy paradox should not be considered a paradox anymore. Still, he argues that it remains a complex phenomenon that has not been fully explained yet and calls for further research to understand the "whole picture". The present thesis thus aims to shed more light on this issue and contribute to the understanding of why users often behave in a privacy-unfriendly way despite their privacy concerns. In line with Kokolakis [119], I thereby assume that the dichotomy between attitude and behavior should not be considered a paradox, but arises from the complexity of privacy decisions, which are subject to the influence of various factors. Users pursue a multiplicity of goals when using digital services and devices, with privacy being only one of many factors that need to be considered. Furthermore, situational elements like social interactions affect the users' eventual behavior and frequently hamper privacy protection attempts. Since users express a strong desire to protect their privacy (at least to a certain degree) when only asked about this particular factor, I understand that users need to be supported in their efforts for privacy protection. The second aim of this thesis therefore is to investigate how users can be supported in protecting their privacy and to outline concrete solutions for this objective.

1.1 Goals and Research Questions

This section describes the goals of the present thesis and the according research questions I aim to answer in order to reach the respective goals. I start with reviewing the existing literature to ground this thesis in prior work and to identify promising directions for further research. The subsequent goals and research questions follow from the respective findings and answers to earlier research questions.

1.1.1 Goal 1: Identify explanation approaches for the privacy paradox

The present thesis aims to contribute to the understanding of people's privacy attitude and behavior in the digital context, which frequently diverge. This phenomenon has been referred to as "privacy paradox" in the literature [119, 167, 208, 8, 35].

For this purpose, I conduct a literature review to identify theoretical and empirical explanation attempts for the privacy paradox that have been suggested in the literature. Hence, I propose the following research questions for this review, with the answers indicating the direction for further goals and the respective

research questions:

RQ1a: Which theoretical explanations have been proposed for the privacy paradox?

RQ1b: Which factors influence users' privacy attitude and behavior?[1]

1.1.2 Goal 2: Understand factors that are important for users' decision to protect their digital privacy

Based on the literature review, I find that awareness of privacy issues, knowledge of and ability to use protection solutions, and obstacles for privacy protection, such as benefits associated with data disclosure, are among the most important factors that determine if users decide to protect their digital privacy (RQ1b). In order to understand these factors more thoroughly, I conduct a qualitative interview study with 24 German lay users to answer the following research questions:

RQ2a: What are people's mental models of possible consequences arising from sharing and not protecting their private data?

RQ3a: What strategies do people apply to protect their data?

RQ4a: What are obstacles for privacy protection and for what reasons do people still use privacy-threatening devices and services?

1.1.3 Goal 3: Investigate how users' awareness of privacy issues can be increased

The interview results show that while most participants name personalized advertisement as a possible consequence of not protecting one's privacy and about half of the participants also fear financial losses, most participants lack awareness of further possible privacy consequences (RQ2a).
I conclude that users need to be informed about this topic and thus identified, based on the literature, an approach to raise people's risk awareness. The results indicate that whereas abstract privacy risks, e.g., referring to possible harm, are considered to be rather likely, whereas privacy risks describing concrete consequences are considered to be more severe. I thus conclude that it could be a promising approach to combine a set of concrete consequences to increase users' perception of how likely (at least one of) these consequences will apply. In order to identify such a set of consequences, I conduct a literature review to answer the following research question:

RQ2b: What are possible privacy consequences that could result from living in smart environments?

1.1.4 Goal 4: Increase users' privacy protection knowledge and ability

Regarding privacy protection strategies (RQ3a), the interview results indicate that although several participants apply protection strategies, there is a general lack of understanding of protection solutions, particularly with regard to privacy enhancing technologies (PETs). I thus outline the development of an easy to use app that further enhances users' privacy knowledge. A first concept of this app is evaluated in a field study with 31 lay users to investigate the app's potential to increase privacy knowledge, awareness, and behavior by answering the following research questions:

RQ3b: Does using the app lead to an increase in knowledge about privacy related topics?

[1] As these constructs might be affected by different variables, thereby causing the dichotomy between users' privacy attitude and actual behavior.

RQ3c: Does using the app lead to a change in privacy awareness?

RQ3d: Does using the app lead to a change in privacy behavior, that is, do participants...
...improve the privacy conditions on their smartphone?
...increase their use of security measures?
...deploy stricter privacy settings on social network sites?
...actively inform themselves about privacy?
...prompt others to protect their data?

The field study results suggest that the improvement of users' privacy through a dedicated knowledge enhancing application seems to be a promising approach. However, the app succeeds in enhancing participants' mobile privacy (which is facilitated by the app), but fails to also enhance their privacy settings in other domains. Hence, I conclude that additional motivational elements need to be included to also prompt privacy enhancing actions in other domains. I rely on the Persuasive Systems Design Model [169] for the development of these motivational elements, a theoretical framework for the design of persuasive technologies, i.e., technologies that support users in changing their behavior in a particular domain.

1.1.5 Goal 5: Identify reasons for users to keep using privacy- threatening technologies and investigate implications for privacy protection

Regarding the obstacles for privacy protection as well as reasons for still using privacy- threatening devices and services (RQ4a), the results of the interview study suggest that protection solutions should be easy to use and understand, which also applies to privacy-friendly alternatives, while the latter should also be used by other people. Participants still report to use privacy-threatening devices and services in order to reach other people, participate in their life, or share their opinion with others, as well as out of convenience. However, as the participants of the interview study frequently refer to social networks and messengers, and the sample considered in the interview study is rather small, I conduct two additional survey studies with 217 and 246 participants, respectively, as well as a consecutive interview study to validate and extend the results by answering the following research questions quantitatively and qualitatively:

RQ4b: What do users want to accomplish[2] by using potentially privacy-threatening devices and services, i.e., Online Social Networks (OSN), messengers, cloud services, digital assistants, game consoles, smart TVs, E-Commerce applications, as well as participating in customer loyalty programs and market research studies?

RQ4c: What do users want to feel like[3] by using potentially privacy-threatening devices and services, i.e., Online Social Networks (OSN), messengers, cloud services, digital assistants, game consoles, smart TVs, E-Commerce applications, as well as participating in customer loyalty programs and market research studies?

I find that users pursue a multiplicity of do-goals when using the considered technologies, but mainly strive to feel related, competent, autonomous, and stimulated when using these technologies. To further investigate whether the actual be-goals that users pursue relate to the application of protection strategies, I conduct a survey study with 280 Facebook users to answer this question exemplarily for the case of the most popular OSN:

RQ4d: Do Facebook users with strict and those with lax privacy settings differ pertaining to the needs/be-goals that motivate them to use Facebook (i.e., (a) autonomy, (b) competence, (c) related-

[2] The so-called "do-goals" [95].
[3] The so-called "be-goals" [95].

ness, (d) meaningfulness, (e) pleasure-stimulation, (f) security and (g) popularity-influence)?

RQ2de: Do Facebook users who deploy certain privacy protection strategies besides the management of privacy settings and those who do not differ pertaining to the needs/be-goals that motivate them to use Facebook (i.e., (a) autonomy, (b) competence, (c) relatedness, (d) meaningfulness, (e) pleasure-stimulation, (f) security and (g) popularity-influence)?

I find that Facebook users with rather lax privacy settings have a greater feeling of being meaningful and stimulated when using Facebook than users with rather strict privacy settings, while the needs/be-goals pursued and the deployment of other protection strategies do not seem to be related.

1.2 Methodological Approach

I apply a multidimensional approach to look at the topic (i.e., understand users' privacy behavior and investigate how they can be supported in protecting their privacy) from different angles (see table 1). I start with analyzing the existing literature to gain new insights through the combination of findings and to identify directions for further research (RQ1a, RQ1b).

I then conduct qualitative interviews to gain a deeper understanding of three factors that have been found to influence a user's decision for or against privacy protection in the quantitative studies considered in the literature review (RQ2a, RQ3a, RQ4a). Based on the findings, I choose to investigate particular aspects of these three factors in more detail.

Privacy risk perception (RQ2b) was first studied in a large-scale online study with a 9x3-between-subject design described in Gerber et al. [83] to cover a broader range of application areas and risk scenarios. A between-subject design was applied to study individual perception of different privacy risks and account for position and learning effects. The online design offers the possibility to investigate the perceptions of a large, reasonably diverse sample of participants. The results indicate that a combination of concrete consequences should be used for risk communication aiming to increase privacy risk awareness, and, since no comprehensive list of such consequences is available yet, I identify such a set for the use case of smart environments in a literature review.

Based on theoretical considerations, I suggest to develop a dedicated intervention to enhance users' privacy knowledge, as they need to be motivated to learn about this topic at the time they receive the respective information. To test whether this approach is feasible, I describe the prototypical development and evaluation of this intervention in a two-week field study (RQ3b, RQ3c, RQ3d). Since the intervention should enhance privacy knowledge (and, consequently, awareness and behavior) in the long run, a retention period of one week is included to test for such long-term effects. The field study design allows to realistically investigate the intervention concept in a user's everyday life and also provides the opportunity to identify possible pitfalls, e.g., usability problems. The evaluation results indicate that additional motivational elements should be included. For this purpose I draw on an established framework for the design of such elements and on empirical results from meta-analyses to make a sound decision on what elements should be included.

The reasons for users to still use privacy-threatening technologies and services (RQ4b, RQ4c) are investigated in a combination of qualitative and quantitative online studies, as well as a qualitative interview study including a card sorting task. The qualitative online study allows to identify categories of usage goals for a larger sample than had been possible to investigate in a lab or interview study. I choose a data-driven approach for the identification of do-goals as these are highly dependent on the usage context, i.e., the technology or service considered, and no extensive theory or model has been proposed yet to describe such do-goals. Be-goals, on the other hand, have been studied several times in earlier research, which lead to the identification of a set of important psychological needs or be-goals. Hence, I rely on this concept and proceed with conducting a quantitative online study to investigate the importance of those be-goals as well as the do-goals identified in the first study. Again, the online design allows to consider a larger sample of

Table 1: Overview of the different methodologies applied in this thesis.

Goal	RQ	Method
1	RQ1a, RQ1b	Literature review (N=181)
2	RQ2a, RQ3a, RQ4a	Qualitative interviews (N=24)
3	RQ2b	Literature review (N=29)
4	RQ3b, RQ3c, RQ3d	Prototype design and evaluation in a field study (N=31), Theory-based concept development
5	RQ4b, RQ4c	Qualitative online study (N=217), Quantitative online study (N=246), Qualitative interviews and card sorting task (N=17)
	RQ4d, RQ4e	Quantitative online study (N=280)

participants, which increases the generalizability of the results. Nonetheless, an additional interview study including a card sorting task is conducted in order to validate the results qualitatively.
Finally, I investigate the relationship between the deployment of privacy protection strategies and be-goals associated with the use of Facebook in a quantitative online study (RQ4d, RQ4e). This time, the online design not only allows to investigate a larger set of Facebook users to allow me to conduct regression models, it also aims to create an environment in which participants can honestly reflect on their deployment of privacy protection strategies, without prompting them towards privacy protection due to effects of social desirability, as might have been the case in interview or lab studies.

1.3 Structure and Publications

The remainder of the thesis is structured as follows:
Chapter 2 describes the literature review that I conducted to identify explanation approaches for the privacy paradox (goal 1). This chapter is based on the paper *"Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. In: Computers & Security 77 (2018), pp. 226–261."* [81].
Chapter 3 describes the interview study with 24 lay users that I conducted to further understand the important factors for users' decision to protect their digital privacy (goal 2). This chapter is based on the paper *"Nina Gerber, Verena Zimmermann, and Melanie Volkamer. Why Johnny Fails to Protect his Privacy. In: Proceedings of the 4th European Workshop on Usable Security (EuroUSEC). IEEE, 2019."* [84].
Chapter 4 focuses on how users' awareness of privacy issues can be increased (goal 3).
Chapter 5 describes the development of the prototype for an app that aims to increase privacy protection knowledge and ability (goal 4). This chapter is based in part on the paper *"Nina Gerber et al. FoxIT: Enhancing Mobile Users' Privacy Behavior by Increasing Knowledge and Awareness. In: Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST). ACM, 2018, pp. 53–63."* [85] (section 5.1, section 5.2, section 5.3, section 5.4).
Chapter 6 presents a set of studies that I conducted in order to identify the reasons users keep using privacy-threatening technologies for and investigate implications for privacy protection (goal 5). This chapter is based in part on the papers *"Sina Zimmermann and Nina Gerber. Why Do People Use Digital Applications? A Qualitative Analysis of Usage Goals and Psychological Need Fulfillment. In: i-com 18.3 (2019), pp. 271–285.* [263] (section 6.3) and *"Nina Gerber, Paul Gerber, and Maria Hernando. Sharing the 'Real Me' – How Usage Motivation and Personality Relate to Privacy Protection Behavior on Facebook. In: Human Aspects of Information Security, Privacy and Trust. Ed. by Theo Tryfonas. Cham: Springer International Publishing, 2017, pp. 640–655."* [80] (section 6.4).
Finally, I discuss the findings and conclude in chapter 7.

2 Explanation Approaches for the Privacy Paradox[5]

Research has shown that although users express concerns about their privacy, they often fail to successfully protect their private data and often provide it voluntarily to organizations or other users. Albeit being subject to many studies, no definite explanation for this phenomenon, often referred to as "privacy paradox", has been found so far. This chapter therefore aims to shed light on the privacy paradox by summarizing the most popular theoretical privacy paradox explanations and taking a closer look at the factors that have been shown to significantly relate to user privacy. Based on a literature review for the search term "privacy paradox", I tried to identify all factors that significantly predict privacy attitude and privacy behavior. Therefore, I first collected all articles that contain study results from either regression analyses or structural equation models dealing with the relationship of various predictor variables with at least one of the two privacy aspects. Although privacy attitude originally refers to the general appraisal of different privacy behaviors, it is often operationalized as the assessment of privacy concerns or perceived risk, respectively. I will therefore consider all three approaches. Since many studies focus on the behavioral intention instead of the actual behavior, I decided to include this topic as well. I report the standardized effect size (β) that could be found in the included studies concerning the association of the different predictor variables with one of the privacy concepts.
The remainder of this chapter is organized as follows: In section 2.1, the methodological procedure is described, section 2.2 summarizes the most popular theoretical explanation attempts for the privacy paradox, section 2.3 focuses on the empirical explanation attempts for the privacy paradox (i.e., the standardized effect sizes for all identified predictor variables are reported) and section 2.4 provides a detailed discussion of the results, including the implications the empirical study results hold for the theoretical privacy paradox explanation attempts.
In the following, I will liberally use quotations from my systematic review article published in "Computers & Security" (2018) without explicitly marking each quote.

2.1 Methodology

I first conducted a literature search, resulting in a primary list of 181 articles dealing with the privacy paradox. Based on these articles, I identified the most popular theoretical explanation attempts for the privacy paradox. To identify the factors that are most appropriate for the prediction of privacy attitude, concerns, perceived risk, behavioral intention and behavior, I then excluded all articles that a) provide empirical evidence only based on the opinion of experts, b) do not describe quantitative user studies and c) do not contain study results from regression analyses or structural equation modeling dealing with the relationship of various variables with at least one of the above mentioned privacy aspects. I further rated the quality of the included studies, but did not exclude any article or study based on its quality rating. The methodological procedure is displayed in fig. 1.

2.1.1 Literature Search

I used the keyword "privacy paradox" to search for publications dealing with this topic in the databases Google Scholar, ACM Digital Library, IEEE Xplore Digital Library and Scopus. The search process took place between November 2015 and February 2016. I excluded papers which were not published in English or before 2006, since technological solutions affecting privacy in the daily life of users like Smartphones or the Internet of Things have been evolving rapidly in the last ten years. Therefore, empirical results that are obtained before 2006 may be based on different understandings of digital privacy and, as a consequence, differ systematically from newer findings.
The preliminary list included 181 articles dealing with the privacy paradox. I identified eight theoretical explanation attempts for the privacy paradox which were referred to in at least two articles. These are

[5] based on the paper "Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. In: Computers & Security 77 (2018), pp. 226–261." [81]

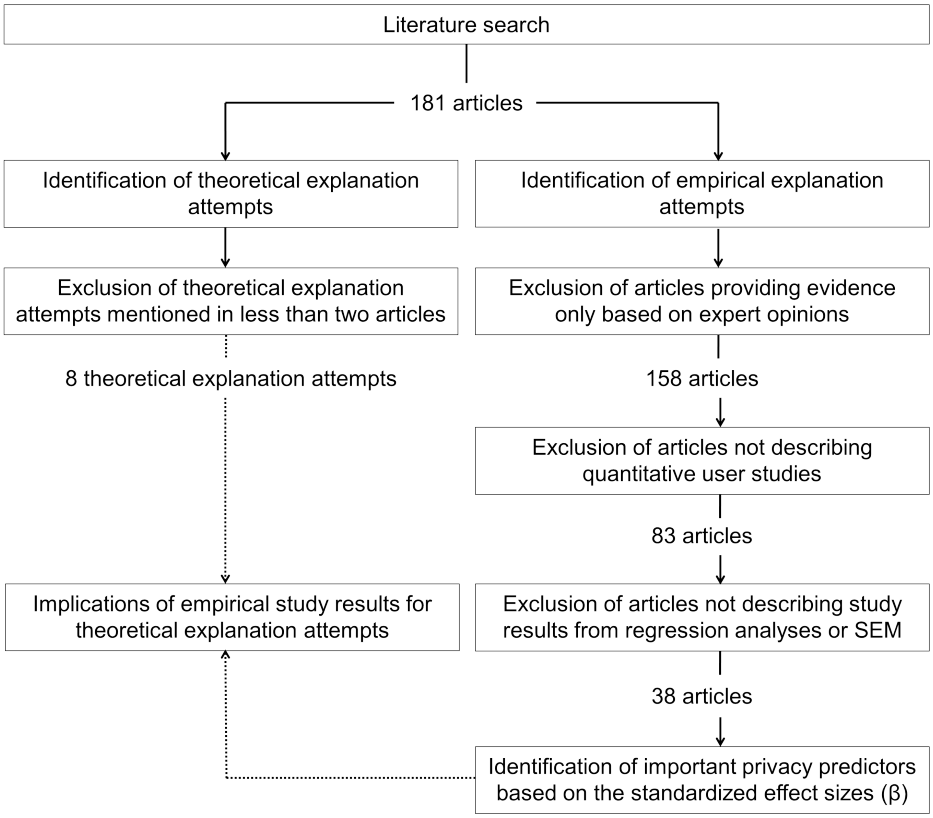

Figure 1: Graphical depiction of the review procedure.

summarized in section 2.2. Of the 181 included articles, 53 dealt with the privacy behavior of users (41 assessed data disclosure behavior, 30 data protection behavior). The behavioral intention was examined in 39 articles, whereas privacy attitude was assessed in 12, privacy concerns in 47 and perceived privacy risk in 20 articles.

2.1.2 Inclusion of Study Results

I decided about the inclusion of study results in the further evaluation based on the guidelines for performing a systematic literature review in the area of software engineering by Kitchenham [115]. She distinguishes between five different levels of evidence drawn from empirical studies, based on the particular study design: Level 1 includes randomized controlled trials and level 2 pseudo-randomized controlled trails (i.e., the allocation to the treatment is not random) and level 5 the assessment of expert opinions based on theory or consensus. No study design can definitely be assigned to level 3 and 4, however, there are several study designs that can be assigned to more than one level, namely randomized experiments that are performed in an artificial setting (level 1-4), comparative studies with non-randomized concurrent controls and allocation, cohort studies, case-control studies or interrupted time series with a control group (level 1-3), comparative studies with historical control, two or more single arm studies, or interrupted time series without a parallel control group (level 2-3), post-test or pre-test/post-test case series (level 2-4) and quasi-randomized experiments that are performed in an artificial setting (level 3-4). I included only studies offering evidence on level 1 to 4, i.e., studies which results are based on the opinion of experts were excluded. This is in line with the suggested procedure by Kitchenham [115] to accept all levels of evidence, except for level 5, which can be excluded if there are a reasonable number of studies that can be assigned to level 1 to 4. A total of 23 articles were excluded in this step, leaving 158 articles.
Of these 158 articles, 83 contained results from quantitative user studies. The other 75 articles, describing qualitative studies (e.g., semi-structured or unstructured interviews) or studies in which no data from users was assessed (e.g., mere mathematical evaluations of technical solutions), were also excluded.

Thirty-eight of the remaining 83 articles contained study results from either regression analyses or structural equation models dealing with the relationship of various variables with at least one of the above mentioned privacy aspects: attitude, concerns, perceived risk, behavior and behavioral intention. These 38 articles constitute the final set of articles included in the present review. A majority of the included studies (31) is published in journals; however, six of the studies are published in conference proceedings.

2.1.3 Quality Assessment

I assessed the methodological quality of the included studies according to the quality attributes for survey research proposed by Malhotra and Grover [155], as except for one, all of the included studies rely on questionnaire-based surveys. The fourth criterion ("Is any form of triangulation used to cross validate results?") was considered as irrelevant for survey studies and therefore excluded. I evaluated the fulfillment of the quality criterions based on the original definitions and on the further detailing developed by Sommestad et al. [209]. Each study was rated independently by three reviewers. Differences in the rating were solved afterwards through group discussion. Although I did not exclude any study on the basis of its quality rating, the reader is invited to evaluate the presented results with respect to the according study quality. The results of the quality assessment and the quality criterions can both be found in Appendix A. I also conducted power analyses for the included studies, using GPower [64] for the regression and the PLS-based SEM analyses and Free Statistics Calculators [210] for the covariance-based SEM analyses. Since none of the included studies fails to achieve sufficient power ($\geq$.8), I did not exclude studies based on their lack of statistical power.
The results are presented in the next two sections, starting with a summary of the eight most popular privacy explanation attempts (section 2.2), followed by the empirical study results concerning the relationship of different predictor variables and privacy attitude, privacy concern, perceived privacy risk, privacy intention and privacy behavior (section 2.3).

2.2 Theoretical Privacy Paradox Explanation Attempts

The following section describes the most popular explanations for the privacy paradox that have been proposed so far. A prior review of possible explanation approaches can be found in Kokolakis [119].

2.2.1 Privacy Calculus

One of the most-established explanations for the privacy paradox is based on the theoretical concept of the "homo oeconomicus". In the economic sciences, the term "homo oeconomicus" refers to the prototype of an economic human, a consumer whose decisions and actions are all driven by the attempt to maximize his/her benefits [184, 72]. If this concept is applied to the privacy context, a user is expected to trade the benefits that could be earned by data disclosure off against the costs that could arise from revealing his/her data [128]. Typical benefits of sharing personal data include financial discounts (e.g., by participating in consumer loyalty programs), increased convenience (e.g., by keeping credit card data stored with an online retailer) or improvement of socialization (e.g., by using social networks and messengers) [233, 242]. Data sharing costs, on the other hand, are less tangible and include all sorts of risk and negative consequences for disclosing personal data (e.g., security impairments, identity theft, unintended third-party usage, or social criticism and humiliation) [236]. According to the privacy calculus model, if the anticipated benefits of data sharing exceed the costs, a user is expected to willingly give his/her data away [128]. Nevertheless, s/he can still express concerns about the loss of his/her data, leading to the observed discrepancy between the expressed concerns or attitude and the actual behavior.

2.2.2 Bounded Rationality & Decision Biases

The recently described privacy calculus model postulates the existence of a rational user, who performs reasoned trade-off analyses for the decision to share (or protect) his/her data. However, numerous studies

on consumer decision behavior have shown that the decision making process is affected by various cognitive biases and heuristics [9, 118]. For example, it is unlikely that every consumer accesses exhaustive information concerning all possible costs and benefits when making a data sharing decision (on the contrary, consumers are often not even aware that their data is being collected [232]). Hence, their decision is based on incomplete information, which can lead to the over- or underestimation of the costs and benefits and might therefore seem irrational to an external observer, but at the same time fairly rational to the decision maker [72]. Furthermore, the human ability for cognitive processing is limited to a certain degree, which means even if a consumer has access to all necessary information, s/he might lack the ability to process all this information correctly and make an informed decision [53]. In the literature, this effect is often referred to as bounded rationality [72, 118]. The resulting imperfect decisions often suffer from cognitive biases, because the decision maker employs certain heuristics to compensate for his/her bounded rationality [119, 219, 232, 255, 228]. Hence, the resulting behavior might not reflect the original intention or the expressed attitude towards that behavior. Popular examples for these cognitive biases are:

- The availability bias: People tend to overestimate the probability of events they can easily recall, e.g., because they are very present in the media [197].
- The optimism bias: People tend to believe that they are at less risk of experiencing a negative privacy event compared to others [44].
- The confirmation bias: People tend to search for or interpret information in a way that confirms their beliefs and assumptions [175].
- The affect bias: People judge quickly based on their affective impressions, thereby underestimating the risks of things they like and overestimating the risks of things they dislike [207].
- The immediate gratification bias, sometimes also referred to as hyperbolic discounting: People tend to value present benefits or risks more than those that lie in the future [6].
- The valence effect: People tend to overestimate the likelihood of favorable events [68].
- The framing effect: People respond differently dependent on the way a question is framed or information is presented [229].
- The phenomenon of rational ignorance: People ignore the potential costs of data sharing because the costs for learning them, e.g., by reading the privacy policies, would be higher than the expected benefits from sharing the data [59].

2.2.3 Lack of Personal Experience and Protection Knowledge

Another explanation accounts for the fact that few users have actually suffered from online privacy invasions. As a consequence, most privacy attitudes are based on heuristics or secondhand experiences. However, only personal experiences can form an attitude that is stable enough to significantly influence the corresponding behavior [57]. In addition to the resulting weak association between attitude and behavior, some users might simply lack the ability to protect their data, because they have no or only limited knowledge of technical solutions like the deletion of cookies, the encryption of e-mails or the anonymization of communication data, e.g., by using the Tor software [20].

2.2.4 Social Influence

Most people are not autonomous in their decision to accept or reject the usage of a messaging application, a social network or e-mail encryption software, respectively. It is rather assumed that the social environment of an individual significantly influences his/her privacy decisions and behavior [220]. Especially in collectivistic cultures, where individuals possess a strong “we” consciousness, do users obey to social

norms [32]. But social influence does also occur in individualistic cultures, for instance when teenagers align to the example of their parents when it comes to data sharing in social networks [90]. In both kinds of culture include individuals usually at least to some extend the (supposed) opinion and behavior of their peers and/or family in their decision to use a specific technology or reveal their data. If significant others tend to self-disclose personal information, e.g., on social networks, some kind of social pressure can occur, eventually build on an idea of reciprocity, i.e., "if they disclose data it would be unfair not to do the same" [72]. Sometimes, the decision not to share personal data can even become a social stigma, for anyone who refuses to disclose his/her habits, actions and attitudes "must have something terrible to hide" [99]. Hence, actual behavior is most likely affected by social factors, whereas the expressed attitude supposedly reflects the unbiased opinion of the respective individual.

2.2.5 The Risk and Trust Model

It is most likely that the perceived risk of data-disclosing, as well as the trustworthiness of the recipient affects the data sharing attitude and behavior of an individual. Some authors explain the privacy paradox by assuming that trust has a direct influence on privacy behavior, whereas the perceived risk influences the reported attitude and behavioral intention. Still this influence is not strong enough to affect the actual behavior [167]. Trust, which is an environmental factor, has a stronger effect in concrete decision situations (i.e., behavior). The perceived risk, on the other hand, dominates in abstract decision situations, for example when a user is asked if s/he would be willing to share his/her data in a hypothetical situation [72], thereby producing the dichotomy between the reported attitude and the actual behavior.

2.2.6 Quantum Theory

Relying on quantum theory, Flender and Müller [72] propose another explanation for the privacy paradox. If human decision-making underlies the same effects as the measurement process in quantum experiments, we can assume that the outcome of a decision process is not determined until the actual decision is made [119] and two decisions are not interchangeable in terms of decision making [72]. Hence, if an individual is asked about a potential decision outcome prior to actually making the decision (i.e., attitude rather than behavior is assessed), his/her answer does not necessarily reflect the actual decision outcome.

2.2.7 Illusion of Control

In a series of studies, Brandimarte et al. [36] dealt with the hypothesis that users suffer from an "illusion of control" when dealing with the privacy of their data. They found that users indeed seem to confuse the control over the publication of information with the control over the assessment of that information by third parties. Therefore, users are more likely to allow the publication of personal information and even provide more sensitive information, if they are given explicit control over the publication of their data. If, on the other hand, a third party is responsible for the publication of the same data, users may perceive a loss of control and express concerns about the usage of their data by others without authorization [37]. According to this hypothesis, the paradoxical behavior is caused by the false feeling of control over the further usage of personal data, which occurs if users can initially decide over the publication of it (e.g., by posting in social networks and managing the privacy settings for the post).

2.2.8 The Privacy Paradox as Methodological Artefact

Another potential reason for the dichotomy between behavior and attitude is based on methodological considerations. One explanation may be the inappropriate operationalization of these constructs in the particular studies dealing with the privacy paradox [57]. Behavior is often assessed as a dichotomous answer (for example by asking if someone has a public Facebook profile or not), whereas attitude is measured on a metric (e.g., a Likert-based) scale. However, dichotomous data always implies a potential limitation of variance, which can in turn lead to a reduction of statistical power. Hence, it is possible that in fact

there is a strong relationship between attitude and behavior and previous studies just failed to verify this relationship due to their inappropriate operationalization.
Another approach is based on the assumption of a multi-dimensional nature of privacy. Dienlin and Trepte [57] suggest that it is important to distinguish between privacy attitudes and privacy concerns on the one hand, and between informational, social and psychological privacy on the other hand. Indeed, a corresponding study by Dienlin and Trepte [57], which accounts for these different facets of privacy revealed an indirect effect of privacy concerns on privacy behavior. Specifically, privacy concerns had an effect on privacy attitudes, which in turn influenced privacy intentions, which finally influenced privacy behavior.
So far, no definite explanation for the privacy paradox has been proposed. However, considering the variety of possible explanations for the privacy paradox, either interpreting the phenomenon or developing extensive models to shed light on it, the dichotomy between privacy attitudes, concerns or perceived risk and privacy behavior should not be perceived as paradox anymore. To further understand which factors relate to user privacy, I report the standardized effect size (β) that could be found in the included studies concerning the association of the different predictor variables with privacy attitude, privacy concern, perceived privacy risk, privacy intention and privacy behavior in the next section.

2.3 Empirical Privacy Paradox Explanation Attempts

This section focusses on empirical attempts to explain the privacy paradox by investigating the factors that significantly predict privacy attitude, concerns, perceived risk, behavioral intention and behavior. To identify how important these factors are for the prediction of the different privacy aspects, I will report the standardized effect sizes (β) found in the included studies for the various predictor variables. Effect sizes will be interpreted as small ($\beta = .10$), medium ($\beta = .30$) or large ($\beta = .50$), as suggested by Cohen [48] for Pearson's correlation coefficient. Only statistically significant results are considered. Significance is presented together with the corresponding effect size, with one asterisk indicating significance on a 5% level ($p < .05$), two asterisks on a 1% level ($p < .01$), and three asterisks on a 0.1% level ($p < .001$). Where path analyses lack sufficient statistical power (<.8), a "(i.p.)" is included in the effect size column. Predictor variables are listed in descending order according to the respective effect sizes, i.e., the best predictor is always reported first and the worst predictor last. The reported effect sizes are either retrieved from regression analyses or structural equation modeling. Thus, the corresponding type of coefficient is reported in the last column, with "SEM" referring to effect sizes from structural equation modeling and "Regression" to those from regression analyses.

2.3.1 Privacy Attitude, Privacy Concerns and Perceived Privacy Risk

The theoretical construct "attitude towards privacy" actually refers to the general appraisal of different privacy behaviors. However, it is often assessed as "privacy concerns" or "perceived privacy risk". Since the relationship between attitude, concerns and perceived risk is not clearly defined in the literature, I will deal with the constructs separately.
Attitude. Some of the included studies actually assessed privacy attitude, i.e., the more general evaluation of a certain privacy behavior or privacy relevant product, instead of more specific privacy concerns or perceived privacy risk. Trepte and Dienlin [57] differentiate three aspects of privacy attitude, Kim and Adler [114] focused on social scientists' attitude towards sharing research data and Schwaig et al. [196] investigated users' attitude towards the information practice of corporations. Other studies assessed specific privacy attitudes, namely towards social network games, location-based social network applications and a location-based mobile website.
Privacy Attitude. In their study, Trepte and Dienlin [57] distinguish between three different privacy concepts: (1) Informational privacy, i.e., (not) giving identifiable information on Facebook, (2) social privacy, i.e., restricting access to one's Facebook profile, and (3) psychological privacy, i.e., (not) communicating personal information on Facebook. Privacy concerns regarding informational privacy are a mediocre to good predictor for informational privacy attitude, whereas social privacy concerns moderately predict so-

cial privacy attitude and psychological privacy concerns weak to moderately predict psychological privacy attitude.

Table 2: Predictor variables for privacy attitude.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns			
for informational privacy	Dienlin & Trepte [57]	0.42***	SEM
for social privacy		0.33***	
for psychological privacy		0.25***	

Social Scientist's Attitude towards Data Sharing. Social scientist's attitude towards sharing research data is moderately predicted by the subjectively gained career benefit and rather weakly by the perceived career risk.

Table 3: Predictor variables for social scientist's attitude towards data sharing.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived career benefit	Kim & Adler [114]	0.36***	SEM
Perceived career risk	Kim & Adler [114]	-0.18***	SEM

Attitude towards an Information Practice. The information practice of a corporation describes the procedure the corporation follows in the handling of a consumer's personal information. The consumer's attitude towards this information practice is very well predicted by his/her concern for information privacy and computer anxiety. Other good predictors are whether s/he has granted the corporation permission to use his/her personal data, the feeling of consumer alienation (i.e., feeling unable to influence market practices, market environment or events within the marketplace, accompanied by a distrust of business and market practices), whether the consumer generally interacts with IT, the level of the consumer's self-esteem and whether the corporation only transfers the information internally.

Table 4: Predictor variables for attitude towards an information practice.

Predictor variable	Primary study	Effect size (β)	Coefficient
Concern for information privacy	Schwaig et al. [196]	-0.70***	SEM
Computer anxiety	Schwaig et al. [196]	-0.70***	SEM
Permission granted	Schwaig et al. [196]	0.66***	SEM
Consumer alienation	Schwaig et al. [196]	-0.61***	SEM
Interaction with IT	Schwaig et al. [196]	0.52***	SEM
Self-esteem	Schwaig et al. [196]	0.51***	SEM
Transfer internally	Schwaig et al. [196]	0.51***	SEM

Attitude towards Social Network Games. Both perceived security and perceived playfulness of a social network game are relatively good predictors for the user's attitude towards such games.

Table 5: Predictor variables for attitude towards social network games.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived security	Shin & Shin [204]	0.50***	SEM
Perceived playfulness	Shin & Shin [204]	0.47***	SEM

Attitude towards Location-based Social Network Applications. The attitude towards location-based social network applications is predicted well and moderately to well by the perceived benefit and risk associated with using the application, respectively. Weak predictors are the social norm towards the application and the degree to which the user sees his-/herself as opinion leader, i.e., someone whose opinion influences others to make decisions.

Table 6: Predictor variables for attitude towards location-based social network applications.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived benefit	Koohikamali et al. [120]	0.50***	SEM
Perceived risk	Koohikamali et al. [120]	-0.37***	SEM
Social norm	Koohikamali et al. [120]	0.14** (i.p.)	SEM
Opinion leadership	Koohikamali et al. [120]	0.08* (i.p.)	SEM

Attitude towards a Location-based Mobile Website. The attitude towards a fictitious mobile website which provides restaurant recommendations based on the users current location is very well predicted by the user's trust towards that website.

Table 7: Predictor variables for attitude towards a location-based mobile website.

Predictor variable	Primary study	Effect size (β)	Coefficient
Trust	Zhang et al. [258]	0.79**	SEM

Privacy Concerns. I further divide the construct "privacy concerns" due to different operationalization in the corresponding studies, which assessed general privacy concerns, but also website and context specific privacy concerns, health information privacy concerns, and privacy concerns of teenagers relating to the use of social network sites (SNS).

General Privacy Concerns. General privacy concerns is best predicted by the feeling of consumer alienation, i.e., feeling unable to influence market practices, market environment or events within the marketplace, accompanied by a distrust of business and market practices. Furthermore, low levels of self-esteem are strongly associated with the expression of privacy concerns. High levels of perceived risk, computer anxiety and a strong disposition to privacy moderately predict high values of general privacy concerns. A small predictive value was shown for social awareness (i.e., passive involvement and raised interest in social issues), gender, with female users expressing higher levels of concerns, internet anxiety, internet literacy, the general willingness to share data on the internet and cultural factors, with users from collectivistic cultures being more concerned.

Website Specific Privacy Concerns. Like for general privacy concerns, for the prediction of website specific privacy concerns the perceived risk plays an important role as well. The particular website's reputation is found to be important especially if it holds a low reputation; however, this effect does not occur for the variable "disposition to privacy", which is a small to moderate predictor for website privacy concerns for all kinds of website reputations. Users tend to be less concerned if the website is familiar to them, they feel that they can control how their released information is processed and if the website does not contain a security cue, which warns users about untrusted site security authorization.

Context Specific Privacy Concerns. Analog to the prediction of general privacy concerns by consumer alienation, the control users perceive about the processing of their data is a crucial factor for the prediction of context specific privacy concerns, with users who feel less in control expressing more privacy concerns. Users also tend to be more concerned if they had experienced an infringement of their privacy before, whereas the presentation of the TRUSTe seal, showing the membership in an industry self-regulated privacy association, combined with the URL link to the according privacy policy, is related with less privacy concerns. Both predictor values can be considered as small to medium.

Table 8: Predictor variables for general privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Consumer Alienation	Schwaig et al. [196]	0.60***	SEM
Self-esteem	Schwaig et al. [196]	-0.54***	SEM
Perceived risk	Liao et al. [142]	0.44***	SEM
Computer Anxiety	Schwaig et al. [196]	0.37***	SEM
Disposition to privacy	Li [137]	0.36***	SEM
Social awareness	Liao et al. [142]	0.20***	SEM
Gender	Abbas & Mesch [3]	0.17**	Regression
Internet anxiety	Li [137]	0.17* (i.p.)	SEM
General willingness to share	Taddicken [220]	-0.15***	SEM
Internet literacy	Liao et al. [142]	0.14**	SEM
Culture - collectivism	Abbas & Mesch [3]	0.10* (i.p.)	Regression

Table 9: Predictor variables for website specific privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived privacy risk	Xu et al. [250]	0.69**	SEM
Website reputation	Li [137]	-0.20** (i.p.)	SEM
	Li [138]	-0.28**	
for high reputation websites		-0.26**	
for low reputation websites		-0.45**	
Disposition to privacy	Li [137]	0.23* (i.p.)	SEM
	Li [138]	0.20* (i.p.)	SEM
for high reputation websites		0.20* (i.p.)	
for low reputation websites		0.26** (i.p.)	
Website familiarity	Li [138]	-0.20** (i.p.)	SEM
for high reputation websites		-0.20** (i.p.)	
Information control	Xu et al. [250]	-0.20** (i.p.)	SEM
Existence of a security cue	Zhang et al. [258]	0.20* (i.p.)	SEM

Table 10: Predictor variables for context specific privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived control	Xu et al. [252]	-0.60**	SEM
Industry self-regulation	Xu et al. [252]	-0.19**	SEM
Privacy experience	Xu et al. [252]	0.16* (i.p.)	SEM

Health Information Privacy Concerns. The sensitivity of the particular health information moderately predicts the respective privacy concerns. The predictive value of previous privacy invasions, however, ranges between small and medium.

Table 11: Predictor variables for health information privacy concerns.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived health information sensitivity	Bansal et al. [26]	0.28***	SEM
Previous online privacy invasion	Bansal et al. [26]	0.17***	SEM

Teenage Privacy Concerns on SNS. Again, the variable best predicting privacy concerns, in this particular case experienced by teenagers concerning their use of social networks, is associated with perceived control: Teenagers are found to hold more privacy concerns if they find it difficult to control their privacy. However, this effect is considerably lesser than for context specific and general privacy concerns. Other variables that predict the extend of privacy concerns somewhat are the frequency of social network use, the existence of parental privacy concerns and the general performance of social risky interactions, with higher values predicting more privacy concerns.

Table 12: Predictor variables for teenage privacy concerns on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived ease of privacy control	Jia et al. [103]	-0.18*** (i.p.)	SEM
SNS use frequency	Jia et al. [103]	0.14** (i.p.)	SEM
	Feng & Xie [69]	0.12** (i.p.)	SEM
Parental privacy concern	Wisniewski et al. [245]	0.13** (i.p.)	SEM
	Feng & Xie [69]	0.12** (i.p.)	SEM
Risky interaction	Jia et al. [103]	0.10* (i.p.)	SEM
	Wisniewski et al. [245]	0.10* (i.p.)	SEM

Perceived Privacy Risk. None of the examined variables was found to be of great significance for the prediction of perceived privacy risk. The predictive power of privacy concerns varies across different studies from small to medium, but was found to be smaller than for the corresponding prediction of privacy concerns by perceived risk. How much risk is perceived is further moderately predicted by the user's trust in the recipient's ability to protect his/her data, the degree of personalization that is gained by data disclosure and the perceived relevance of the collected information. Furthermore, negative values of perceived privacy regulatory protection (which refers to the user's perception of provisions and systems that protect his/ her personal data, in terms of existence and adequacy) were found to predict an increase of the perceived privacy risk. In accordance with that, users perceive less risk if they trust for example the governmental and commercial entities that are associated with information privacy, if they have an initial joyful emotional reaction at the first impression of the data receiving website, as well as if they are younger and male, though the last-mentioned effect was negligible. On the other hand, users perceive higher privacy risk if they are well aware of privacy risks in general, if they have already experienced privacy infringements, if the respective data is rather sensitive, if their first emotional reaction to the receiving website is fearful and, finally, if they have a maternalistic personality, meaning they have a strong desire to protect the socially vulnerable from external danger.

2.3.2 Privacy Related Behavioral Intention and Willingness

I will distinguish between the "intention" and the "willingness" to disclose data, since it is not specified in the literature whether these concepts can be considered as similar.

Intention Due to different operationalization in the included studies, I will report the predictor values separately for the general intention to disclose information, the intention to disclose information on social network sites (SNS), the intention to make Facebook data publicly (i.e., beyond the social network) accessible and the intention to disclose data to an online retailer.

General Intention to Disclose Information. The general intention to disclose information can be very well predicted by the user's trust in the receiving website according to Bansal et al. [26], slightly better than moderately according to Li [137] and moderately to weakly according to Wakefield [232]. Likewise, high values of privacy protection belief, i.e., the belief that one is able to control how the disclosed information is used moderately to weakly predict an increase in intention to disclose information. High values of perceived privacy risk, on the other hand, moderately predict a decrease in the intention to disclose information, along with high values of website privacy concern and, to a lesser extent, general privacy concern. A small to

Table 13: Predictor variables for perceived privacy risk.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns	Miltgen et al. [163]	0.34***	SEM
	Zhou [260]	0.23**	SEM
	Li et al. [134]	0.22***	SEM
	Keith et al. [109]	0.18***	SEM
Level of trust in the recipient's ability to protect data	Beldad et al. [31]	-0.32***	Regression
Personalization	Xu et al. [253]	0.29**	SEM
Perceived relevance of information	Li et al. [134]	-0.28***	SEM
Perceived privacy regulatory protection	Miltgen & Smith [164]	-0.25***	SEM
Privacy risk awareness	Keith et al. [109]	0.25***	SEM
Initial joy	Li et al. [134]	-0.21***	SEM
Prior experience with privacy infringement	Xu et al. [253]	0.20**	SEM
	Bansal et al. [26]	0.17***	SEM
	Baek & Kim [21]	0.08***	Regression
Assessment of data sensitivity			
for publicly accessible contact data	Beldad et al. [31]	0.18*	Regression
for confidential data		0.19**	
Initial fear	Li et al. [134]	0.17* (i.p.)	SEM
Trust	Zhou [260]	-0.15*	SEM
	Miltgen & Smith [164]	-0.10**	SEM
Age	Baek & Kim [21]	-0.10***	Regression
Gender	Baek & Kim [21]	0.02* (i.p.)	Regression
Maternalistic personality	Baek & Kim [21]	0.11**	Regression

moderate predictive effect was also found for the perceived benefits gained through information disclosure and the experience of a positive affect. Experiencing a negative affect, the prior experience with the receiving website and the number of years a person has spent in full-time employment (regardless which kind of job s/he holds) also somewhat predict the disclosure intention.

Intention to Disclose Information on SNS. The benefits users expect to gain from the disclosure of their data are an excellent predictor of their intention to disclose information on SNS. Moderate predictive power could be shown for the attitude towards disclosure and the willingness to disclose. The small predictive effect of gender found by Van Gool et al. [90] suggests that female adolescents have a higher intention to self-disclose. The same goes for older adolescents and those whose friends and parents have a positive attitude towards data disclosure on social networks. Privacy concerns, on the other hand, are somewhat negatively associated with the intention to disclose information on social networks.

Intention to Make Facebook Data Publicly Accessible. The intention to make Facebook data publicly accessible, that is, to share the answer to various Facebook items with "everyone on the internet', is best predicted by different variables, depending on the type of information. The trust someone has in Facebook mostly predicts his/her intention to share interests data, whereas the need for consent (i.e., the belief that Facebook should only share data or make changes in its settings with the permission of the user) is strongly associated with the intention to share contact data, rather moderately with the intention to share activity data, only weakly with the disclosure of location data and not significantly with the disclosure of interests

Table 14: Predictor variables for general intention to disclose information.

Predictor variable	Primary study	Effect size (β)	Coefficient
Website trust	Bansal et al. [26]	0.85***	SEM
	Li [137]	0.42***	SEM
	Wakefield [232]	0.23**	SEM
Website privacy concern	Li [137]	-0.43***	SEM
Perceived privacy risk	Keith et al. [109]	-0.42***	SEM
	Li et al. [134]	-0.37**	SEM
	Norberg et al. [167]	-0.34*	Regression
Privacy concern	Bansal et al. [26]	-0.27***	SEM
	Li et al. [134]	-0.15* (i.p.)	SEM
	Keith et al. [109]	-0.07** (i.p.)	SEM
Privacy protection belief	Wakefield [232]	0.26***	SEM
	Li et al. [134]	0.19*	SEM
Perceived benefits	Keith et al. [109]	0.22***	SEM
Positive affect (enjoyment)	Wakefield [232]	0.19**	SEM
Negative affect	Wakefield [232]	-0.11* (i.p.)	SEM
Prior positive experience with the website	Bansal et al. [26]	0.08** (i.p.)	SEM
Employment	Keith et al. [109]	0.07** (i.p.)	SEM

Table 15: Predictor variables for intention to disclose information on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Perceived benefit	Xu et al. [250]	0.81***	SEM
	Xu et al. [250]	0.81***	Regression
Willingness	Van Gool et al. [90]	0.34***	SEM
Attitude	Van Gool et al. [90]	0.32***	SEM
Privacy concerns	Xu et al. [250]	-0.19* (i.p.)	SEM
	Xu et al. [250]	-0.14** (i.p.)	Regression
Subjective norm of friends	Van Gool et al. [90]	0.17***	SEM
Subjective norm of parents	Van Gool et al. [90]	0.15***	SEM
Gender	Van Gool et al. [90]	0.11***	SEM
Age	Van Gool et al. [90]	0.07*	SEM

data at all. At the same time, knowledge about privacy policies does not predict the disclosure of location or contact data, and only marginally predicts the disclosure of interests and activity data.

Intention to Disclose Data to an Online Retailer. Like the intention to disclose Facebook data to the public, the intention to disclose information to an online retailer (e.g., for registration purposes) is predicted by different variables according to the particular type of disclosed information. The absence of collection concerns (i.e., general concerns about online companies collecting data) is strongly associated with the intention to disclose contact data, but there is only a weak relationship for health data. Control concerns, that is, a strong desire to control the processing of one's own personal data, is a weak to moderate predictor of the disclosure intention for interests and work data, but not for health or contact data.

Willingness I report the predictor values for general willingness to disclose information and willingness to disclose information about peer relationships on Facebook.

Willingness to Disclose Information. Many variables were found to predict the willingness to disclose information in general. In line with the privacy calculus model, the user's decision to disclose information

Table 16: Predictor variables for intention to make Facebook data publicly accessible.

Predictor variable	Primary study	Effect size (β)	Coefficient
Need for consent			
for activity data	Knijnenburg et al. [118]	-0.25***	Regression
for location data		-0.14*	
for contact data		-0.58***	
Trust in Facebook			
for activity data	Knijnenburg et al. [118]	0.30***	Regression
for location data		0.33***	
for contact data		0.28***	
for interests data		0.49***	
Knowledge about privacy policy			
for location data	Knijnenburg et al. [118]	-0.10* (i.p.)	Regression
for interests data		-0.16***	

Table 17: Predictor variables for intention to disclose data to an online retailer.

Predictor variable	Primary study	Effect size (β)	Coefficient
Collection concerns			
for health data	Knijnenburg et al. [118]	-0.16* (i.p.)	Regression
for contact data		-0.45***	
for interests data		-0.21*	
for work data		-0.27***	
Control concerns			
for interests data	Knijnenburg et al. [118]	0.23*	Regression
for work data		0.23*	

is strongly associated with the perceived value or benefits they can gain through that disclosure (e.g., the "perceived value", the "perceived usefulness" or the fact that they "liked the targeted ads"). This applies to both cases, the situation in which the benefits (e.g., personalization) are overt ("overt-based") or hidden ("covert-based"). Users are unwilling to share browsing information if the data storage retention period is indefinite; however, this circumstance is less important for the disclosure of demographic information. Privacy concerns are likely to be moderate predictors for the willingness to disclose information, irrespective of the information type. Facebook users tend to exhibit a greater willingness to disclose information ("Facebook usage"), and also do users who are personally innovative (e.g., early adopters) or prone to discounts (e.g., coupons). In contrast, users are less willing to disclose information if these are shared with third parties, for example Facebook, and not only with the recipient ("usage scope"; in Leon et al. [133] the recipient is a health site). Age, on the other hand, was shown to be a negligible predictor for the willingness to disclose information.

Willingness to Disclose Information about Peer Relationships on Facebook. How willing teenagers are to disclose information about their peer relationships on Facebook is moderately predicted by the mental prototype they have of a person who performs this very behavior. If they perceive the prototype, that is, the typical person who would disclose information about peer relationships on Facebook, as similar to them and also evaluate the prototype as positive, they are more willing to disclose peer relationship information on Facebook themselves. The attitude towards disclosure, gender and age are of lesser, but still statistically significant predictive power for the willingness to disclose, with female and older adolescents being more willing to disclose.

Table 18: Predictor variables for willingness to disclose information.

Predictor variable	Primary study	Effect size (β)	Coefficient
Liked targeted ads			
for browsing information	Leon et al. [133]	0.68***	Regression
for computer information		0.59***	
for demographic information		0.62***	
for location information		0.62***	
for personally identifiable information		0.62***	
Perceived value			
for covert-based scenario	Xu et al. [253]	0.60**	SEM
for overt-based scenario		0.56**	
Retention period: indefinite			
for browsing information	Leon et al. [133]	-0.47***	Regression
for demographic information		-0.17*	
for location information		-0.28***	
Privacy concerns	Lee & Cranage [127]	-0.41***	Regression
for browsing information	Leon et al. [133]	-0.29***	Regression
for computer information		-0.25***	
for demographic information		-0.33***	
for location information		-0.34***	
for personally identifiable information		-0.26***	
Perceived usefulness	Lee & Cranage [127]	0.33***	Regression
Usage scope: health site and Facebook			
for location information	Leon et al. [133]	-0.33***	Regression
for personally identifiable information		-0.33***	
Usage scope: all sites			
for browsing information	Leon et al. [133]	-0.30***	Regression
Facebook usage			
for browsing information	Leon et al. [133]	0.15***	Regression
for computer information		0.22***	
for demographic information		0.21***	
for location information		0.19***	
for personally identifiable information		0.19***	
Personal innovativeness			
for covert-based scenario	Xu et al. [253]	0.19**	SEM
for overt-based scenario		0.11* (i.p.)	
Coupon proneness			
for covert-based scenario	Xu et al. [253]	0.15** (i.p.)	SEM
Age			
for demographic information	Leon et al. [133]	-0.004*	Regression
for location information		-0.008***	

Table 19: Predictor variables for willingness to disclose information about peer relationships on Facebook.

Predictor variable	Primary study	Effect size (β)	Coefficient
Prototype similarity	Van Gool et al. [90]	0.32***	SEM
Prototype favorability	Van Gool et al. [90]	0.21***	SEM
Attitude	Van Gool et al. [90]	0.13***	SEM
Gender	Van Gool et al. [90]	0.11***	SEM
Age	Van Gool et al. [90]	0.07*	SEM

2.3.3 Privacy Related Behavior

The examined privacy behavior comprises the disclosure of information, either in general, on a social network or towards a particular application, as well as the actual usage of data sharing applications, the management of privacy settings and the performance of privacy protection behavior.

Information Disclosure. The operationalization of information disclosure in the included studies comprises general information disclosure, information disclosure on social network sites (SNS), the breadth and depth of information disclosure on SNS, the disclosure of less sensitive information on SNS, teenager's information disclosure on social media, information disclosure towards a recommender application for mobile apps, the disclosure of location information on a location-based social network application and the sharing behavior regarding personal profile information in a mobile application.

General Information Disclosure. Whether someone tends to disclose information in general was found to be highly associated with his/her willingness to self-disclose in the first place. The association between behavioral intention and actual disclosure might be much smaller. A moderate association was found for the perceived relevance of the social web in the user's social environment, the number of social web applications used (with users who use only a few applications tending to disclose more information overall) and the awareness of how the disclosed information is used (in the case of the study conducted by Wang et al. [233], for personalized advertising). A small negative association was found for the control over what the disclosed information is used for, the experienced comfort during information disclosure and the existence of a security cue on the receiving website in form of a banner warning that a trusted security certificate could not be detected. Albeit contra intuitive at the first glance, the negative association between information disclosure and control about the further processing of the disclosed information may be caused by an increase in awareness about potential consequences, which is in turn triggered by the theoretical preoccupation with the processing of personal information. A marginal predictive effect was found for age.

Information Disclosure on SNS. The privacy intention, i.e., the intention users have concerning the respective disclosure behavior, was shown to be the main variable predicting information disclosure on SNS in general, with a greater predictive power for psychological privacy behavior (that is, how personal is the social network profile and how many personal things are posted there) than for informational privacy behavior (the amount of identifying information that can be found on the SNS). Furthermore, a large to medium predictive effect was shown for privacy concerns, whereas the privacy attitude only weakly predicts the information disclosure on social networks, for both identifiable and personal information.

Information Disclosure on SNS (Breadth). The breadth of information disclosure is defined as the range of topics that is posted on the SNS [136]. Analog to the general information disclosure on SNS, privacy concerns are also a good to moderate predictor for the breadth of information disclosure. A weak to moderate predictive effect was shown for gender (with females tending to disclose more broadly) and, to a lesser extent, for age, the degree pf activity and experience of the user on SNS. A marginal predictive effect was found for the number of posted blogs on the social network and the number of social network friends.

Information Disclosure on SNS (Depth). The depth of information disclosure refers to the sensitivity of the disclosed information [136]. Gender does not only predict the breadth, but also the depth of information

Table 20: Predictor variables for general information disclosure.

Predictor variable	Primary study	Effect size (β)	Coefficient
General Willingness to Self-Disclose	Taddicken [220]	0.59***	SEM
Number of applications	Taddicken [220]	-0.35***	SEM
Ads awareness	Wang et al. [233]	-0.28***	SEM
Social relevance	Taddicken [220]	0.27***	SEM
Existence of a security cue (certificate warning)	Zhang et al. [258]	0.14*	SEM
Comfort level in disclosing information	Wang et al. [233]	0.13*	SEM
Intent to disclose	Keith et al. [109]	0.12**	SEM
Control over what information is used for	Wang et al. [233]	-0.12**	SEM
Age	Taddicken [220]	-0.02*** (i.p.)	SEM

Table 21: Predictor variables for information disclosure on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy intention			
informational privacy	Dienlin & Trepte [57]	-0.65***	SEM
psychological privacy		-0.79***	
Privacy concerns	Becker & Pousttchi [30]	-0.43***	SEM
Privacy attitude			
informational privacy	Dienlin & Trepte [57]	-0.11*	SEM
psychological privacy		-0.08* (i.p.)	

disclosure on social networks on a small to moderate level, again with female users disclosing in more depth. Minor predictive effects have been shown for age, the number of social network friends, the user's degree of activity and experience on social networks, and the number of posted blogs on the SNS.

Information Disclosure on SNS (Less Sensitive Information). The disclosure of less sensitive information on SNS shows a similar picture regarding the predictive variables compared to the social network information disclosure breadth: Gender was shown to be a better – but still weak – predictor than user activeness and experience in social networks. On the other hand, age, along with the number of posted blogs and friends only marginally predict information disclosure.

Teenage Information Disclosure on Social Media. Teenagers' disclosure of information about peer relationships on social media is best predicted by the intention to do so, whereas the willingness was found to be less important. They also tend to disclose more sensitive information if they also disclose basic information, for example their real name, birth date and school name. The results also suggest a moderate to small predictive value of social network complexity, which describes how diverse the network relationships of a user are, for example whether s/he is friends with her/his parents, siblings, the extended family, school friends, other friends etc. The more complex the social networks, the more do teenagers tend to disclose personal and sensitive information. The size of the own social network (that is, number of social network friends) is also a weak to mediocre predictor for teenage information disclosure on social media, with teenagers disclosing more contact and insensitive information if they have a large number of social network friends. Somewhat smaller predictive value was found for social network usage frequency, age, gender (with males disclosing more contact information and females disclosing more peer relationship information), the direct intervention of parents in the information disclosure on social networks and the general trust in

Table 22: Predictor variables for information disclosure on SNS (breadth).

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns	Becker & Pousttchi [30]	-0.43***	SEM
Gender	Li et al. [136]	-0.18** (i.p.)	SEM
for young users (< 24)		-0.21**	
for middle-aged users (25- 39)		-0.20**	
for older users (> 40)		-0.19* (i.p.)	
User activeness and experience on SNS			
for older users (> 40)	Li et al. [136]	0.07* (i.p.)	SEM
Age	Li et al. [136]	-0.04*	SEM
for male users		-0.05* (i.p.)	
for female users		-0.05* (i.p.)	
Number of posted blogs	Li et al. [136]	0.01** (i.p.)	SEM
for male users		0.01** (i.p.)	
for female users		0.01** (i.p.)	
for young users (< 24)		0.01** (i.p.)	
for middle-aged users (25- 39)		0.01** (i.p.)	
for older users (> 40)		0.01** (i.p.)	
Number of friend	s		
for female users	Li et al. [136]	0.01* (i.p.)	SEM

Table 23: Predictor variables for information disclosure on SNS (depth).

Predictor variable	Primary study	Effect size (β)	Coefficient
Gender	Li et al. [136]	-0.20** (i.p.)	SEM
for young users (< 24)		-0.25**	
for middle-aged users (25- 39)		-0.20**	
Age	Li et al. [136]	-0.03* (i.p.)	SEM
for female users		-0.03*(i.p.)	
User activeness and experience on SNS			
for older users (> 40)	Li et al. [136]	-0.03* (i.p.)	SEM
Number of friends			
for female users	Li et al. [136]	0.01* (i.p.)	SEM
Number of posted blogs	Li et al. [136]	0.01* (i.p.)	SEM

other people. Regarding the direct interaction with the SNS, teenagers disclose more information if they also set their profiles as private, if they have social network friends that do not go to school with them and also if they have strangers as friends on the social network. However, these relationships can also be considered as rather weak.

Information Disclosure towards a Mobile App Recommender. How much of their phone usage (context) and demographic data users disclose towards an app that recommends new apps based on the disclosed data is well to moderately predicted by their general collection concerns and weak to moderately by the extent of their mobile internet usage. However, users tend to disclose context data more easily than demographic data.

Location Disclosure on Location-Based Social Network Application. Whether users disclose their location on location-based social network applications can at least be moderately predicted by their attitude towards

Table 24: Predictor variables for information disclosure on SNS (less sensitive information).

Predictor variable	Primary study	Effect size (β)	Coefficient
Gender	Li et al. [136]	-0.17** (i.p.)	SEM
for young users (< 24)		-0.17** (i.p.)	
for middle-aged users (25- 39)		-0.16** (i.p.)	
for older users (> 40)		-0.15* (i.p.)	
User activeness and experience on SNS			
for older users (> 40)	Li et al. [136]	0.07* (i.p.)	SEM
Age	Li et al. [136]	-0.04* (i.p.)	SEM
for male users		-0.04* (i.p.)	
for female users		0.05* (i.p.)	
Number of posted blogs	Li et al. [136]	0.01** (i.p.)	SEM
for male users		0.01** (i.p.)	
for female users		0.01** (i.p.)	
for young users (< 24)		0.01** (i.p.)	
for middle-aged users (25- 39)		0.01** (i.p.)	
for older users (> 40)		0.01** (i.p.)	
Number of friends			
for female users	Li et al. [136]	0.01* (i.p.)	SEM

such applications. Unlike for the prediction of general willingness to disclose data, the incentives gained through location disclosure serve only as weak predictor for the decision to actually disclose one's location on SNS apps.

Sharing of Profile Information in a Mobile App. Whether users share their personal profile in a mobile app with their friends or with every user of the app is somewhat predicted by their intent to disclose data in general.

Usage of Data Sharing Applications The included studies assessed the usage of a location sharing application as well as the usage of social network games.

Usage of a Location Sharing Application. Whether users decide to use a location sharing app or not is best predicted by the amount of benefits they can gain through the usage, with entertainment being twice as important as impression management (i.e., the ability of someone to control the impression of others toward him/her). Social influence and the intention to disclose data are small to mediocre and the competence-based and general trust in the location sharing application (LSA) network rather weak predictors for the usage decision.

Usage of Social Network Games. The usage intention was shown to be the only significant predictor for the actual usage of social network games.

Privacy settings on SNS were assessed in general and specifically for teenagers.

Privacy Settings on SNS. How strict or lax users set their privacy settings in social networks is mainly predicted by their privacy intention, their privacy concerns (with a greater predictive effect for the Dutch social network Hyves than for the German network StudiVZ) as well as the perceived norms regarding what information should only be shared with friends. Stronger privacy concerns and more restrictive norms were related to stricter privacy settings, whereas the intention reflects the behavior insofar as users who want to distinguish their identity on Facebook are less identifiable (informational privacy), users who want to restrict access to their Facebook profile tend to do so (social privacy), users who want to have a less personal profile have one (psychological privacy) etc. A small to moderate predictive effect was shown for the tendency to use the internet for the purpose of impression management, the privacy attitude and high scores on the personality trait narcissism, i.e., the feeling of being a very special person.

Table 25: Predictor variables for teenage information disclosure on social media.

Predictor variable	Primary study	Effect size (β)	Coefficient
Intention			
for peer relationship information	Van Gool et al. [90]	0.58***	SEM
Basic Information Disclosure			
for sensitive information	Wisniewski et al. [245]	0.29***	SEM
Network size/ Number of friends			
for contact information	Xie & Kang [248]	0.21***	Regression
for insensitive information		0.24***	
SNS complexity			
for personal information	Jia et al. [103]	0.20***	
for sensitive information		0.23***	SEM
SNS use frequency			
for personal information	Jia et al. [103]	0.21***	SEM
	Xie & Kang [248]	0.10* (i.p.)	Regression
for sensitive information	Jia et al. [103]	0.17*** (i.p.)	SEM
Willingness			
for peer relationship information	Van Gool et al. [90]	0.17***	SEM
Gender	Jia et al. [103]	-0.12** (i.p.)	SEM
for contact information	Xie & Kang [248]	-0.16***	Regression
for peer relationship information	Van Gool et al. [90]	0.17***	SEM
Age	Jia et al. [103]	0.16** (i.p.)	SEM
for personal information	Xie & Kang [248]	0.15**	Regression
for peer relationship information	Van Gool et al. [90]	0.06*	SEM
Privacy settings			
for contact information	Xie & Kang [248]	-0.10* (i.p.)	Regression
for insensitive information		-0.14**	
Parental direct intervention	Wisniewski et al. [245]	-0.13** (i.p.)	SEM
Having SNS friends that do not go to school with the participant			
for personal information	Xie & Kang [248]	0.10*	Regression
Having strangers as SNS friends			
for contact information	Xie & Kang [248]	0.13*	Regression
for insensitive information		0.12*	
Trust in other people			
for contact information	Xie & Kang [248]	0.10*	Regression

Table 26: Predictor variables for information disclosure towards a mobile app recommender.

Predictor variable	Primary study	Effect size (β)	Coefficient
Collection concerns			
for context data	Knijnenburg et al. [118]	0.46***	Regression
for demographic data		0.22***	
Mobile internet usage			
for context data	Knijnenburg et al. [118]	0.25***	Regression
for demographic data		0.15*	

Impression management as usage purpose was related to less restrictive privacy settings, as were high

Table 27: Predictor variables for location disclosure on location-based social network application.

Predictor variable	Primary study	Effect size (β)	Coefficient
Attitude towards location-based social network application	Koohikamali et al. [120]	0.43***	SEM
Incentives	Koohikamali et al. [120]	0.11* (i.p.)	SEM

Table 28: Predictor variables for sharing of profile information in a mobile app.

Predictor variable	Primary study	Effect size (β)	Coefficient
Intent to disclose	Keith et al. [109]	0.13***	SEM

Table 29: Predictor variables for usage of a location sharing application.

Predictor variable	Primary study	Effect size (β)	Coefficient
Benefits – entertainment	Beldad & Citra Kusumadewi [32]	0.32***	Regression
Social influence	Beldad & Citra Kusumadewi [32]	0.21***	Regression
Intent to disclose	Keith et al. [109]	0.18***	SEM
Benefits – impression management	Beldad & Citra Kusumadewi [32]	0.15***	Regression
Competence-based trust in LSA	Beldad & Citra Kusumadewi [32]	0.14***	Regression
General trust in LSA network	Beldad & Citra Kusumadewi [32]	0.11**	Regression

Table 30: Predictor variables for usage of social network games.

Predictor variable	Primary study	Effect size (β)	Coefficient
Usage intention	Shin & Shin [204]	0.39*	SEM

values of narcissism. The effect of privacy attitude is similar to privacy intention, with users who think it is favorable to distinguish their identity on Facebook tend to be less identifiable etc.

Teenage Privacy Settings on SNS. The privacy concerns of teenagers about their online data being collected by marketers weakly predicts their decision to implement privacy-setting strategies, such as deleting photo tags or intentionally posting false information about themselves. A weak association was also found between the implementation of these strategies and the teenagers' level of SNS use.

Again, in some studies privacy protective behaviors were assessed in general whereas others focused on protective behaviors of teenagers on SNS.

Privacy-Protective Behaviors. Several variables were found to moderately to weakly predict the performance of privacy-protective behaviors: The years of experience someone has with using the internet, the perceived rewards one gets for data disclosure, privacy risk concerns and the tendency to believe that one is less likely to experience privacy infringements compared to younger users. Smaller predictive effects were found for internet usage, autonomy (not further specified), age (with younger users showing more privacy-protective behaviors), perceived personal risk, household income and gender, with males reporting higher levels of privacy-protective behavior.

Teenage Privacy Protection on SNS. Teenagers are rather likely to remedy their disclosures on social networks if they also tend to interact with unknown others in a risky way on the corresponding SNS

Table 31: Predictor variables for privacy settings on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy intention			
for informational privacy	Dienlin & Trepte [57]	0.65***	SEM
for social privacy		0.45***	
for psychological privacy		0.79***	
Privacy concerns			
for Hyves, random sample	Utz & Kramer [230]	0.35**	Regression
for Hyves, self selected sample		0.29***	
for StudiVZ		0.21**	
Perceived norms regarding what to show only to friends			
for Hyves, random sample	Utz & Kramer [230]	0.33**	Regression
for StudiVZ		0.31**	
Impression management			
for Hyves, self selected sample	Utz & Kramer [230]	0.22**	Regression
Privacy attitude			
for informational privacy	Dienlin & Trepte [57]	0.11* (i.p.)	SEM
for social privacy		0.20***	
for psychological privacy		0.08* (i.p.)	
Narcissism			
for StudiVZ	Utz & Kramer [230]	-0.16* (i.p.)	Regression

Table 32: Predictor variables for teenage privacy settings on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Privacy concerns about their online data being collected by marketers			
implementation of privacy-setting strategies	Feng & Xie [69]	0.17***	SEM
Teenage level of SNS use		0.10* (i.p.)	

(rather strong predictor) and have privacy concerns (weak to mediocre predictor). Remedy of disclosure is further weakly predicted by female sex, tendency to disclose sensitive information, the performance of advice-seeking behaviors, the participation of parents in direct intervention or active mediation as well as the frequent usage of SNS. Whether teenagers seek advice about their social network privacy behaviors is moderately to weakly predicted by their privacy concerns, their tendency to disclose sensitive information, and weakly by their age (with younger teenagers being more likely to seek advice) and gender (with female teenagers being more likely to seek advice) as well as the participation of their parents in direct interventions.

2.4 Discussion

The following section combines the identified privacy paradox explanation attempts, either derived from theoretical considerations or drawn from empirical studies. First, I identify the main predictors for privacy attitude, concerns, perceived risk, behavioral intention and behavior based on the empirical study results in section 2.4.1. In section 2.4.2, I identify predictor variables for future studies and in section 2.4.3, I discuss which implications these empirical study results hold for the theoretical privacy paradox explanation

Table 33: Predictor variables for privacy-protective behaviors.

Predictor variable	Primary study	Effect size (β)	Coefficient
Years of internet experience			
technical behavior	Park [171]	0.25***	SEM
social behavior		0.21***	
Comparative optimism toward young users	Baek & Kim [21]	0.24**	Regression
Perceived rewards for data disclosure	Miltgen & Smith [164]	-0.24***	SEM
Privacy risk concerns	Miltgen & Smith [164]	0.23***	SEM
Internet use	Baek & Kim [21]	0.11*	Regression
technical behavior	Park [171]	0.11* (i.p.)	SEM
social behavior		0.21***	
Gender	Baek & Kim [21]	-0.04** (i.p.)	Regression
technical behavior	Park [171]	-0.19***	SEM
Autonomy			
technical behavior	Park [171]	0.15**	SEM
Age			
technical behavior	Park [171]	-0.14**	SEM
social behavior		-0.15**	
Perceived personal risk	Baek & Kim [21]	0.14**	Regression
Household income			
social behavior	Park [171]	-0.13*	SEM

approaches. Section 2.4.4 deals with the limitations of this review. Finally, I draw some summarizing conclusions from this review in section 2.4.5.

2.4.1 Main Predictors of Privacy Attitude, Concerns, Perceived Risk, Behavioral Intention and Behavior

Although a multiplicity of significant predictor variables for privacy attitude, privacy concerns, perceived privacy risk, privacy behavioral intention and privacy behavior were investigated, unfortunately, no variable could be identified as a "clear winner" for the prediction of the respective constructs. There are several possible explanations for this circumstance. First, many of the predictor variables were only investigated in a single study. However, some predictor variables were studied repeatedly, partially resulting in rather unequal effect sizes. The standardized path coefficients for the prediction of general intention to disclose information based on website trust, for example, ranged from 0.23 to 0.85. For the prediction of perceived privacy risk, the standardized path coefficients for prior experience with privacy infringement vary between 0.08 and 0.20. Furthermore, some of the authors relied on different definitions for the subordinate constructs attitude, concerns, perceived risk, behavioral intention and behavior or focused on very specific aspects of the respective construct, like teenage information disclosure on social media instead of general information disclosure. Finally, there are not only differences in the quality of the considered studies (see Appendix A), but also in the characteristics of the considered sample (e.g., students vs. older participants, collectivistic vs. individualistic cultural background etc.). No inconsistencies should be caused by the employed study methodology, though, since all considered studies are surveys of an explanatory nature, i.e., aiming to find proposed causal relationships between variables.

In an attempt to still identify the most significant predictors for the different privacy aspects attitude, concerns, perceived risk, behavioral intention and behavior, all predictor variables with an effect size of at

Table 34: Predictor variables for teenage privacy protection on SNS.

Predictor variable	Primary study	Effect size (β)	Coefficient
Risky interaction			
remedy of disclosure	Jia et al. [103]	0.44***	SEM
	Wisniewski et al. [245]	0.46***	SEM
Privacy concern			
remedy of disclosure	Jia et al. [103]	0.23***	SEM
	Wisniewski et al. [245]	0.10**	SEM
advice seeking	Jia et al. [103]	0.36***	SEM
	Wisniewski et al. [245]	0.19***	SEM
Sensitive disclosure			
remedy of disclosure	Jia et al. [103]	0.14***	SEM
	Wisniewski et al. [245]	0.12***	SEM
advice seeking	Jia et al. [103]	0.20***	SEM
Gender			
remedy of disclosure	Jia et al. [103]	0.16***	SEM
advice seeking		0.10*	SEM
Advice-Seeking			
remedy of disclosure	Wisniewski et al. [245]	0.12***	SEM
Age			
advice seeking	Jia et al. [103]	-0.11**	SEM
Parental direct intervention			
remedy of disclosure	Wisniewski et al. [245]	-0.10*	SEM
advice seeking		-0.10*	
Parental active mediation			
remedy of disclosure	Wisniewski et al. [245]	0.10**	
SNS frequency			
remedy of disclosure	Jia et al. [103]	0.08*	SEM

least 0.25 ($\beta \geq 0.25$) are listed in this section. In fig. 2-fig. 5, the corresponding effect sizes found in the different studies are displayed.

Privacy Attitude, Concerns and Perceived Risk. Most of the variables with high predictive value indeed predict privacy attitude (or attitude towards specific products and technologies), instead of concerns or perceived risk. The list of very good predictors for attitude include trust towards the particular mobile website, information privacy concerns, computer anxiety, whether the user has granted permission for further data processing and the feeling of consumer alienation (i.e., feeling unable to influence market practices, market environment or events within the marketplace, accompanied by a distrust of business and market practices). Other good predictors are the users' self-esteem, whether they have experience in interacting with information technology, whether the respective data is only transferred further inside the data receiving corporation as well as the perceived security, playfulness and benefit regarding the application. Perceived career benefit is a mediocre predictor for social scientist's attitude towards sharing research data sets.

Among the most significant predictors for privacy concerns are situation-specific factors like the perceived risk or control, respectively, and the website's reputation. However, user-related factors like consumer alienation, self-esteem, computer anxiety and disposition to privacy also play a major role for the development of privacy concerns. How sensitive the particular data is, although still relevant, was found to be of less importance.

The results indicate that there are only mediocre predictors for perceived privacy risk, at least among the investigated variables. These comprise the level of trust in the recipient's ability to protect the provided data, the perceived protection through privacy regulations, the perceived relevance of the according information and the degree of personalization on the according website or application. Surprisingly, the study results suggest that privacy concerns and privacy risk awareness are also only moderately suited to predict perceived risk. Since perceived risk, on the other hand, seems to be a rather good predictor for privacy concerns, it could be worthwhile to take a closer look at how users evaluate privacy risks (see fig. 2).

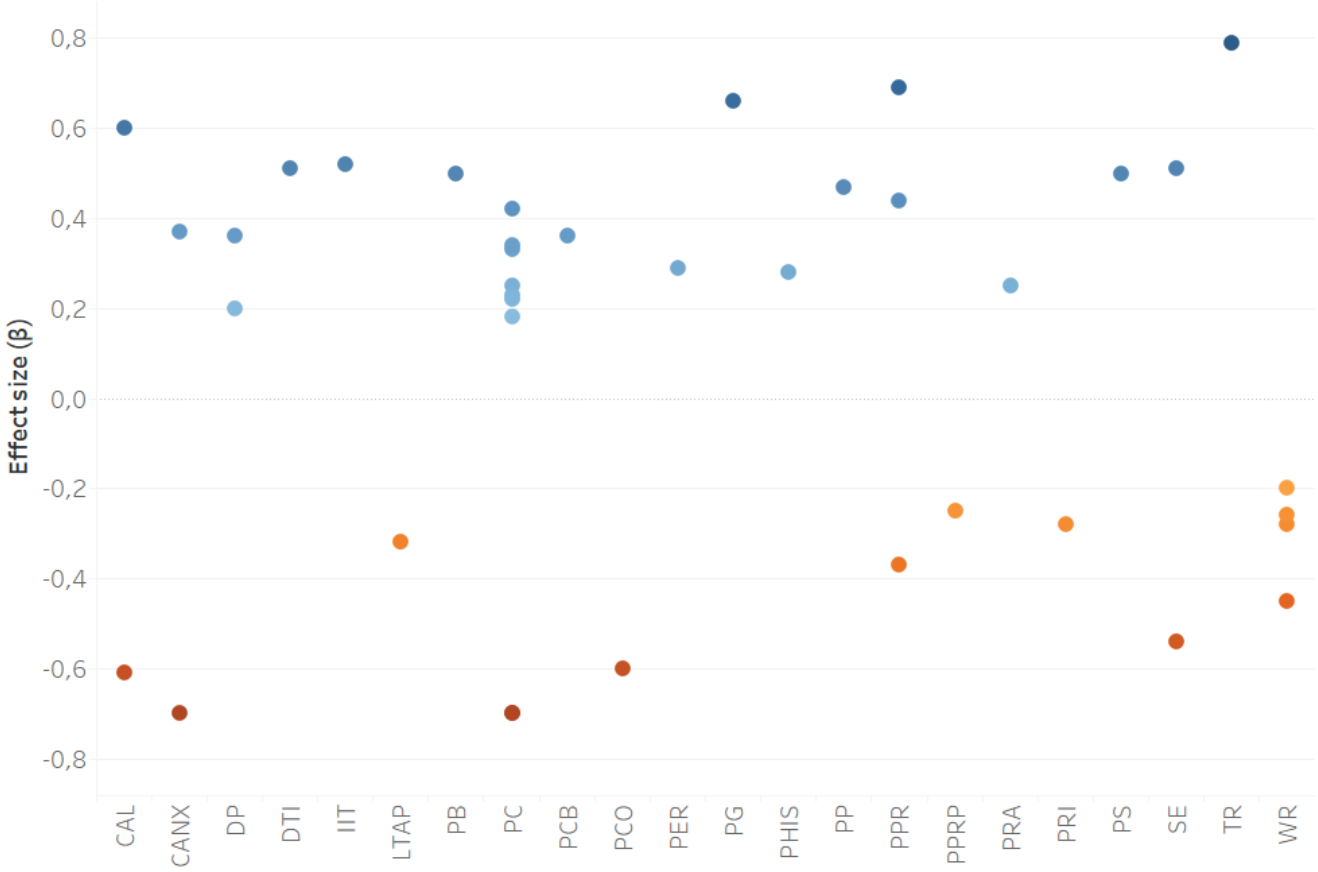

Figure 2: The effect sizes ≥0.25 reported in the included studies for privacy attitude, concerns and perceived risk.

Privacy Related Behavioral Intention and Willingness. The benefits someone can gain through data disclosure represent important predictors for a user's behavioral intention as well as willingness to disclose data, either in a general way ("perceived benefit/value', "perceived usefulness") or rather concrete ("liked targeted ads"). Regarding the user's individual characteristics, someone's need for consent and to what degree someone perceives oneself as similar to the subjective prototype of a user that discloses his/her data were found to be of most predictive power for intention and willingness to disclose data.

Although the identified effect sizes differ considerably across the considered studies, the trust a user has in a website significantly predicts his/her intention to share data with this website. This is in line with the significant predictive value of the user's privacy protection belief. Other important predictors for the behavioral intention are the level of (website, collection or general) privacy concerns, the perceived risk of data disclosure, the general attitude towards data sharing and willingness to share data. Nonetheless, it is noteworthy that willingness to disclose data only predicts 34% of the variance in behavioral intention.

General privacy concerns were found to be an even better predictor for willingness to disclose data than for behavioral intention. Important situational factors for the willingness to disclose data are the usage scope of the respective website, along with the retention period of the disclosed data (see fig. 3).

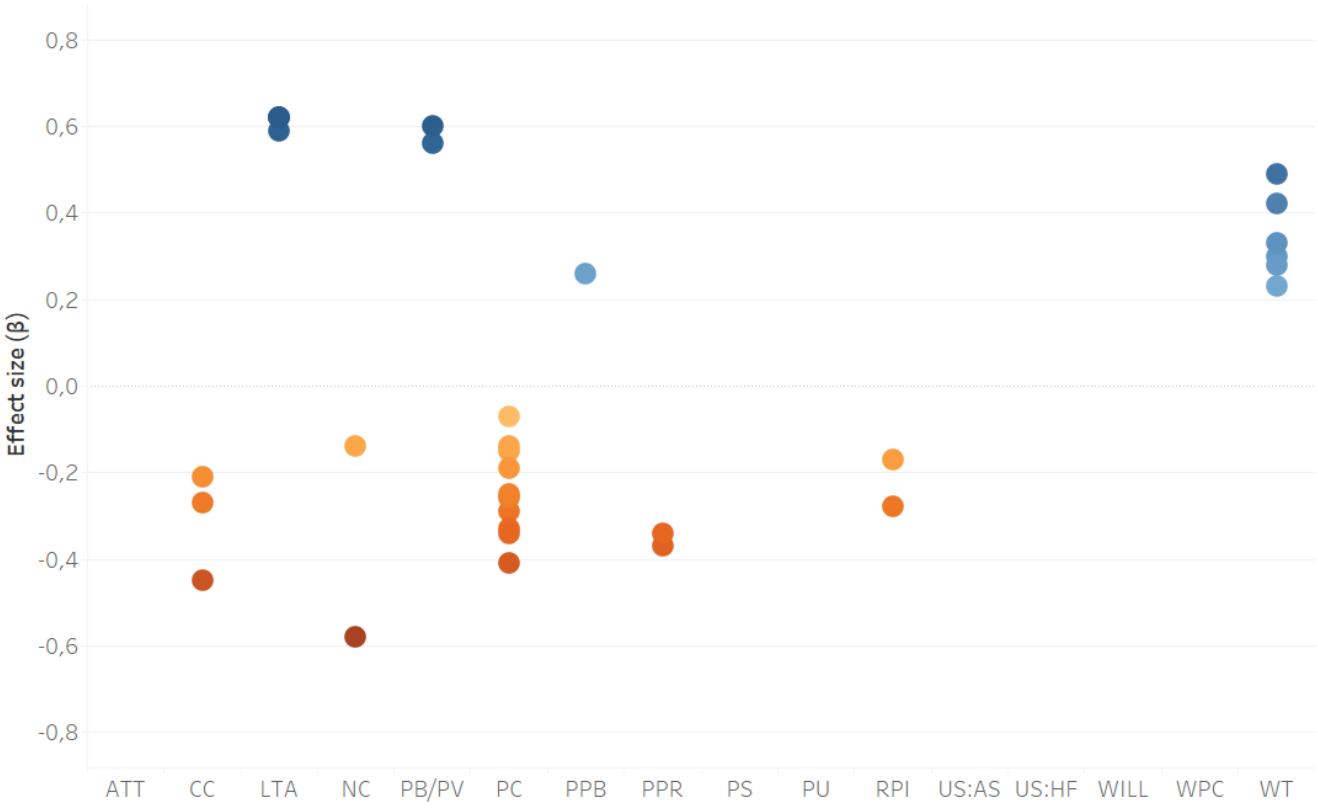

Figure 3: The effect sizes $\geq$ 0.25 reported in the included studies for privacy related behavioral intention and willingness.

Table 35: Main predictor variables for privacy attitude, concerns and perceived risk.

Predictor variable	Outcome variable	Effect size (β)
Trust (TR)	Attitude towards location-based mobile website	0.79**
(Information) Privacy concerns (PC)	Attitude towards information practice	-0.70***
	Privacy attitude	0.25*** to 0.42***
	Perceived privacy risk	0.18*** to 0.34***
Computer Anxiety (CANX)	Attitude towards information practice	-0.70***
	Privacy concerns (general)	0.37***
Perceived privacy risk (PPR)	Website privacy concerns	0.69**
	Privacy concerns (general)	0.44******
	Attitude towards location-based social network apps	-0.37***
Permission granted (PG)	Attitude towards information practice	0.66***
Perceived control (PCO)	Context specific privacy concerns	-0.60**
Consumer Alienation (CAL)	Attitude towards information practice	-0.61***
	Privacy concerns (general)	0.60***
Self-esteem (SE)	Privacy concerns (general)	-0.54***

Continued on next page

Table 35 – *Continued from previous page*

Predictor variable	Outcome variable	Effect size (β)
	Attitude towards information practice	0.51***
Interaction with IT (IIT)	Attitude towards information practice	0.52***
Data transfer internally (DTI)	Attitude towards information practice	0.51***
Perceived security (PS)	Attitude towards social network games	0.50***
Perceived benefit (PB)	Attitude towards location-based social network apps	0.50***
Perceived playfulness (PP)	Attitude towards social network games	0.47***
Website reputation (WR)	Website privacy concerns	-0.20** to -0.45**
Disposition to privacy (DP)	Privacy concerns (general)	0.36***
	Website privacy concerns	0.20*
Perceived career benefit (PCB)	Social Scientists' attitude towards data sharing	0.36***
Level of trust in the recipient's ability to protect data (LTAP)	Perceived privacy risk	-0.32***
Personalization (PER)	Perceived privacy risk	0.29**
Perceived relevance of information (PRI)	Perceived privacy risk	-0.28***
Perceived health information sensitivity (PHIS)	Health information privacy concern	0.28***
Perceived privacy regulatory protection (PPRP)	Perceived privacy risk	-0.25***
Privacy risk awareness (PRA)	Perceived privacy risk	0.25***

Table 36: Main predictor variables for privacy related behavioral intention and willingness.

Predictor variable	Outcome variable	Effect size (β)
Website trust (WT)	Intention to disclose information (general)	0.23** to 0.85***
	Intention to make Facebook data publicly accessible	0.28*** to 0.49***
Perceived benefit/ Perceived value (PB/PV)	Intention to disclose information on SNS	0.81***
	Willingness to disclose information	0.56** to 0.60**
Liked targeted ads (LTA)	Willingness to disclose information	0.59*** to 0.68***
Need for consent (NC)	Intention to make Facebook data publicly accessible	-0.14* to -0.58***
Retention period: indefinite (RPI)	Willingness to disclose information	-0.17* to -0.47***
Collection concerns (CC)	Intention to disclose data to an online retailer	-0.16* to -0.45***
Website privacy concern (WPC)	Intention to disclose information (general)	-0.43***

Continued on next page

Table 36 – *Continued from previous page*

Predictor variable	Outcome variable	Effect size (β)
Perceived privacy risk (PPR)	Intention to disclose information (general)	-0.34* to -0.42***
Privacy concern (PC)	Willingness to disclose information	-0.25*** to -0.41***
	Intention to disclose information (general)	-0.15* to -0.27***
Willingness (WILL)	Intention to disclose information on SNS	0.34***
Perceived usefulness (PU)	Willingness to disclose information	0.33***
Usage scope: health site and Facebook (US:HF)	Willingness to disclose information	-0.33***
Usage scope: all sites (US:AS)	Willingness to disclose information	-0.30***
Attitude (ATT)	Intention to disclose information on SNS	0.32***
Prototype similarity (PS)	Willingness to disclose information about peer relationships on Facebook	0.32***
Privacy protection belief (PPB)	Intention to disclose information (general)	0.19* to 0.26***

Information Disclosure Behavior. One of the most important predictors for actual data disclosure is the intention to disclose data, along with the general willingness to self-disclose. Concerns regarding data collection or privacy infringement were found to be of lesser, but still significant, importance for the prediction of disclosure behavior. Furthermore, other more or less privacy related behaviors like the number of used applications, the disclosure of basic information or the extend of mobile internet usage were found to predict disclosing behavior to some degree. Other significant predictors for disclosing behavior are the user's attitude towards the receiving application, the perceived entertainment benefits that can be gained through disclosure, the user's general awareness of ads and the perceived relevance of the social web in the user's social environment. Information disclosure behavior was further shown to be the only outcome variable that can be somewhat predicted by a demographic variable, with female users being more likely to disclose their data (see fig. 4).

Table 37: Main predictor variables for information disclosure behavior.

Predictor variable	Outcome variable	Effect size (β)
(Privacy) Intention (INT)	Information disclosure on SNS	0.65*** to 0.79***
	Teen information disclosure on social media	0.58***
	Usage of social network games	0.39*
General Willingness to Self-Disclose (WILL)	Information disclosure (general)	0.59***
Collection concerns (CC)	Disclosure towards a mobile app recommender	0.22*** to 0.46***
Attitude towards location-based social network application (ATT)	Location disclosure on location based-social network application	0.43***
Privacy concerns (PC)	Information disclosure on SNS + Information disclosure on SNS (breadth)	-0.43***

Continued on next page

Table 37 – *Continued from previous page*

Predictor variable	Outcome variable	Effect size (β)
Number of applications (NoA)	Information disclosure (general)	-0.35***
Benefits – entertainment (BEN-E)	Usage of a location sharing application	0.32***
Basic Information Disclosure (BID)	Teen information disclosure on social media	0.29***
Ads awareness (AA)	Information disclosure (general)	-0.28***
Social relevance (SR)	Information disclosure (general)	0.27***
Gender (GEN)	Information disclosure on SNS (depth)	-0.20** to -0.25**
Mobile internet usage (MIU)	Disclosure towards a mobile app recommender	0.15* to 0.25***

Protection Behavior and Privacy Settings. Whether users protective behavior, including the management of privacy settings in social networks is best predicted by their participation in risky interactions and their behavioral intention. The perceived social norms concerning specific privacy settings, the experience someone has with using the internet and the expressed privacy concerns are of mediocre predictive value (see fig. 5).

Table 38: Main predictor variables for protection behavior and privacy settings.

Predictor variable	Outcome variable	Effect size (β)
Risky interaction (RI)	Teenage privacy protection on SNS	0.44*** to 0.46***
Intention (INT)	Privacy settings on SNS	0.45***
Privacy (risk) concerns (PC)	Teenage privacy protection on SNS	0.10** to 0.36***
	Privacy settings on SNS	0.21** to 0.35**
	Privacy-Protective Behaviors	0.23***
Perceived norms regarding what to show only to friends (PN)	Privacy settings on SNS	0.31** to 0.33**
Years of internet experience (YIE)	Privacy-protective behaviors	0.21*** to 0.25***

Relationships Between the Main Predictor Variables. The relationships between the main predictor variables and the investigated outcome variables privacy attitude, concerns, perceived risk, behavioral intention and behavior found in the included studies are displayed in fig. 6-fig. 9. I categorized the main predictor variables and identified predictor variables that are related to the user's experience and demographics (fig. 6), the user's cognition (fig. 7), characteristics of the respective online service (fig. 8), and the user's privacy perceptions and beliefs (fig. 9).

2.4.2 Predictor Variables for Future Studies

Some path analyses did not achieve sufficient statistical power ($\geq$.8) to allow for a reliable decision about the investigated predictor variables. These predictor variables are thus interesting candidates for future studies. Whereas those variables that were found to have a significant predictive value in spite of insufficient power are marked by an "i.p." in the results section, potential predictor variables which failed to provide significant predictions are displayed in table 39-table 42.

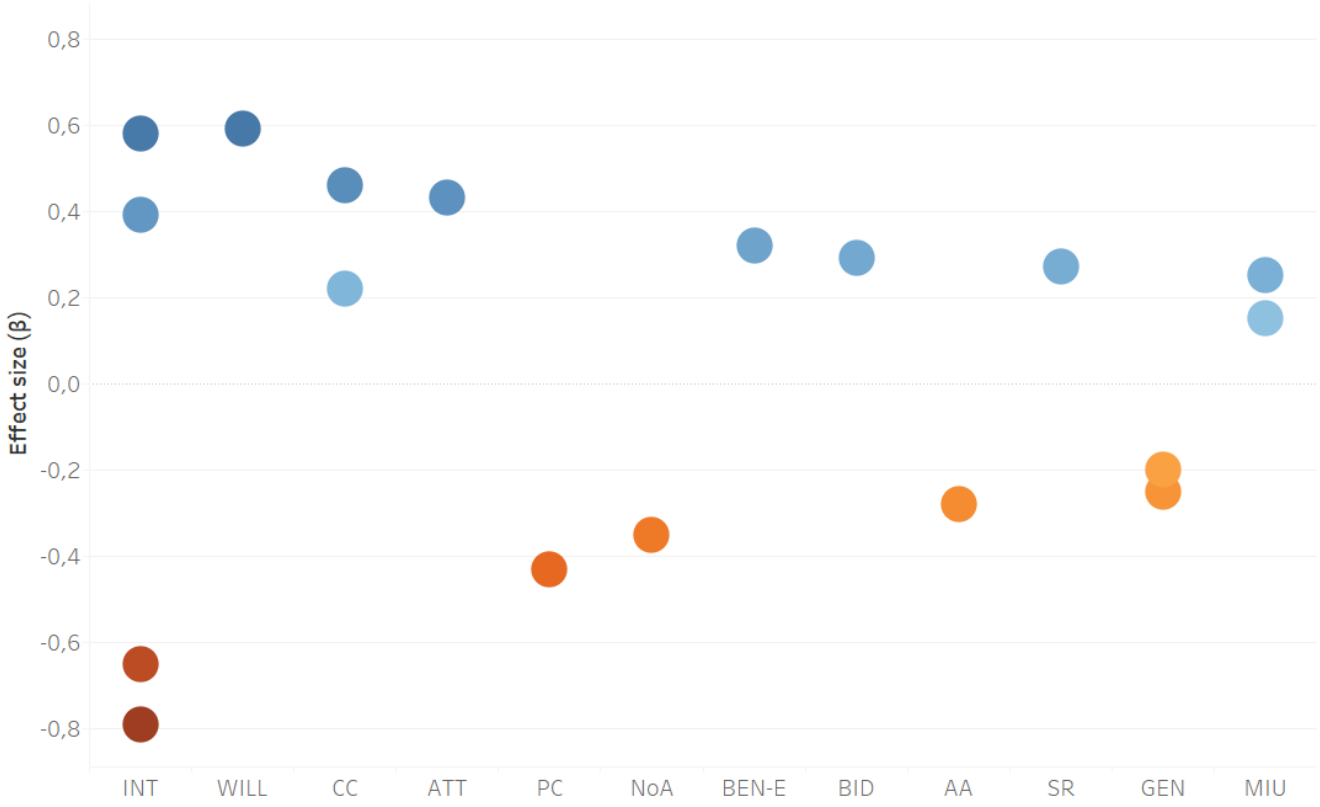

Figure 4: The effect sizes ≥ 0.25 reported in the included studies for information disclosure behavior.

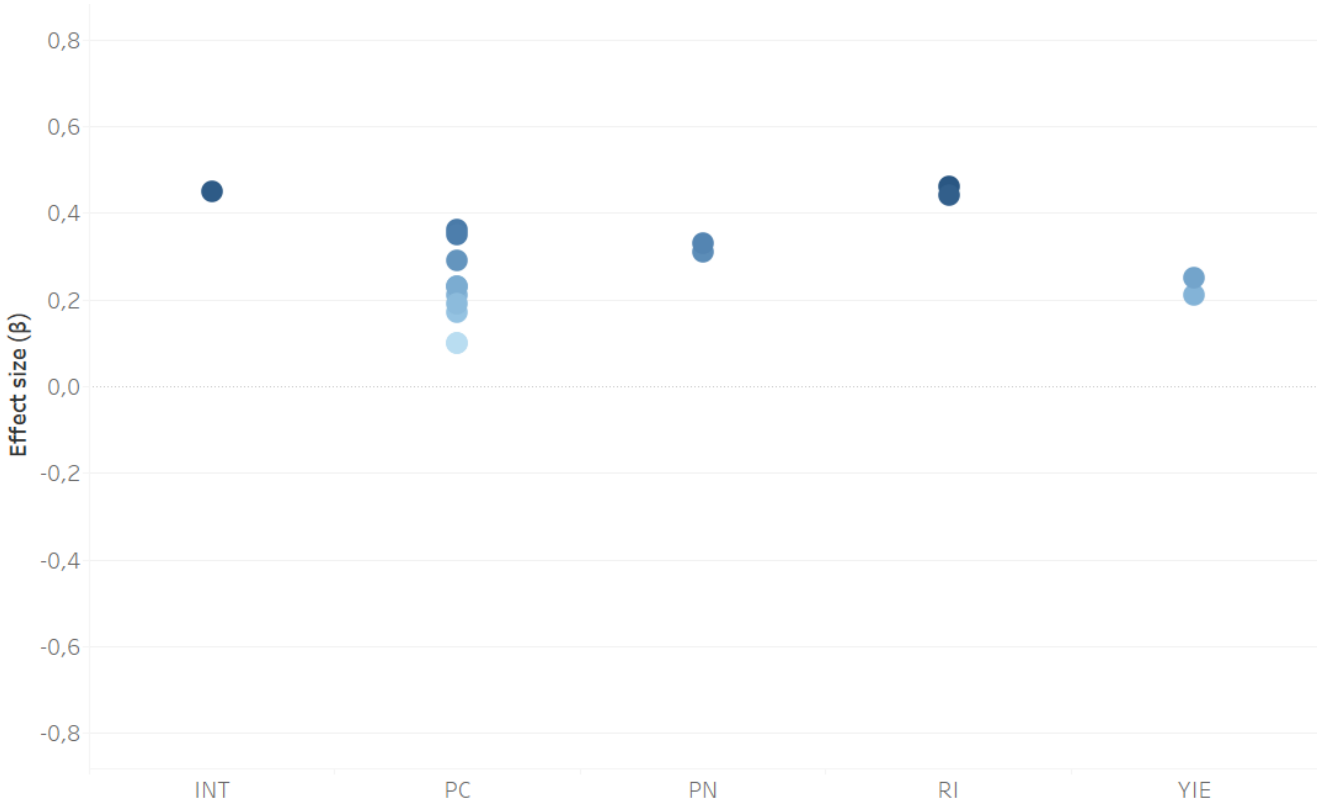

Figure 5: Main predictor variables for protection behavior and privacy settings.

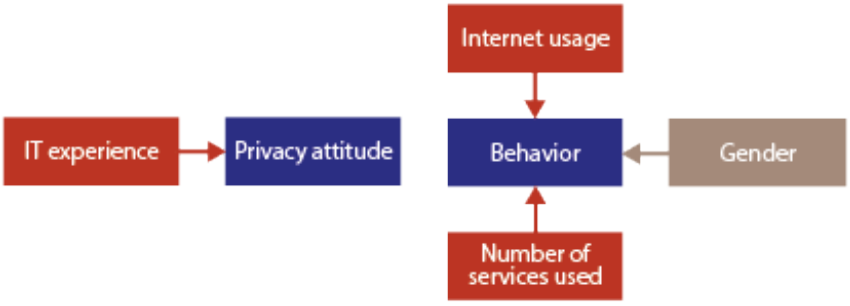

Figure 6: Relationship between main predictor variables and investigated outcome variables related to the user's experience and demographics.

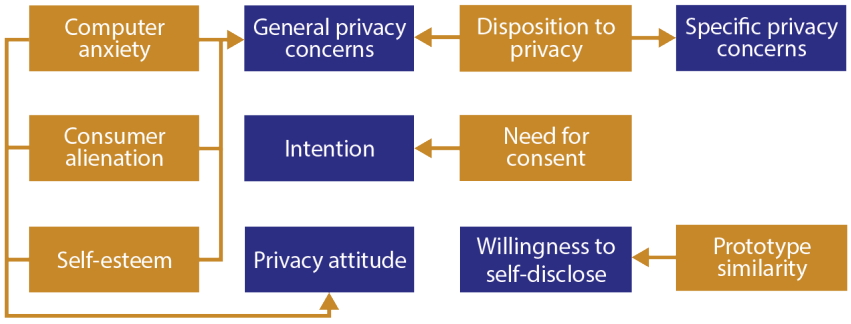

Figure 7: Relationship between main predictor variables and investigated outcome variables related to the user's cognition.

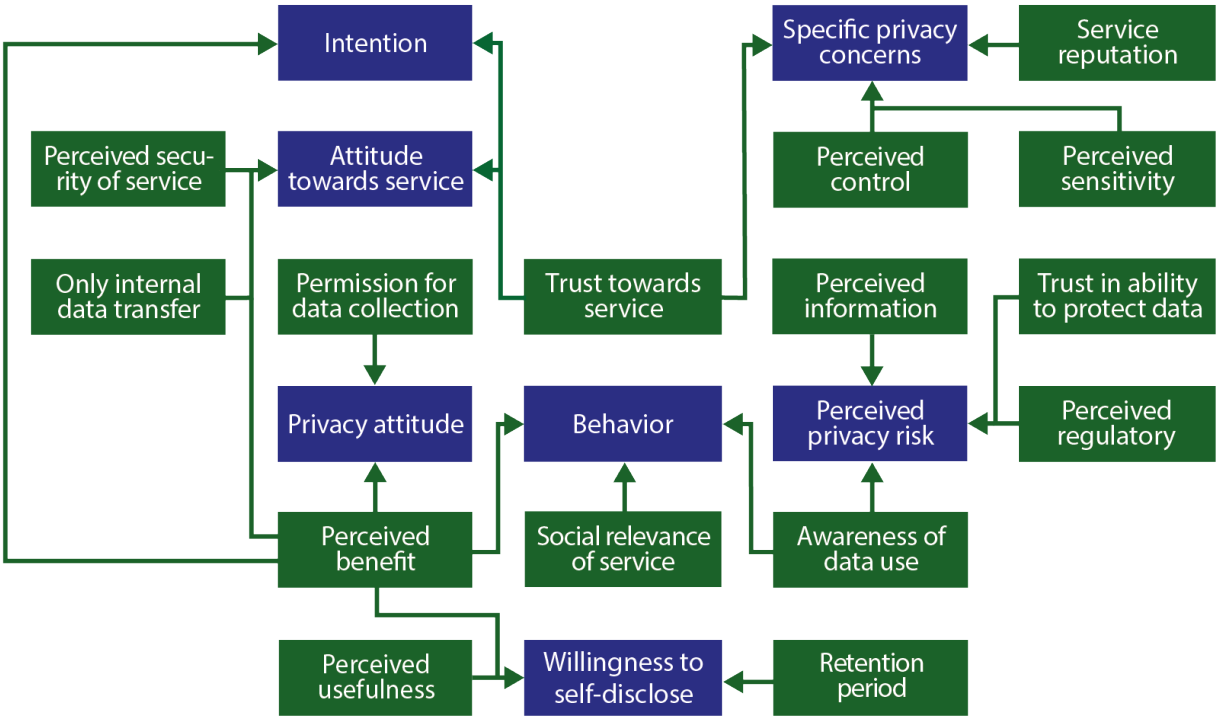

Figure 8: Relationship between main predictor variables and investigated outcome variables related to characteristics of the respective online service.

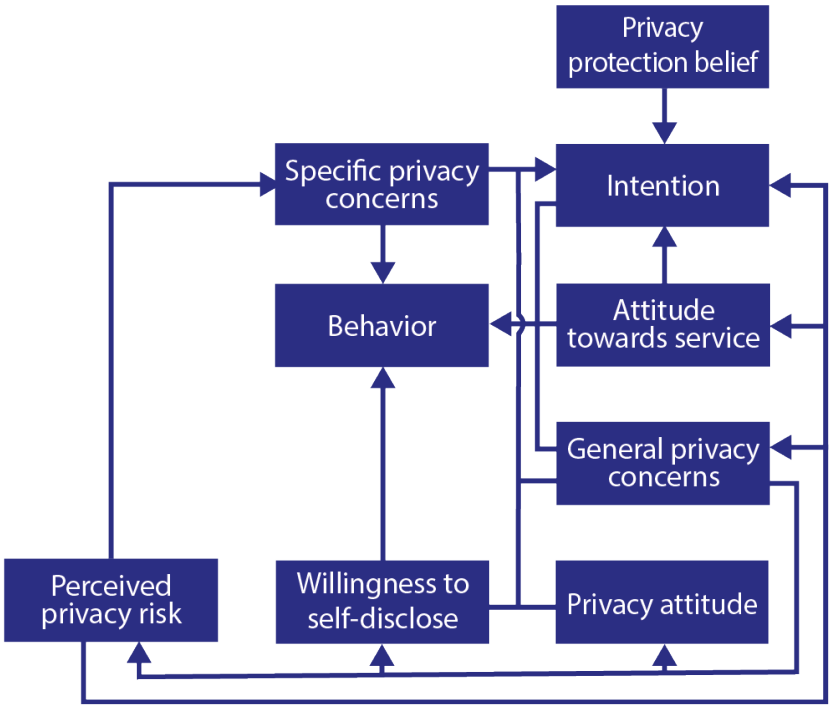

Figure 9: Relationship between main predictor variables and investigated outcome variables related to the user's privacy perceptions and beliefs.

Table 39: Predictor variables for privacy attitude, concerns and perceived risk lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/ required N
SNS complexity		Jia et al. [103]	
concern-centric model	Teenage Privacy Concerns on SNS		588/ 6,051
risk-centric model			588/ 10,433
Age		Jia et al. [103]	
concern-centric model	Teenage Privacy Concerns on SNS		588/ 1,325,882
risk-centric model			588/ 1,325,882
Gender		Jia et al. [103]	
concern-centric model	Teenage Privacy Concerns on SNS		588/ 11,430
risk-centric model			588/ 15,453
Basic Information Disclosure	Teenage Privacy Concerns on SNS	Jia et al. [103]	588/ 43,789
for sensitive information			588/ 52,994
Information sensitivity	Website Specific Privacy Concerns	Xu et al. [250]	171/ 20,468
Subjective norm	Website Specific Privacy Concerns	Xu et al. [250]	171/ 2,241
Perceived enjoyment	Attitude towards Social Network Games	Shin & Shin [204]	280/ 326
Perceived usefulness	Attitude towards Social Network Games	Shin & Shin [204]	280/ 192
Personalization			
for overt-based scenario	Perceived Privacy Risk	Xu et al. [253]	278/ 1,713
Previous privacy experience			
for overt-based scenario	Perceived Privacy Risk	Xu et al. [253]	278/ 1,257
General privacy concerns	Website Specific Privacy Concerns	Li [137]	110/ 962
Internet experience	General privacy concerns	Li [137]	110/ 362
Gender	General privacy concerns	Li [137]	110/ 362
Age	General privacy concerns	Li [137]	110/ 15,451
Education	General privacy concerns	Li [137]	110/ 1,713
Website familiarity			
for low reputation websites	Website Specific Privacy Concerns	Li [138]	110/ 143
Individual self-protection	Context Specific Privacy Concerns	Xu et al. [252]	178/ 1,257
Government legislation	Context Specific Privacy Concerns	Xu et al. [252]	178/ 759

Continued on next page

Table 39 – *Continued from previous page*

Predictor variable	Outcome variable	Primary study	Actual N/ required N
Age	Context Specific Privacy Concerns	Xu et al. [252]	178/ 61,827
Gender	Context Specific Privacy Concerns	Xu et al. [252]	178/ 15,451
Education	Context Specific Privacy Concerns	Xu et al. [252]	178/ 61,827
Desire for information control	Context Specific Privacy Concerns	Xu et al. [252]	178/ 962
Trust propensity	Context Specific Privacy Concerns	Xu et al. [252]	178/ 3,860
Awareness of privacy statement	Perceived Privacy Risk	Li et al. [134]	175/ 5,344
Internet literacy *for experienced shoppers*	General privacy concerns	Liao et al. [142]	259/ 614
Social awareness *for experienced shoppers*	General privacy concerns	Liao et al. [142]	259/ 425
Education	Perceived Privacy Risk	Baek & Kim [21]	2,028/ 6,865
Household income	Perceived Privacy Risk	Baek & Kim [21]	2,028/ 61,827
Liberal-conservative	Perceived Privacy Risk	Baek & Kim [21]	2,028/ 61,827
Internet use	Perceived Privacy Risk	Baek & Kim [21]	2,028/ 6,865
Online knowledge	Perceived Privacy Risk	Baek & Kim [21]	2,028/ 61,827
Paternalisitic personality	Perceived Privacy Risk	Baek & Kim [21]	2,028/ 2,469
Age	General privacy concerns	Abbas & Mesch [3]	567/ 1,038
Power disctance	General privacy concerns	Abbas & Mesch [3]	567/ 1,012
Uncertainty avoidance	General privacy concerns	Abbas & Mesch [3]	567/ 386,412
Trust in technology	Perceived Privacy Risk	Miltgen et al. [163]	326/ 1,222
Level of trust in the recipient's willingness to protect data	Perceived Privacy Risk	Beldad et al. [31]	208/ 507

Table 40: Predictor variables for privacy related behavioral intention and willingness lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
Coupon proneness			
for overt-based scenario	Willingness to disclose Information	Xu et al. [253]	278/ 3,860
Trust in website	General intention to disclose Information	Norberg et al. [167]	68/ 9,141
Negative affect	General intention to disclose Information	Wakefield [232]	
for high security websites			163/ 2,197
for low security websites			138/ 51,097
Positive affect	General intention to disclose Information	Wakefield [232]	
for low security websites			138/ 1,899
Privacy protection belief	General intention to disclose Information	Wakefield [232]	
for high security websites			138/ 298
Privacy concerns	General intention to disclose Information	Li [137]	110/ 61,827
Disposition to privacy	General intention to disclose Information	Li [137]	110/ 962
Age	Willingness to disclose Information	Leon et al. [133]	
for demographic information			2912/ 386,412
for location information			2912/ 96,604
Perceived privacy risk	Intention to Disclose Information on SNS	Xu et al. [250]	171/ 36,585
Information control	Intention to Disclose Information on SNS	Xu et al. [250]	171/ 171,740

Table 41: Predictor variables for information disclosure behavior lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
Privacy concerns	General Information Disclosure	Taddicken [220]	2,739/ 17,483
Website Specific Privacy Concerns	Basic Information Disclosure	Jia et al. [103]	588/ 43,789

Continued on next page

Table 41 – *Continued from previous page*

Predictor variable	Outcome variable	Primary study	Actual N/required N
for sensitive information			588/ 82,827
Ease of SNS Privacy Control	Basic Information Disclosure	Jia et al. [103]	588/ 23,529
for sensitive information			588/ 27,016
Age	Basic Information Disclosure	Jia et al. [103]	
for sensitive information			588/ 432,912
Gender	Basic Information Disclosure	Jia et al. [103]	588/ 432,912
Trust in website	General Information Disclosure	Norberg et al. [167]	68/ 51,097
Perceived privacy risk	General Information Disclosure	Norberg et al. [167]	68/ 3,049
Privacy concerns	Information disclosure	Dienlin & Trepte [57]	
for authentic first name			595/ 6,865
for authentic second name			595/ 1,257
for cell-phone number			595/ 15,451
political or religious views			595/ 1,553
frequency of posts on SNSs			595/ 1,713
Gender	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for insensitive information			588/ 759
for personal information			588/ 21,387
Age	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for insensitive information			588/ 1,772
for contact information			588/ 2,197
Parents' education	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for insensitive information			588/ 6,034
for personal information			588/ 3,339
Parents' race	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 1,604
for contact information			588/ 1,604
Hispanics	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 4,766
Household income	Teenage Information Disclosure on Social Media	Xie & Kang [248]	

Continued on next page

Table 41 – *Continued from previous page*

Predictor variable	Outcome variable	Primary study	Actual N/required N
for contact information			588/ 42,936
SNS use frequency	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for insensitive information			588/ 813
for contact information			588/ 2,794
Network size/ Number of friends	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 653
Having SNS friends that do go to school with the participant	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for insensitive information			588/ 1,772
for contact information			588/ 31,546
Having SNS friends that do not go to school with the participant	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for insensitive information			588/ 893
for contact information			588/ 7,347
Having family members as SNS friends	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 1,257
for contact information			588/ 1,459
Having strangers as SNS friends	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 31,546
Trust	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 1,967
Privacy settings	Teenage Information Disclosure on Social Media	Xie & Kang [248]	
for personal information			588/ 2,039
Facilitating conditions	Location Disclosure on Location-Based Social Network Application	Koohikamali et al. [120]	303/ 17,123
Information search	Usage of a Location Sharing Application	Beldad & Citra Kusumadewi [32]	655/ 1,713
Information dissemination	Usage of a Location Sharing Application	Beldad & Citra Kusumadewi [32]	655/ 2,469
Character-based trust in LSA	Usage of a Location Sharing Application	Beldad & Citra Kusumadewi [32]	655/ 6,865
Privacy concerns	General Information Disclosure	Taddicken [220]	2,739/ 17,483

Continued on next page

Table 41 – *Continued from previous page*

Predictor variable	Outcome variable	Primary study	Actual N/required N
Website Specific Privacy Concerns	Basic Information Disclosure	Jia et al. [103]	588/ 43,789
	for sensitive information		588/ 82,827
Ease of SNS Privacy Control	Basic Information Disclosure	Jia et al. [103]	588/ 23,529
	for sensitive information		588/ 27,016
Age	Basic Information Disclosure	Jia et al. [103]	
	for sensitive information		588/ 432,912
Gender	Basic Information Disclosure	Jia et al. [103]	588/ 432,912
Trust in website	General Information Disclosure	Norberg et al. [167]	68/ 51,097

Table 42: Predictor variables for protection behavior and privacy settings lacking statistical power.

Predictor variable	Outcome variable	Primary study	Actual N/required N
Education	Privacy-Protective Behaviors	Park [171]	
social behavior			419/ 1,066
Household income	Privacy-Protective Behaviors	Park [171]	
technical behavior			419/ 1,333
Marriage	Privacy-Protective Behaviors	Park [171]	
technical behavior			419/ 1,415
social behavior			419/ 5,673
Autonomy	Privacy-Protective Behaviors	Park [171]	
social behavior			419/ 3,501

2.4.3 Theoretical Implications of the Empirical Study Results

Regarding the previously proposed explanations for the privacy paradox (see section 2.2), some of the suggested variables were indeed strongly associated with the corresponding privacy constructs, whereas other variables were shown to be only weakly related to privacy attitude, concerns, perceived risk, behavioral intention or actual behavior.

Privacy Calculus. There definitely is some evidence for the privacy calculus model [119], with possible benefits the user can gain through data disclosure being among the best predictors for disclosing intention as well as actual disclosure. At the same time, users do not seem to consider possible benefits when reflecting about their privacy concerns. This is in line with the privacy calculus model, which describes the weighting of costs and gains only within the decision process about actual behavior.

Bounded Rationality & Decision Biases. Although there is no evidence for a strong relationship between the three privacy constructs attitude, behavioral intention and behavior and any of the variables describing a psychological bias [9, 119], at least optimism and affect were found to be mediocre predictors for protective behavior and behavioral intention, respectively.

Lack of Personal Experience and Protection Knowledge. Concerning technical knowledge and experience [57, 18] computer anxiety was found to predict privacy attitude very well and privacy concerns to some degree, whereas actual experience (e.g., number of used applications, mobile internet usage, years of experience with using the internet) significantly predicts actual privacy behavior. Surprisingly, the study results suggest that prior experience with privacy infringements actually does not serve as a good predictor for privacy attitude, behavior or behavioral intention. However, it could be possible that the considered studies did not include enough participants who had actually experienced a serious infringement of their privacy in the past, leading to a lack of statistical power for that factor. Hence, further research is needed to investigate the potential influence of prior experiences with privacy infringement.

Social Influence. Mainly behavior (disclosure and protection) was found to be predicted through social factors like the perceived social norm of what information should be only shared with friends and the social relevance of social networks. This is in line with the proposed influence of social factors [119, 220], on especially actual behavior, for behavior being the only variable that can actually be observed by the user's social environment.

The Risk and Trust Model. There is only partial support for the risk and trust model [72, 163]: The perceived privacy risk is indeed one of the best predictors for privacy concerns, whereas the user's trust in the recipient's ability to protect his/her data serves as a rather mediocre predictor. Conversely, trust in a location-based mobile website was found to be an excellent predictor for the user's attitude towards that website. Additionally, trust is of major significance for the prediction of the behavioral intention, at least according to some of the study results. Perceived risk was also found to predict behavioral intention to some extent. However, neither risk nor trust were a significant predictor for actual privacy behavior, contradictory to the proposed model, which suggests trust to be a significant predictor for privacy behavior. The importance of trust for the prediction of the user's behavioral intention and attitude does not exactly fit to the proposed model either. Therefore, further research is needed to clarify the interplay of risk and trust on the one side and privacy attitude or concerns, behavioral intention and behavior on the other side.

Illusion of Control. To what extend the user feels in control about the disclosure and processing of his/her personal data [36] significantly predicts his/her privacy concerns, but there is no evidence for a significant relationship of perceived control and behavioral intention or behavior. However, only few of the considered studies investigated the influence of perceived control, so the lack of empirical evidence could be probably caused by the lack of empirical studies in the first place.

Quantum Theory and the Privacy Paradox as Methodological Artefact. There are also few studies dealing with quantum theory or the privacy paradox as methodological artefact, apart from the research introduced in section 2.3. Again, further studies are needed to decide about the adequacy of the proposed models and explanations. However, the results implicate that researchers should indeed distinguish between privacy attitude and privacy concerns, as proposed by Dienlin and Trepte [57].

2.4.4 Limitations

Although a first step towards understanding the complex construct of privacy behavior and attitude, the present study suffers from several limitations. First, the literature search that forms the basis of this review was not exhaustive and thus presents only a first step towards understanding which variables are most relevant for the prediction of privacy attitude and behavior. Further systematic reviews are needed to gain a more comprehensive picture of the complex phenomenon "user privacy". Also, the underlying body of literature might suffer from publication bias, due to the general tendency in research to preferably publish positive or significant results, compared to negative or insignificant results. This should be kept in mind when interpreting the results or planning user studies on its basis. Furthermore, I focused on quantitative results drawn from survey studies using regression analysis and structural equation modeling,

thereby omitting findings not only from qualitative research, but also from quantitative experimental studies which used other analyses methods, e.g., analysis of variance. It would be interesting to compare the findings from these research approaches with the present results. Last, I did not account for differences in the quality or representativeness of the receptive studies. Future reviews could for example weigh the particular effect sizes based on study quality.

2.4.5 Conclusion

Since the behavioral intention was found to be one of the main drivers for privacy protection behavior, a promising approach would be to focus on enhancing this behavioral intention to protect one's privacy. Behavioral intention, on the other hand, was found to be best predicted by service-specific characteristics and the user's privacy concerns or perceived risk, respectively. A first step would thus be to raise lay users' awareness of privacy issues, e.g., through privacy awareness campaigns or messages.
A third factor for the user's privacy intention relates to social considerations. Another possible approach could therefore be to emphasize restrictive social privacy norms of peers and family members or focus on groups of users to collectively enhance their privacy behavior instead of individuals. However, the users' intention to protect their privacy can only result in successful protection behavior if they also know how to protect themselves. Hence, it is important to provide them with knowledge of and the ability to use protection solutions as well.
However, privacy researchers and developers should not only aim to implement factors related to privacy protective behavior. It would also be worthwhile to take a closer look at the factors that prevent privacy friendly behavior, for example whether the user strives for certain benefits or discloses data for a certain purpose like impression management. Privacy friendly alternatives need to provide the same core functionalities the users value on the original products (e.g., gained benefits and possibility for impression management) or only a small part of users will trade their familiar products for privacy friendly ones in the long run.
I will thus focus on these three aspects in the next chapter.

3 Factors That are Important for Users' Decision to Protect Their Digital Privacy[7]

The results presented in chapter 2 suggest that the perceived privacy risk, the knowledge of and ability to use protection solutions, and the benefits people gain by using privacy-threatening devices are among the most relevant factors that affect whether people choose to protect their privacy. Whereas chapter 2 only considers quantitative results from survey or laboratory studies, the research described in this chapter takes a closer look at the three identified factors from a qualitative point of view. I conducted semi-structured interviews with 24 lay users for this purpose.
In the following, I will liberally use quotations from my article published in "Proceedings of the 4th European Workshop on Usable Security (EuroUSEC)" (2019) without explicitly marking each quote.

3.1 Related Work

This work relates to people's mental models of privacy consequences, obstacles for privacy protection, including reasons for continuing to use privacy-threatening devices and services, and strategies people apply to protect their privacy.

3.1.1 Mental Models of Privacy Consequences

There are many surveys assessing how people perceive different privacy risks, however, most of them present a set of risks and ask participants to rate their degree of concerns on a scale [170, 191, 77, 65]. This approach is not sufficient to measure whether people are actually aware of these privacy risks without prompting them. Among the few who deployed a different approach are Harbach, Fahl and Smith [91], who asked German students and members of Amazon Mechanical Turk to name IT security and privacy risks and consequences in a survey. They found that participants usually overestimated the amount of risks they were aware of. This is in line with other studies, e.g., interviews conducted by Wash [237], which indicate that people are often not aware of threats and hence underestimate dangers. The consequence most frequently provided by both groups of participants in Harbach et al.'s study was financial loss, whereas the most salient risks were malware, hackers and the theft of account credentials.
The most comprehensive approach to accessing people's awareness of privacy consequences was conducted by Karwatzki et al. [108], who ran a total of 22 focus groups in which they asked their participants directly to name all privacy consequences they are aware of. The authors derive seven categories of privacy consequences based on the responses: physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences. Albeit providing valuable insights on people's awareness of privacy consequences, Karwatzki et al. do not report the frequency of consequences mentioned in the different categories. Moreover, their participants mostly referred to consequences that could arise from using OSN. It is thus questionable which of their findings are application-specific and which generalize to other online services and technologies.
Other examples of assessing people's awareness of privacy risks are interviews conducted by Friedman et al. [74], who found that people were concerned about risks to their information and especially their privacy, but did not further specify these privacy risks, a survey on security and privacy risks of eHealth wearables [33], interviews combined with a field study concerning the risks of WiFi use [116], a comprehensive study on user regrets regarding Facebook posts [235], a survey assessing perceived risks of using mobile devices to conduct online transactions [226], and surveys and interviews concerning risks of cloud storage [47]. Shirazi and Volkamer [205] conducted interviews with 20 people on identification and tracking on the web, and found that their participants most often mentioned personalized advertising as a possible consequence, which some of them even considered to be beneficial. Melicher et al. [159] found that participants in their interview study were less comfortable with hidden outcomes of online tracking (e.g., price discrimination) than with more overt consequences (e.g., targeted advertisement). Although investigating specific privacy risks, Melicher et al. focused on online tracking and thus considered mainly risks specific to this application.

[7] based on the paper "Nina Gerber, Verena Zimmermann, and Melanie Volkamer. Why Johnny Fails to Protect his Privacy. In: Proceedings of the 4th European Workshop on Usable Security (EuroUSEC). IEEE, 2019." [84]

3.1.2 Strategies for Protecting One's Privacy

Several studies have been conducted on how people protect their privacy by deploying a set of strategies. Most of these studies focus on a particular context, e.g., managing photos which are shared with other people [217], managing privacy in OSN in general [244, 216] or with respect to others revealing information about oneself [125], or when using WiFi [116]. Other studies describe strategies people deploy to address specific problems, e.g., identity theft [161], or online harassment [153]. Further, there are also studies dealing with a specific protection strategy, like webcam covering [151], or lying for privacy reasons [190].
A few studies focus on the general deployment of privacy protection strategies. Oomen and Leenes [170] differ between three sets of privacy protection strategies: (1) behavioral, such as providing incorrect information, using anonymous email addresses or pseudonyms, (2) employment of security measures and use of PETs, such as spam filters, firewalls, and anti spyware, and (3) use of more advanced PETs, such as encryption tools, anonymous remailers, trust certificates, and cookie crunchers. In a survey with Dutch students, they found that about half of their participants employed behavioral protection strategies, whereas the majority (between 74 and 89%) took standard security measures and used PETs, and about a third used some of the more advanced protection strategies, with trust certificates being the most (31%) and anonymisers (3%) the least frequently used.
In a lab study with corresponding interviews, Coles-Kemp and Kani-Zabihi [49] found that in an online registration task, when participants where not comfortable providing their information, most of them chose to give false information, discontinue with the registration or continue the registration and provide accurate information, but reduce their engagement with the service. In their interview study, Abu-Salma et al. [4] also asked their participants about strategies they applied if they wanted to protect their communication data. The most common strategy was to deliver sensitive information in person, or using video-chat and voice-mails if a personal meeting was not possible. Other practices include sending information by post, using a foreign language for voice messages, and cutting a message into several chunks which were then send via different communication channels. Some participants also reported to use a "code" to exchange sensitive information with others, regardless of the communication channel used.
A number of studies have dealt with the deployment of different privacy protection strategies by Facebook users. Young and Quan-Haase [254] found that university students mainly adopted privacy protection strategies that restricted access to their personal data for different members of the Facebook community, rather than strategies that would allow them to control data access for third parties. Furthermore, they showed that university students do not use fictitious information as protection strategy, since this would lead to confusion among friends and peers. Another study by Staddon, Acquisti and LeFevre [212] showed that users who value privacy features most generally show more privacy actions such as not providing certain information, limiting post visibility or deleting posts. Concerning cultural differences, the results of Peters, Winschiers-Theophilus and Mennecke [174] indicate that US users would rather remove friends from their contact list than change their privacy settings to restrict the visibility of their data, whereas Namibian users refuse from the deletion of friends due to the concern of being rude. When it comes to teenagers, Feng and Xie [69] found that older teenagers tend to implement more privacy protection strategies (e.g., deleting someone from their friends list, deleting older posts), whereas Litt [148] showed that younger adults are more likely to show a wider use of technological privacy tools than older adults, maybe due to greater knowledge of and skills in using these technologies. Using interviews, user diaries and surveys, Wang et al. [235] identified three different sets of protection strategies, namely proactive (e.g., rejecting friend requests, managing privacy settings), in-situ (e.g., self-censoring), and reactive (e.g., deleting content, untagging photos), with the last being the most frequently used strategy in their study.

3.1.3 Obstacles for Privacy Protection

A few qualitative studies have been conducted on what obstacles users face when aiming to protect their privacy in several contexts. Shirazi and Volkamer [205], for example, conducted interviews with 20 people, most of them lay users, to investigate why most people do not use tools to protect themselves against

identification and tracking on the web. They identified seven different explanations: (1) people mainly worry about privacy issues other than identification and tracking, (2) people are not aware of the assessment of meta-data, (3) people are not aware of the possibility to use meta-data for identification and tracking, (4) people are not concerned because of several misconceptions such as being not aware of consequences or the feeling that they have nothing to hide, (5) people are not aware of protection tools, (6) people are not able to use protection tools properly, (7) people become side-tracked. Renaud, Volkamer and Renkema-Padmos [183] combined semi-structured interviews, a survey, and a literature review to identify obstacles to the adoption of end-to-end (E2E) encrypted email. Their final list of seven explanations includes lack of awareness, concern, and knowledge about how to protect oneself, as well as misconceptions of how to protect oneself, no perceived need to act, inability to use E2E encryption and becoming side-tracked. In a more recent study, Abu-Salma et al. [4] interviewed sixty users of different communication tools to identify factors that influence the adoption of secure messaging tools. Like Renaud et al. [183], they found that usability is not the major obstacle for the adoption of secure communication tools. In the messaging context, other factors like fragmented user bases, along with interoperability of the different messaging services are significant adoption obstacles. Participants also reported not to use a communication tool if they evaluate its message and voice call functionality to be of low quality.

3.2 Methodology

I conducted an exploratory study consisting of semi-structured interviews with 24 participants and subsequent qualitative analysis to further evaluate perceived privacy risk, the knowledge of and ability to use protection solutions, and the benefits people gain by using privacy-threatening devices. The interviews were conducted in German, questions and quotations were translated for this chapter.

3.2.1 Research Questions

The first factor considered in this study is the perceived privacy risk, which has been shown to be a good predictor for people's intention to share or protect their private data, respectively. In line with this, it has been argued that people simply lack awareness of privacy risks which leads to their unconcerned handling of private data [76]. Risk perception is usually defined as the perceived probability of adverse consequences and the perceived severity of those [227, 150]. This is also in line with threat avoidance theory, which states that in order to be motivated to avoid a threat in the IT context, people have to perceive this threat as malicious, i.e., that they are susceptible to this threat and that the negative consequences will be severe [140]. Hence, people's risk perception should depend on their awareness of possible adverse consequences resulting from sharing and not protecting their private data and my first research question for the interview study thus is:

RQ2a: What are people's mental models of possible consequences arising from sharing and not protecting their private data?

The second factor describes the knowledge of and ability to use privacy protection solutions. This factor addresses the fact that even if people are aware of privacy problems and motivated to encounter them, they could fail to do so because they lack knowledge about protection mechanisms (e.g., the Tor software or encryption tools) [20] or they suffer from an "illusion of control" when dealing with the privacy of their data [36]. In line with that, prior studies showed that people indeed seem to confuse the control over the publication of information with the control over the assessment of that information by third parties. According to this hypothesis, the paradoxical behavior is caused by the false feeling of control over the further usage of personal data, which occurs if users can initially decide over the publication of it (e.g., by posting in online social networks and managing the privacy settings for the post). Hence, to investigate whether users simply lack knowledge about possible protection solutions or whether they apply strategies which are not effective but mainly make them feel like they have control over their data, I propose the

second research question for the interview study as follows:

RQ3a: What strategies do people apply to protect their data?

The third factor focuses on what prevents people from protecting their privacy. One of the most popular explanations for the privacy paradox, which has further gained substantial support by the quantitative results described in chapter 2, the "privacy calculus" [128], also describes the weighting up of costs and benefits of privacy protection. I therefore aim to gain an understanding of what users consider to be the costs of privacy protection and benefits of using privacy-threatening devices and services by answering the following research question:

RQ4a: What are obstacles for privacy protection and for what reasons do people still use privacy-threatening devices and services?

3.2.2 Recruitment and Participants

I aimed for a heterogeneous sample, i.e., interviewing people with different professional and sociodemographical backgrounds, experiences, and expertise regarding online privacy. Therefore, I asked my student research assistants to invite friends and family members of whom they thought would be interested in participating in this study. These were then contacted to make an appointment without telling them about the research topic. Instead, they were told the interviews would focus on their "use of digital applications". Additionally, I sent a corresponding invitation email via the mailing list used to advertise studies among the university's undergraduate psychology students. I proceeded to recruit new participants until data saturation was reached, i.e., there came no new themes up during the interviews. Undergraduate students received course credits for participating, however, non-student participants did not receive any compensation but participated voluntarily.
The interview group consisted of 24 participants (15 female, 9 male). Participants ranged between 17 and 53 years of age (M=26.29, SD=6.90). Nineteen participants were students, the other five participants' professional backgrounds included online journalist, event manager, office clerk, media manager, and researcher. None of the participants had a professional background in the computer sciences.
I conducted several pilot interviews to check the soundness of the questions and structure of the interview guidelines. Based on the feedback of the participants and my own impression during these pilot interviews, I improved the interview guidelines iteratively.

3.2.3 Study Procedure

The interview guidelines can be found at Appendix B. The interviews took between 27 and 91 minutes, with an average of 48, and comprised the following sections:
Welcome and general instructions. First, participants were welcomed and informed about the study procedure and purpose[8]. They were further informed about the study conditions (see section 3.2.5) and asked whether they consented to the recording of their interview.
Use of Digital Communication Channels. In the first part of the interview, participants were asked to explain how they used technology, i.e., hard- and software, to communicate with other people. I did not ask actively about privacy, but if participants mentioned privacy-related issues on their own, I encouraged them to explain these in more detail.
Use of Privacy-Relevant Applications and Services. Afterwards, I asked participants whether they used (and if yes, which) OSN, messengers, navigation apps, shopping apps, cloud services, online banking, electronic pay services, loyalty programs, digital assistants, and game consoles. I further asked whether

[8] Note that in order not to bias participants towards privacy, they were told that the interview topic would be their use of digital applications instead of telling them I was interested in their privacy beliefs and behavior.

they owned a smart TV and whether they had already gotten the new version of the German ID card. Again, I did not ask about privacy issues actively, but encouraged participants to talk about their privacy beliefs if they had mentioned them first. Where applicable, I asked participants to justify their decisions not to use certain applications or products.

Data Privacy Attitude and Behavior. The final part focused on participants' privacy beliefs and behavior. I asked them about their attitude towards data privacy, what their social and professional environment thought about data privacy, how they experienced the media coverage of this topic and what they thought about personalized services like Amazon's product recommendations. They were asked to explain which negative consequences could possibly arise from data sharing and whether they had already experienced such consequences in the past.

3.2.4 Evaluation Methodology

I used open coding [215, 214] for the analysis to account for the exploratory nature of our study. Thus, I was able to only consider such themes and issues that were highly relevant for the participants, which had not been possible by using pre-defined codings. The analysis was done by me and another researcher to ensure the quality of the codings. First, we reviewed the transcripts and audio files to identify relevant themes and sub-categories from the participants' responses. Our final codebook included four meta themes and 31 sub-categories. Based on these, we independently coded all transcripts. Differences in the coding were solved through discussion afterwards. I report the number of participants who mentioned a theme or sub-category in the following section. Where applicable, I add (translated) quotes.

3.2.5 Ethical Considerations

Ethical requirements for research involving human participants are provided by an ethics commission at the Technische Universität Darmstadt. All relevant ethical requirements regarding research with personal data were met. Participants were first informed about the procedure of the study, after which they could decide to proceed or stop the interview. They were further told that they could stop the interview at any time without stating reasons and in this case all data collected so far would be deleted. I further assured them that the collected data would only be used for research purposes, their identity would not be linked to their responses, and their data would only be handled by members of my research group and never passed on to third parties.

3.3 Results

In this section, the results of the data analysis are presented. RQ2a is addressed in section 3.3.1, RQ3a in section 3.3.2, and RQ4a in section 3.3.3. Section 3.3.4 describes additional findings about common privacy misconceptions. Where applicable, I provide the corresponding number of participants who made a statement and add the quotes from the participants that I translated from German.

3.3.1 Mental Model of Privacy Consequences

A few participants (7) thought even if they provided all their data, nothing bad would happen at all: "Well, many people are pretty skeptical and say they don't want to be under surveillance in any case [...] and make a huge scandal out of it. I can't really understand why...on the one hand I think I feel a bit...almost threatened, if some data of me is found, but then I have...because at the moment I lack the idea of how you could use this against me, that's why." (P9)

Personalized Advertisement. Almost all participants (20) mentioned that they would be shown or sent personalized advertisement as a possible consequence of disclosing data. Most participants did not like the idea of receiving personalized ads, but did not worry too much about it. A few participants, however, reported to look favorable upon being shown personalized ads: "And of course it's in my interest to get advertisement for products I'm potentially interested in and not just for ladies' underwear [...] I think it's a good thing it's tailored to me, since I'm actually interested in the products that I am shown." (P19).

Financial Loss. About half of the participants (12) talked about financial loss as a consequence of disclosing data, particularly banking details. Whereas some participants were mainly worried about passwords to their online banking accounts, others were concerned about their IBANs as well because they were not sure if it was possible to use this to debit money: "I am always...I don't know if that works, but if somebody could debit a sum just having your IBAN, that would actually be the fear. But I don't know if that would really work." (P7)

Job Applications. A few participants (8) stated to be worried about a potential future employer getting access to their postings on social media and thus limiting their chances of getting a job they had applied to: "[...] when you provide your actual data and start posting things which are rather less favorable in terms of employers being able to find you easily and see what a person you are socially, if you are trustworthy or not...and that could easily backfire." (P4)

Safety Threats. A few participants (7) were worried about becoming victims of harassment or stalking due to disclosure of their current location: "[...] that somebody shows up at your home and bothers you" (P7)

Spam Mails. A few participants (6) were worried about receiving spam mails if their email address got disclosed.

Identity Theft. A few participants (6) mentioned the risk of identity theft, either as an abstract threat: "Maybe somehow on the Internet, a doppelganger, e.g., that someone collects every information about me and somehow creates a new identity, which then is another me." (P7) or with regard to specific actions, like financial transactions, crime commitment or social interaction: "[...] that criminals could possibly take your identity to buy things or commit crimes and so on." (P3)

Exposure. Few participants (6) thought data disclosure could result in being exposed because they had done something they did not want their friends and family to know about: "[...] because there could be data that I would be embarrassed of if friends would find out about it. Because I suppose they wouldn't approve of certain behaviors or because I suppose they would make fun about it, if they'd know it." (P1)

Criminal Prosecution. The few participants (5) who talked about the possibility of being criminally prosecuted mostly stated that only people committing crimes should be worried about this: "If I'd be a criminal. Then there would be information about me. Either where I am, what I buy, whom I contact. That I don't want to become public. But that does not apply in my case. I don't care who knows where I am at what time, how much I bought." (P2)

Political Prosecution. Few participants (5) talked about possible consequences that could result from governmental surveillance. Those who did mostly stated to trust the current German government, but were concerned about possible implications regarding future governments: "Many people say they don't give a damn whether someone eavesdrops on them, why should someone care about their issues. But overall, I think that's not quite that simple. We currently live in a democracy, the constitutional state works in that our personal rights are protected rather well - so far. But that could change one day and if the government can access all communication channels then it could exploit this." (P8)

Monopolization. A few participants (5) expressed concerns about the monopoly of certain organizations through control over a great amount of consumer data: "And I think we are disclosing more and more about ourselves due to reasons of security or convenience and hence, certain organizations are getting more and more powerful, and those may dictate us a lot of things in the future. [...] And organizations are not always interested in the common welfare, but in their own profits and if they have such a great power they could use this to restrict our freedom one day." (P3)

Data Abuse. Few participants (4) were worried about the unintended use of their data: "That happened to some comedian, the AfD [german political party] canvassed with his photo. That's...that can be misused. [...] And suddenly you appear as a dessous model in the US and have never heard about that before." (P11)

Burglary. Only very few participants (3) talked about burglary as a potential risk of disclosing one's location data. Those who did, however, rated the risk as rather low.

Propaganda. Very few participants (2) reported to be worried about their data being used to influence their opinion in some way. Statements concerning this topic mainly referred to the recent US election: "Um, recently in the US elections the way the Republicans run their election campaign and there was a media report about it. About an analytic software, how you categorize certain groups of people. To break it down, they knew which people they should address and what would be reasonable, what groups of people should be addressed to suceed with the election campaign." (P8)

Less Favorable Insurance Tariffs. Location and health data were mentioned by very few participants (2) in association with the risk to get a less favorable health insurance tariff: "Or, if we're getting on with these fitness and health trackers that store various data, that, e.g., a health insurance company could say 'Well, we saw via your app or fitness tracker that you don't work out very much. No wonder you're sick now, that's your own fault. We're not paying you anything."' (P3)

Not Being Granted a Credit. Only one participant mentioned the possibility of being refused a credit: "Well then, it could be possible that not just the employer uses the data, but also banks if they grant credits. That they can access what you bought at Rewe [a German supermarket] in the past and then infer from this you're not able to handle money well and then refuse to grant you the crucial credit." (P1)

3.3.2 Protection Strategies

Most of the strategies participants described to deploy for protecting their data relied on reducing data disclosure, either by not using certain services, not sharing certain data or limiting the amount of recipients. Some participants, however, also reported to actively provide false or misleading information to "confuse the system".

Refrain From Using Services that Could Infringe Upon One's Privacy. Some participants (8) deliberately decided not to use certain services to prevent these from accessing their data. The list of these "critical" services does not only comprise apps demanding extensive permissions and OSN, but also game consoles, Google's search engine, loyalty programs, cookies and applications that gather certain kinds of data (e.g., one's location). Some participants reported not to use those privacy-critical services right from the start, whereas others have used them for some time but then decided to abandon the use. In their choice of an alternative service, participants mainly relied on the service provider's reputation: "Well, regarding the phone that I use, an iPhone and not an Android, of which...You know both share information with the NSA, but as far as I know only Google also uses it for marketing purposes [...]." (P13) Another strategy is to rely on the opinion of experts: "For example, Signal is recommended by Edward Snowden [...] it helps in the decision to use it if someone like Edward Snowden recommends it." (P13)

Do Not Share Sensitive Data. Some participants (13) stated to not share certain kinds of data, e.g., their name, email address, phone number, location, and bank data. However, only one participant mentioned his/her sharing behavior in OSN in this regard: "If you have liked 'ZEIT ONLINE' [a German newspaper], you always get their news feed and some things there are interesting every once in a while, where you think it would be worthwhile to promote it a little and it could interest someone, e.g., a pal, but instead of liking it or tagging my pal, I leave it be and think 'whatever'." (P8)

Limit the Amount of Data Recipients. A few participants (2) reported to share data, but limit the amount of recipients, for example by reducing the number of Facebook friends or not posting something on Facebook at all because they have so many friends there: "Maybe because so many are watching. Back then you had about 30 friends, it didn't matter what you posted on your timeline. And now it's, I don't know for sure, like 400. Thus you think twice before you post something." (P8) Others use Facebook's privacy settings to keep their postings away from unwanted readers.

Provide False or Misleading Information. A few participants (6) reported to act according to the principle "security through obscurity" by providing false information on purpose, mainly by using a false identity: "Well, depending on the service provider, quasi depending on the importance, I also provide false data, I don't simply use false data but instead I have set up a fake profile which I always use." (P10)

3.3.3 Protection Obstacles

I identified five obstacles that prevent our participants from protecting their data, with three concerning their skills and motivation, and one concerning other people and ethical considerations, respectively.

Too Much Effort. Some participants (9) reported to refrain from reading security policies since these were too cumbersome to understand. The same seems to apply regarding the use of privacy-friendly applications: "Because after all it [Threema] is rather cumbersome. And because only a few people use it and I think you can still share everyday things via WhatsApp." (P16)

Too Complicated. Very few participants (2) complained about privacy policies being too complicated to understand.

Lack of Knowledge. This is in line with a few participants (4) stating lack of knowledge about protection possibilities and processing of their released data as one reason for not protecting themselves more: "I wish I'd know which data I should protect better and how. Maybe I would also take better care if I'd know. If I'd concentrate more on this I'd probably know why it is important to protect these data, but it's just too hard for me to access these information." (P12)

Behavior of Other People. A few participants (8) referred to other people who refrained to use alternative privacy-friendly messengers or even shared data about third people: "In my opinion, if you have the opportunity to use a secure service, why shouldn't you do it, I think. The only thing speaking against it is, for example Telegram, it's just not spread that much. If you delete WhatsApp and only use Telegram, you simply don't reach a huge amount of your friends." (P8) "With social networks like Facebook [...] as soon as anybody posts something or tags you, it's already gotten out where you are or where you were or anything." (P4)

Ethical Considerations. One participant also explained that s/he thought it would be unethical to use free services that build on the processing of personal data as their business model without proving personal data: "The thing is, the anonymous search engines use Google's data, more or less...I think, in terms of ethics, that's kind of...not perfectly ethical, with the anonymous search engines using Google's servers, since they cost and not giving something in exchange to Google for this...to use it for free...actually the deal is that Google shows ads for this." (P13)

Furthermore, participants stated four different reasons for using applications or devices that could possibly harm their privacy, with all but one being related to social factors.

Social Pressure. Most (19) participants reported to use certain messenger or OSNs, even if they are skeptical towards them in terms of privacy protection, because most of their friends also use them: "Well, I actually view WhatsApp with skepticism due to reasons of data privacy. However, since all of my friends use WhatsApp I also use it, for you won't get very far with an alternative messenger that might be more suitable but that nobody uses." (P1) Accordingly, they stated that they would transfer to other messengers or OSN if their friends would do so. However, this effect also applies to the use of such applications that are considered as privacy-friendly: "Friends of mine started with this and then all of them had it and then we had a group chat and then everyone transferred to Threema and then I thought 'Come on, then you're also going to Threema'." (P11)

To Keep Oneself and Others Up-to-date. Many participants stated to use OSN to keep themselves informed of what happens in the life of their friends and family or to inform others about what is going on in their own life: "Once in a while you wonder about what friends with whom you don't meet very often do at the moment. [...] I don't get an email, I don't get a WhatsApp message, I get all information via Facebook what happens in my surroundings." (P8) "[...] I want my family - because we live so far apart...sometimes I like it to communicate with them. [...] so they know where I am, where I was on the weekend, I don't know, stuff like this and I want to show it, because they want to know how I am and they want to know what I did." (P17)

Convenience. Some participants (7) admitted to use certain applications out of convenience: "Anyhow you have an easy opportunity to contact a large amount of people and invite to something, who have then

the opportunity to discuss things like who brings what, when does it start, what's the address again in this group or event. And that simplifies a lot of things." (P5)

Express One's Opinion. Very few participants (2) referred to the opportunity to express and spread their own opinion about a certain topic: "But when I post something then often with the idea to let people in my social surroundings know something, either what I do or what I like. [...] Last year at Christmas I found out about gift coupons offered by the Oxfam company that supported charitable projects. That's something I want more people to know of and maybe support it, and so I spread it." (P2)

3.3.4 Common Privacy (Mis)conceptions

I also identified certain (mis)conceptions about data privacy in our participants' responses that have already been observed by other privacy researchers in prior studies.

I Have Nothing to Hide. Some participants stated they were not interested in privacy very much because their data was not sensitive at all: "Yes, well, I must say I don't get the whole hype about this...I always think those who have nothing to hide don't have to be so upset about it. [...] if someone would intercept me, I'd say he wouldn't find anything or it wouldn't be relevant [...]" (P15)

I Am Not Important Enough. Accordingly, a few participants also thought they were too unimportant to be intercepted: "[...] but I have a lot of confidence. On the one hand in the systems, on the other hand that I am too ordinary. That it wouldn't be worthwhile to spy on my data." (P2)

It Is not Possible to Protect My Data. A few participants said even if they wanted to do so, it would not be possible to protect their data from being accessed in one way or another: "I think it is like the lock at my apartment, if someone really wants to get in, he can break it open. If someone really wants to have my data, he gets it. Once I use smartphones and notebooks, that's a truth I have to deal with...or that I have to accept, respectively." (P18)

3.4 Discussion

In this section, I discuss the meaning of the results in order to answer the research questions proposed in section 3.2.1.

3.4.1 Mental Models of Privacy Consequences

Regarding RQ2a, I found that while most participants named personalized advertisement as a possible consequence of not protecting one's privacy and about half of my participants also fear financial losses, most participants lack awareness of further possible privacy consequences. This is in line with the results from Harbach et al. [91] and Shirazi and Volkamer [205], who also identified financial loss and personal advertisement as the most salient privacy consequences. However, individual participants provided additional possible consequences besides personalized advertisement and financial loss. The list of resulting consequences also relates to the results of Karwatzki et al. [108], since all consequences named by the participants could be categorized as either physical, social, resource-related, psychological, prosecution-related, career-related, or freedom-related. However, most consequences provided by the participants are more specific than the broad categories of consequences identified by Karwatzki et al. [108], and some refer to more than one category. The resulting list of consequences could thus be better suited to complete people's mental models of possible data collection consequences, e.g., in interventions and campaigns than Karwatzki et al.'s categories. I investigate this topic in more depth in chapter 4.

3.4.2 Strategies for Protecting One's Privacy

Regarding RQ3a, the participants reported to apply several privacy protection strategies, i.e., refrain from using privacy-threatening services, not share sensitive data, limit the amount of data recipients, or provide false information. These strategies indicate that the participants do not suffer from an "illusion of control", in the sense that they think their privacy is safe because they can decide what kind of information is shared

with whom and have the possibility to change this decision later on, e.g., by editing their profile, while actually once an information is shared online users cannot control who already gained access to that information and how it is processed by third parties in the future. However, some participants reported a lack of knowledge about possible protection measures to be an obstacle for privacy protection, and some participants did not report on applying a successful protection strategy at all. Furthermore, all of the protection strategies the participants reported to use fall in the category of "behavioral" protection strategies described by Oomen and Leenes [170]. None of the participants reported to use standard security measures and PETs or more advances PETs. Whereas I suppose this is rather due to a lack of knowledge about what programs are running on their computer and how these are involved in the protection of their private data than an actual abandonment of standard security measures, it shows significant deficits in participants' understanding of how data is processed on their computer. These results are contrary to those of Litt [148], who found that younger adults tend to apply more technically based protection strategies. Although my sample was rather young, my participants do not seem to be automatically more technically adept than older users.
Hence, it is not sufficient to hope that problems referring to a lack of technical expertise in the deployment of protection strategies will vanish on their own once most online users are digital natives. It seems thus crucial to further educate users about strategies for privacy protection, e.g., by developing trainings, campaigns, info material, or dedicated privacy assistants that provide information about possible protection solutions and help users to apply these solutions successfully. I pursue this approach in chapter 5.

3.4.3 Obstacles for Privacy Protection

Regarding RQ4a, I found that participants refrain from applying protection solutions or using privacy-friendly alternatives since these are too cumbersome to use, too complicated to understand, or due to the contradictory behavior of other people. Contrary to prior studies (e.g., [205, 183, 231]), the major obstacles for privacy protection reported by my participants are related to usability and social factors, of which the latter were also identified to be crucial for the adoption of secure messengers by Abu-Salma et al. [4]. Whereas there are already many ongoing efforts to improve the usability of PETs (successful or not), social factors are harder to influence from the outside, i.e., as a privacy researcher or activist. Yet there also lies an opportunity in people's social suggestability, as some also report to having started to use a privacy-friendly service because a significant other used this service as well. Hence, future attempts to motivate users to increase their privacy could focus on the social aspect, for example by letting other people invite their peers to privacy-friendly OSN, messengers, search engines etc.
Most participants reported to still use privacy-threatening services in order to reach other people, participate in their life, or share their opinion with others. Another reason for using non-privacy-friendly services and devices is the convenience that these products offer. However, as a majority of the corresponding answers refers to the use of social networks and messengers, I will focus more thoroughly on the question why people continue to use privacy-threatening devices and services in chapter 6 to also consider other use cases.

3.4.4 Limitations

The study suffers from several limitations that should be kept in mind when drawing conclusions based on the results. I used a convenience sample, which resulted in the majority of the participants being students, thus the sample is most likely skewed (i.e., younger, higher educated and eventually over averagely tech-savvy) compared to the general population. Furthermore, it would be recommendable to validate the results with a greater number of participants. Also, although I aimed to investigate the general privacy behavior of people across different contexts, some online services, such as online social networks and messengers, are very well-known to most people, unlike new devices and services like smart home systems. Hence, it is likely that these contexts are over-represented in the answers of my participants.

4 Awareness of Privacy Issues

As shown in chapter 2, privacy protection behavior is best predicted by the users' behavioral intention, which is in turn closely related to privacy concerns and the perceived privacy risk. Risk perception is usually defined as the perceived probability of adverse consequences and the perceived severity of those [227, 150]. It follows from this definition that in order to perceive the risk of sharing – and not protecting – their private data to be high, people have to be (1) aware of possible consequences that could result from this behavior and (2) perceive the probability and severity of these consequences to be high.

The interview results described in chapter 3 suggest that lay users lack awareness of consequences that could result from sharing and not protecting their private data, a circumstance that has also been shown in previous studies [76, 91, 256, 12]. However, these studies usually considered US-American participants [76, 256, 12] or did not focus specifically on the privacy context [91]. My interview study, on the other hand, included a convenience sample of mostly young lay users and it remains unclear whether the seeming lack of awareness of possible privacy consequences can be generalized to a broader German population.

A survey study conducted by Gerber et al. [82] with 1052 participants addresses this issue by relying on a panel for recruitment to strive for a more heterogeneous sample. Participants were recruited via the Clickworker panel [88]. The study was split in two parts and investigates (1) users' awareness of possible consequences of using smart home devices, smart health devices, and OSN (described in Gerber et al. [82]), and (2) users' perception of different kinds of privacy risks associated with the use of these technologies (as described in Gerber et al. [83]).

The use cases were chosen due to the fact that there is ambiguous evidence about people's risk perception of well-known and unknown technologies [74, 63, 77]. Thus, both types of technologies are considered in the study, relatively well-known (OSN) and emerging technologies (smart home and smart health devices). Further, while the home is often considered to be a private place, health data is often considered to be rather sensitive, and OSN are often talked about in the media, including reports about possible risks of using OSN. Hence, these use cases were chosen to be included in the study [83]. One third of participants reported to use smart home or smart health devices on a regular basis, but most participants reported to use OSN at least sometimes.

Participants were randomly assigned to a use case. In the first part of the study, they were asked to name all consequences they could think of that could result from using the respective technology (OSN, smart home, or smart health devices) [82]. In the second study part, they were presented one of nine different risks scenarios and asked to indicate the probability and severity of the presented risk scenario on a visual analogue scale[9]. Due to the technical implementation of the questionnaire in SoSciSurvey, the scales reach from 1 to 100. However, participants only saw the scale labels "strongly agree" and "strongly disagree" [83]. The items were based on validated instruments [141]. They were further checked for validity and reliability in a pilot study [83].

The second study part included abstract and specific risk scenarios [83]: Specific risk scenarios specify a concrete consequence that could result from the use of the considered technologies, while abstract risks scenarios do not specify such a consequence. The examples for concrete consequences included in the specific risk scenarios were based on the categories of privacy consequences identified in the focus groups with lay users conducted by Karwatzki et al. [108]. The abstract risk scenarios state that data is collected by the manufacturer or service provider (R1), that the data is collected and analyzed (R2), adds a description of usage pattern (R3), and states the possibility that this process of data collection and analysis could harm the user (R4). The specific risk scenarios add an explanation how the user could be harmed by describing the possible consequences of restricted choice of nutrition if the user does not want to get a worse health insurance premium (R5), stalking (R6), targeted burglary (R7), the publication of inappropriate content in social networks due to identity theft (R8), and worse chances regarding job applications (R9).

The results of the first study part indicate that most users lack awareness of possible (negative) consequences that can result from the use of data-collecting technologies [82]: Only 262 of the 2462 overall responses

[9] This type of scale was chosen to ensure metric data [182, 218]

described specific consequences resulting from data sharing. Regarding the different use cases, 47 described privacy consequences relating to the use of smart home devices, 72 relating to the use of smart health devices, and 153 relating to the use of OSN. Using a closed coding approach based on the categories of privacy consequences identified by Karwatzki et al. [108], the authors find that most of the consequences are social, resource-related, career-related, and freedom-related.
Regarding the second study part [83], the results indicate that the abstract risk scenarios (R1–R4) were considered to be more likely compared to the specific risk scenarios (R5–R9) (see fig. 10). Not surprisingly, the collection of data (R1) was rated as most likely across all use cases. (R9), referring to worse chances regarding job applications, was considered least likely. The severity, on the other hand, was rated higher for the specific risk scenarios, with burglary (R7) and stalking (R6) being perceived as most severe overall. An unexpected result was the evaluation of the risk scenario referring to the collection of data (R1), which was considered more severe than, e.g., the collection and analysis of data. A MANOVA with the privacy risk scenario and the use case as independent variables (IV) and the mean of the perceived probability and severity of the different risk scenarios as dependent variables (DV) confirmed these results statistically, while no statistically significant difference was found between the three use cases, as well as no significant interaction between use case and risk scenario [83]. The evaluation results indicated two clusters of risk scenarios (see fig. 11), which was also confirmed by a cluster analysis and Mann-Whitney-U-tests [83].
The results indicate that while users seem to lack awareness of consequences that can result from the disclosure of their data when using data-capturing technologies (chapter 3, [82]), they also feel that single, concrete consequences are rather unlikely to happen to themselves [83]. Hence, people may need to be shown a combination of different privacy consequences in order to increase the perceived likelihood of any of these consequences actually occurring to themselves, as also stated in Gerber et al. [83]. The only extensive collection of privacy consequences that can result from the disclosure of data is provided by Karwatzki et al. [108]. Since Karwatzki et al. investigated lay users in their focus groups and did not specify any particular use cases, their results unfortunately can not be used to identify a list of privacy risks that could be used as a basis for this combination of privacy consequences. Hence, I conducted a literature review to investigate whether additional privacy consequences associated with living in smart environments (more precisely: smart home and smart health households) could be identified based on the research and considerations of other researchers.

4.1 Identification of Privacy Consequences Associated with Living in Smart Environments

I used the keywords “privacy risks smart home”, “privacy threats smart home”,“privacy consequences smart home”, “privacy risks smart health”, “privacy threats smart health”, and “privacy consequences smart health” to search for publications dealing with these topics in the databases ACM Digital Library, IEEE Xplore Digital Library and Scopus. I excluded papers which were not published in English.
Overall, I found 25 papers describing privacy consequences in the context of living in smart home households and four papers describing privacy consequences in the context of living in smart health households:

Prosecution-related

- Criminal prosecution [51, 223, 247]
- Unwarranted searches [262]
- Police surveillance [27]

Social

- Social “penalization” [27]
- Loss of reputation [27, 14, 113, 223, 247]
- Divorce [27]

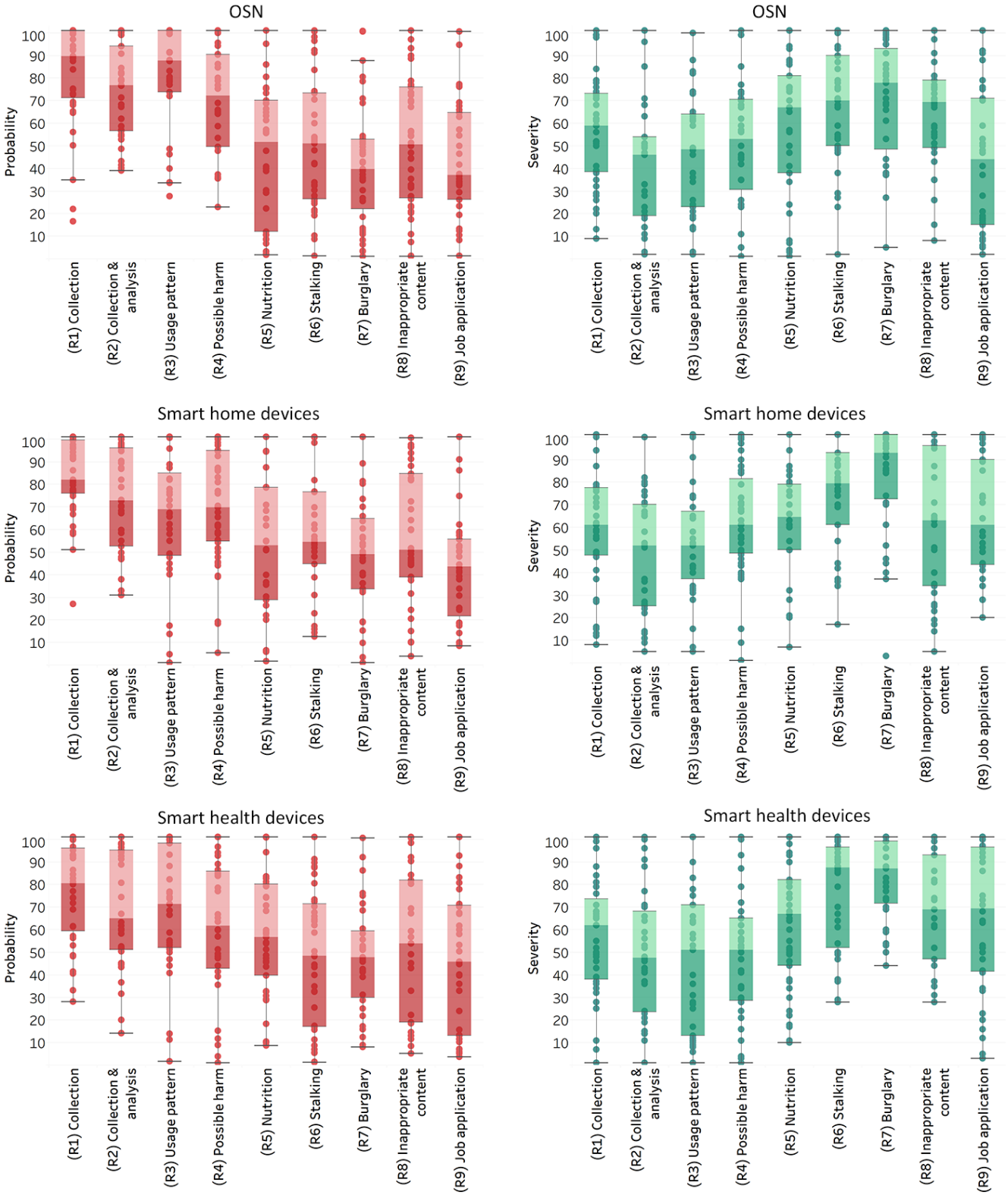

Figure 10: Data distribution for the probability ratings (left) and the severity ratings (right), taken from Gerber et al. [83].

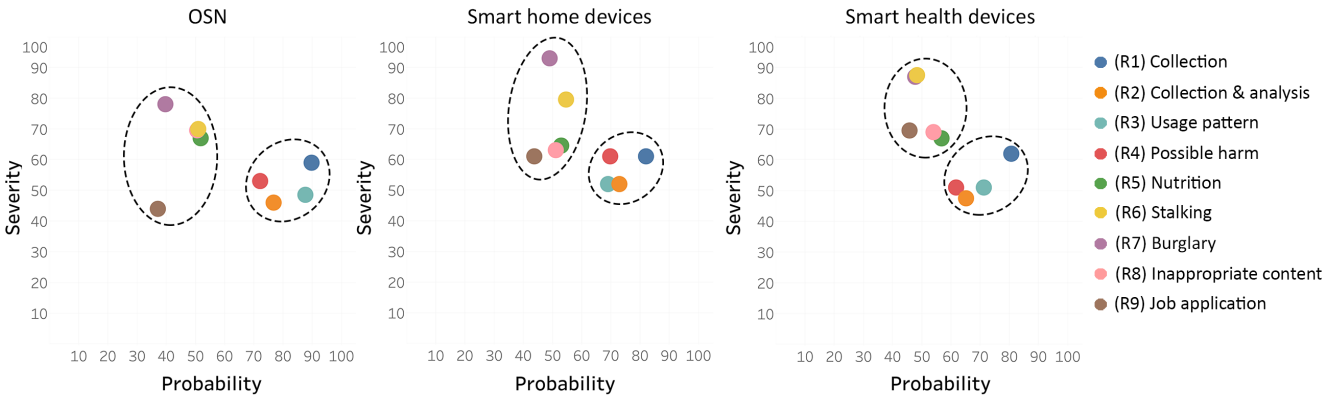

Figure 11: When plotted in terms of severity and probability, the risk scenarios seem to build two clusters. Figure taken from Gerber at al. [83].

- Social Embarrassment [158, 96, 51, 41, 223]
- Cyber bullying [17, 41]
- Damage of credibility [96, 113, 247]
- Loss of trust [223]

Freedom-related

- Restricted behavior [34, 27]
- Restriction of energy usage [51]
- Personalized advertisements [262, 187, 27, 158, 101, 93, 126, 259, 51]

Psychological

- Discomfort due to being watched [262, 27, 96, 179, 51]
- Discomfort due to loss of control [96]
- Fear of being treated unfairly [51]

Career-related

- Being penalized by employer [27]
- Worse chances of getting a job [158]
- Not getting a job [51, 188]

Resource-related

- Targeted burglary [194, 262, 27, 14, 101, 51, 62, 41, 100, 221]
- Targeted robbery [29]
- Blackmail [168, 29, 96, 113, 11]
- Price discrimination [129]
- Detection of warranty violation [262]

- Worse insurance rates [158, 247]
- Worse credit conditions [158]
- Not getting an insurance [158, 188]
- Not getting a credit [158]
- Unauthorized purchases [96]
- Spam [112, 100]
- Exclusion from services [129]

Physical

- Stalking [29, 262, 101, 41, 100, 221]
- Kidnapping [51, 62]
- Physical harm (due to information about medical condition) [113, 13]

4.2 Conclusion

Participants seem to lack awareness of concrete consequences that could result from using privacy-threatening devices and applications (chapter 3, [82]). As the study conducted by Gerber et al. [83] further indicates, approaches aiming to raise people's awareness by confronting them with possible privacy consequences should include several examples of concrete consequences, as single consequences are considered to be less likely. I thus identified an exemplary set of concrete privacy consequences that could arise from living in smart environments from the literature. Information about these consequences should be included in the knowledge content of the privacy app, the development of which is described in the next chapter.

5 Privacy Protection Knowledge and Ability[11]

As shown in the last chapter, a possible reason for some lay users to refrain from protecting their data might be that they are simply not aware of privacy issues and therefore see no need to protect their data (see also [70, 53, 15, 176]). Yet there is at least another group of users that effectively expresses concerns about the control of their personal data [65, 180, 219, 152]. These users might be highly motivated to protect their data, but lack the ability and knowledge to do so [172, 10, 20].
An important factor for people to protect their privacy is thus not only the willingness, but also the ability to do so. As shown in chapter 3, even young lay users often lack knowledge regarding technical protection strategies and the deeper interrelations of digital devices and services in terms of privacy infringement. To address this issue, I outline the development of a technology-based, yet easy to use privacy-enhancing solution in this chapter.
First, I describe the development of the Android-based application "FoxIT" which utilizes several techniques to support users in managing their online privacy. It mainly focuses on mobile privacy, but also covers some other privacy aspects (e.g., privacy settings in social networks). The app's functionalities comprise a static analysis of smartphone and app permissions (including an evaluation of the results) and various lessons about privacy relevant issues. Furthermore, gamification elements were included to enhance use motivation. I then report on the results of an evaluation study and outline the development of possible improvements for FoxIT as implied by the evaluation results.
In the following, I will liberally use quotations from my article published in "Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST)" (2018) without explicitly marking each quote.

5.1 Related Work

This work relates to research on mobile app permissions, privacy awareness, and privacy education.

5.1.1 Smartphone App Permissions

Researchers have chosen different approaches to deal with the issue of smartphone permissions. Some have focused on the detection and prevention of data leaks, mainly in Android apps [66, 23, 98, 28, 50, 261]. Examples include the Android extension TaintDroid, which tracks the flow of privacy-sensitive data through third-party applications [61] and Privacy Leaks, which is built on the TaintDroid platform and aims to raise awareness about privacy leakage on the smartphone [23]. Furthermore, Liccardi et al. conducted a "sensitivity score" based on the number of permissions that accessed personal information about users [143].
Others have studied permission interfaces from a user's perspective. In two user studies, Shklovski et al. [206] confronted their participants with app behaviors while assessing their reactions. While only two out of 89 participants were unconcerned ("I do not care") about the tracking and data collecting behavior of apps, a significant proportion of their participants found it "disturbing" and "creepy". Nonetheless they also admitted that such concerns were often overridden by other factors when installing an app. The authors found a great desire for greater transparency and control over information disclosure on the side of the end user. Investigating users' mental models of app permissions, Felt et al. found that many users do not understand the relationship between requested resources and risks [66]; whereas the study results by Lin et al. suggest that even when users are aware of the used resources, they still have trouble understanding why an app needs certain resources [145]. Both results indicate that without additional information, users lack the ability to make informed decisions. Several study results also indicate that Android's previous approach of presenting permission notices only in the Play Store (in contrast to just-in-time permission requests during the app use, which was implemented in Android 6.0) leads to poor

[11] based in part on the paper "Nina Gerber et al. FoxIT: Enhancing Mobile Users' Privacy Behavior by Increasing Knowledge and Awareness. In: Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST). ACM, 2018, pp. 53–63." [85]

permission comprehension and recall [66, 144, 24, 111]. To overcome the deficiency of current privacy notifications, researchers have proposed several alternative permission interfaces [145, 257, 173, 222]. For example, Lin et al. proposed a privacy summary interface based on crowdsourcing data, which informs users when apps breach people's privacy expectations [145]. Paturi et al. present an icon-based interface, which informs users about privacy threats posed from the app provider or associated third parties [173]. Choe et al. also use a visual interface to provide users with a "privacy rating" for apps [45] and Harbach et al. include examples of personal information in the permission interfaces (e.g., personal photos for the media permission, the current location for the location permission) [92]. Kraus et al. display a comparison of the number of requested permissions for an app with the number of permissions usually requested by apps from the same category [123]. The "Privacy Facts" interface by Kelley et al. provides a checklist for the requested permissions [110] and another approach by Lin et al. provides additional information to the users about how many users were surprised about an app requesting certain permissions [146]. Gerber et al. proposed "COPING", which aims to provide more, well-structured information about the individual permission requests. The authors evaluated their interface against several other alternatives and concluded that simply reducing the complexity of an interface actually impairs decision quality rather than improving it through better understandability [87].

Since Android 6.0, users can grant or reject app permissions during app runtime, similar to the iOS permission management approach. Although both iOS and Android users seem to prevent some apps from accessing their data [15, 71], the implemented permission managers do not allow users a satisfying privacy protection because they lack sufficient information to assist users in making informed decisions. Hence, Liu et al. conducted and evaluated an enhanced permission manager, which helps users managing their smartphone privacy settings. Participants in their field study adopted 78.7% of the recommendations made by their privacy assistant [149]. Another permission manager called "AppOps" was developed and evaluated in a field study by Almuhimedi et al. [15]. They combine information about what resources installed apps can access with privacy nudges (e.g., "Your position has been shared x times with app 1, 2 and 3 over the last 14 days"). Other solutions for the management of already installed apps were provided by Fu et al. [75] and Balebako et al. [23].

Again, other researchers focus on the behavior of app developers to enhance end-users' smartphone privacy. For example, users often rely on the text description provided by the app's developers when choosing a new app in the app store. However, developers often focus on promoting their app and fail to warn about privacy-sensitive permissions in these text descriptions. Watanabe et al. aim to improve users' smartphone privacy awareness by providing explanations for this circumstance and suggesting possible solutions [238]. Balebako et al. investigated how developers make decisions about privacy [25]. They further suggest some nudges that aim to improve privacy practices of app developers [22]. Felt et al. propose guidelines to aid platform designers in choosing more appropriate permission-granting mechanisms [67], whereas Jain and Lindqvist evaluated developers' interaction with enhanced privacy-preserving location APIs [102].

Schaub et al. [192] present a design space for privacy notice designs, classifying privacy notices in terms of timing, channel, modality and offered control. My approach provides on demand notices, displaying visual (text-based and graphical) notifications on the primary channel (the smartphone). It is decoupled from the actual permission management, but offers a direct link to the smartphone's permission settings. This is explained in more detail in section 5.2.1.

5.1.2 Privacy Awareness

In the given context, privacy awareness refers to the users' understanding about what data is collected by whom and for what purposes, with which third parties this data is shared, and what corresponding risks and benefits may arise [7, 178]. Pötzsch further distinguishes between different privacy awareness dimensions: user-independent vs. user-specific, as well as application-independent vs. application-specific [178]. Privacy awareness is crucial for enabling users to not only understand the benefits, but also the risks of data disclosure and, consequently, make more informed decisions [53, 178].

Accordingly, studies dealing with end users' privacy awareness found that especially non-expert users were more likely to protect their privacy when their privacy awareness was increased [193]. Participants in a user study conducted by Shih et al. were more privacy aware and less willing to disclose data when a vague purpose of data collection was presented [203]. Kang showed that the more privacy threats users were able to identify, the more protective actions they took [105]. Malhotra et al. found that users also find it important to be aware of and have direct control over personal information online [156]. One example for privacy awareness-enhancing technologies is "NoTrace", a Mozilla Firefox add-on, which uses specific awareness modules to inform users about which information is leaked towards third parties and which information could be inferred based on their behavior [154]. Other examples focusing on mobile privacy are described in section 5.1.1.

However, raising privacy awareness alone may result in users disclosing less information than before, which could be harmful for service and application providers [233]. Hence, Deuker suggests combining the creation of privacy awareness with tools that support users to react in a reasonable way, thereby shifting the focus from problem awareness to awareness of possible solutions [53]. Even if this awareness of possible solutions does not translate directly into solution-oriented behavior, as the privacy paradox, i. e., the discrepancy between attitudes towards behavior and actual behavior in the context of one's own privacy [167], impressively shows, it is nevertheless a necessary prerequisite for this [243, 117]. With FoxIT, I aim to provide users with the knowledge that is necessary to apply these solutions effectively. This is explained in more detail in section 5.2.2.

5.1.3 Privacy Education

Likewise, Xu et al. suggest to enhance users' privacy protection by combining education and training with Privacy-Enhancing Technologies (PETs) [251]. Indeed, the results by Kang et al. [105], who conducted a qualitative study on users' mental models of the internet and internet data, show a significant lack of knowledge about how their data is collected, shared or stored and how they could protect themselves. This is in line with the findings of Ackermani et al. [5] and Balebako et al., whose results indicate that users wish to remain anonymous, yet have a very limited understanding of smartphone applications' data sharing practices. The authors therefore call for education of users as well as for interfaces raising privacy risk awareness [23]. Concerning privacy behavior, in a study conducted by Poikela and Kaiser, participants with limited knowledge of location-based apps reported more often than others that they perceive no risks in using these apps, whereas knowledgeable participants were found to protect themselves more from privacy risks [176]. Although experts suggested that knowledge about protection tools is positively related to their application, Kang et al. were not able to show this effect in their study. However, their sample was likely to be skewed towards enhanced protection knowledge [105].

In order to address knowledge gaps and thus implement educational measures, in addition to the classical knowledge transfer strategies, the concept of serious games, which uses gamification elements to increase the motivation for learning among users and thus improve learning success [264, 106] has been established during the last years. By pursuing challenging tasks, reaching goals through their own decisions and building their own knowledge by trying out different alternatives without worrying about the consequences in real life, users are encouraged to actively and critically examine the learning content [78]. Such games are used, for example, in physics [46, 166], medicine [39, 38], software development [160] and IT security [139, 213, 224] to provide content to users.

While there are several app-based interventions which aim to enhance knowledge about security [139, 213, 224], to my knowledge FoxIT is the first mobile intervention that focuses not solely on awareness or rather basic app permission knowledge, but also on advanced knowledge about privacy. This is explained in more detail in section 5.2.2. Also, it uses gamification aspects to foster the motivation for education on the user's side, which are described in detail in section 5.2.3.

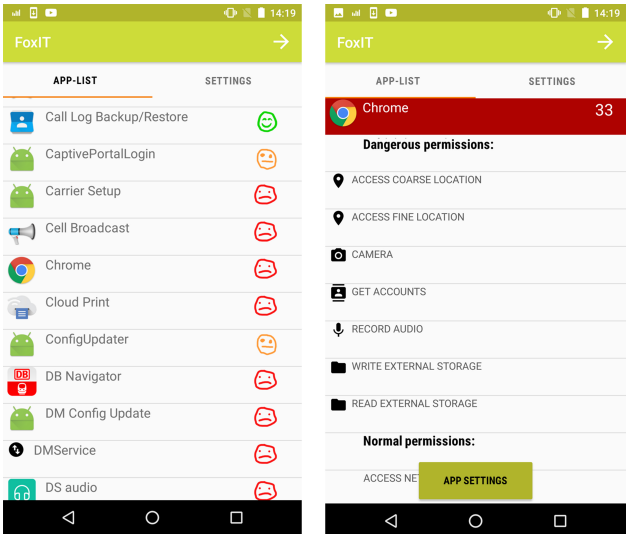

Figure 12: Result screen for the analysis of app permissions, app list overview (left) and detailed view for one app (right).

5.2 The FoxIT App

The FoxIT app was developed iteratively in a user-centered design approach. Various experts on usability, human computer interaction and privacy were requested to give their feedback on previous versions. These were also discussed with lay persons in several user studies. All this enabled us to improve the content.
Since Android is the most commonly used smartphone operating system, it was decided to run the app on Android. The smartphone specific lesson content also refers to Android's functionalities and settings. FoxIT was developed using a Google Nexus 5 smartphone with Android 6.0. The code is available on GitHub[12]. The app content is described in the following sections.

5.2.1 Analysis of Smartphone Settings and App Permissions

When first used, a short tutorial is presented to explain the main features of FoxIT. Afterwards, the user is prompted to analyze the current settings of his/her smartphone and the granted permissions of the installed apps. Depending on the number of installed apps, this analysis usually takes between 10 and 30 seconds. The analysis results concerning the app permissions are displayed first (see fig. 12). To gain a quick overview, apps are either marked as harmless concerning their permissions (indicated by a green happy looking face), moderate (indicated by an orange neutral looking face) or critical (indicated by a red sad looking face). The categorization is based on Google's classification of the permission protection level [89]. Apps requesting at least one "dangerous" permission are categorized as critical, apps requesting no "dangerous" permission, but at least one "normal" permission are categorized as moderate, and apps requesting only "other" permissions are categorized as harmless. This categorization is not an absolute assessment of the actual threat, but is intended to focus the users' attention on those apps in which personal data could be at risk. Hence, the apps in which the user can actually intervene by using the permission management system in Android 6, and thus withdraw individual permissions if necessary, are pointed out to the users. FoxIT also offers a direct link to the configuration of Android permissions after clicking on a particular app (compare below).
Users can obtain further information by clicking on an app name (see fig. 12). The total number of requested permissions can be found on the right side next to the app name. Criticality of the app's requested permission is displayed via the background color (green, orange or red). The decision to use different background colors as well as the final color set is based on the feedback of five and seven lay

[12] https://github.com/sleep-yearning/FoxIT

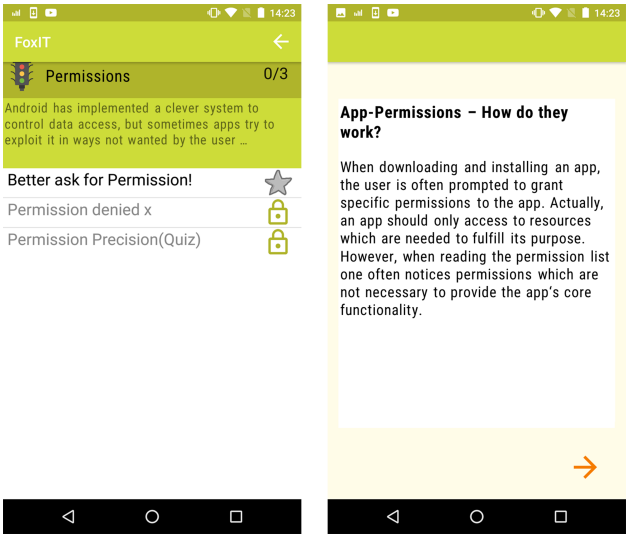

Figure 13: Example course (left) and lesson (right) about app permissions.

persons, who participated in a qualitative (semi-structured face-to-face interviews) and quantitative study (paper-and-pencil questionnaire), respectively, of an earlier FoxIT version. Beneath the app name, all permissions for the selected app are listed separately and categorized as "dangerous", "normal" or "other", also based on Google's classification of the permission protection level [89]. Further explanations of the permissions can be accessed by clicking on the permission name. An additional button offers the possibility to directly switch to the respective app's setting interface to change the according permissions, if intended. The analysis results for smartphone settings can be retrieved by swiping left or clicking on the "settings"-button in the toolbar. Like for app permissions, analysis results for smartphone settings are displayed in a list, either indicating whether a functionality (e.g., installation of apps from unknown sources) is activated or not, or specifying particular setting values (e.g., type of location tracking: GPS). The analysis can be repeated anytime in the setting menu. It should be noted that although FoxIT provides the function to scan smartphone settings and permissions requested by the installed apps, the FoxIT app itself does not request any particular permissions to conduct this analysis. In fact, these information can be assessed by any app installed on a smartphone without needing further permissions.

5.2.2 Privacy lessons

Currently, users can access a total of 61 lessons dealing with different privacy topics, assigned to ten separate courses (see fig. 13 for an example). These courses cover the following topics:

1. Historical, cultural and societal aspects of privacy
2. Encrypted messaging
3. Root and super user
4. Deep and dark net
5. Facebook privacy settings
6. Google services
7. Passwords
8. App permissions
9. Data privacy acts

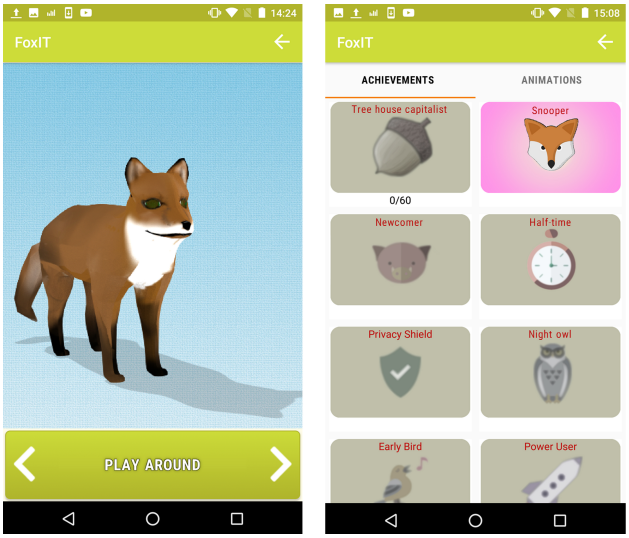

Figure 14: Animated fox (left) and trophy screen (right).

10. Messaging apps

At the end of each course, users can test their knowledge by completing short quizzes. This follows the learning principles proposed by Murphy [165] by offering an opportunity to practice the newly attained knowledge and gain direct feedback about the learning process. An additional course explains the app's functionality in more detail compared to the tutorial. Especially the analysis results of the smartphone settings and app permissions are clarified. A course comprises 5-10 slides with brief information texts (see 13 for an example). Where applicable, pictures are included, for example to show how a Panopticon looks like.
The course topics aim to cover four aspects of privacy knowledge:

- Highlighting the relevance of dealing with privacy issues (course 1)
- Basic background information about legal aspects (course 9)
- Detailed information about privacy settings and policies of popular online services/Android (course 3, 5, 6, 8, 10)
- Detailed information about privacy protection solutions (course 2, 4, 7)

This selection of course topics is based on the feedback of four privacy researchers, who put the focus on understandability and relevance of the topics for a large user base. For example, the use of encryption requires a certain level of technical expertise, whereas passwords are relatively easy to handle. Hence, users with different technical skills should receive valuable information. However, the set of lesson topics should be considered as rather preliminary, since it is planned to constantly revise and supplement topics and lessons, for example if new research findings or technical solutions are introduced in the privacy field. Thus, the topics were selected with the idea of putting together a preliminary, interesting and informative collection to test the app concept instead of already finding a comprehensive compilation of all topics.

5.2.3 Gamification Elements

FoxIT mainly relies on levels and achievements as gamification techniques [19]. Furthermore, the app features a mascot, an animated fox (see fig. 14). The fox can be accessed via the main menu. The fox was chosen as a metaphor for the knowledge transfer in FoxIT, since foxes are often considered to be "cunning". The design of the fox, along with the set of animations it should feature, was developed based

on the feedback of ten lay persons participating in a qualitative study, namely semi-structured face-to-face interviews, of an earlier FoxIT version. They mainly wished the fox to look animated and comic-like, but at the same time still realistic. The animations should reflect the natural behavior of a fox, however, playful activities like jumping around or frolicking were more popular than those with a possible negative connotation like hunting other animals. The final animations were chosen accordingly.
By completing lessons, users gain digital coins in forms of mushrooms and acorns. The mushrooms can be used to activate new courses and lessons. Additionally, a new (randomly chosen) lesson is activated on a daily basis. Acorns can be traded for new fox animations. Certain use behaviors or actions like completing half of the courses can further lead to the activation of various trophies, reflecting the current state of use (e.g., "newcomer", "early bird", "power user"). The animations serve as achievements, whereas the activation of new courses can be seen as some sort of levels, reflecting the progress the user makes, and the trophies can be attributed to both aspects.

5.3 Field Study

A two-week field study was conducted to gain first insights into how users react to prolonged use of FoxIT in a natural setting. I describe the study content and procedure below.

5.3.1 Research Questions

I was interested in the effects of prolonged use of FoxIT concerning privacy knowledge, awareness and behavior. Thus, the research questions are:

RQ3b: Does using FoxIT for two weeks lead to an increase in knowledge about privacy related topics?

RQ3c: Does using FoxIT for two weeks lead to a change in privacy awareness?

I will distinguish between different aspects of behavior to gain a more detailed understanding of possible effects of FoxIT use. The third research question is therefore divided into various sub-questions:

RQ3d: Does using FoxIT for two weeks lead to a change in privacy behavior, that is, do participants...
...improve the privacy conditions on their smartphone?
...increase their use of security measures?
...deploy stricter privacy settings on social network sites?
...actively inform themselves about privacy?
...prompt others to protect their data?

5.3.2 Recruitment and Participants

Participants were recruited by word-of-mouth to make certain that the investigator carrying out the study could sufficiently explain the FoxIT concept before collecting any data. Besides, it was aimed to increase commitment by relying on personal contacts. A total of 97 Android users were invited to participate in the evaluation, none of them experts for data privacy or security issues. Of these, 78 completed the first survey, 43 the second and 40 the third. Of these 40 users, five were excluded from the analysis since they failed to upload their use data. Another four were excluded because they completed less than ten lessons, leaving 31 participants. Unfortunately, only 14 participants who dropped out of the study early gave feedback on why they dropped out (5 did not download the app, 4 left after the first and 5 after the second survey). They provided different reasons for quitting (participants could provide more than one reason): 6 participants said the study procedure was too time-consuming, 4 stated the app's UI was not usable enough, 3 said the app contained technical flaws, 2 could not download the app and another 2 reported they were not interested in privacy topics. One participant each did not like the lesson content, was traveling at the

time the study was conducted and thus had no access to the internet, needed the storage capacity on her smartphone for other purposes, and used a Windows phone.
The field study included 31 participants who used FoxIT for two weeks. Due to the recruitment practice, participants can be considered as a "convenience sample" that is not balanced across gender, privacy knowledge or other characteristics. Participants ages ranged from 18 to 54 years (M=27.97, SD=11.60). The sample included 15 females and 16 males. Ten were from computer-related fields, 16 were from non-technical fields, 3 were from engineering-related fields and 2 were from medical-related fields. There were 19 students, one housewife, one pensioner, and the rest were full- or part-time employees. All participants lived in Germany. On average, participants used FoxIT for 105.64 minutes (SD=88.34, min=17, max=475) and completed 37.71 lessons (SD=17.60, min=13, max=61).

5.3.3 Study Procedure

A two-week field study was conducted, with participants using the app on their own smartphone. This approach was chosen to obtain realistic data, since the permission analysis would be based on the participants' actual smartphone content. Furthermore, using the app occasionally over a two-week period might reflect a more natural use behavior than constraining use to only one (long) lab session. The whole study was conducted online to allow for a non-local sample, because participants would not need to attend the laboratory. In a first email, participants received the link to an initial survey, along with contact data in case they had any questions, suggestions or faced any problems during the study. The second email, which was sent three days later, contained an explanation of the study procedure and instructions for installing the app. Participants were encouraged to install the app immediately and use it over a period of two weeks. Two weeks after the enrollment (i.e., directly after the use period had ended), they were invited to answer another survey to assess any changes that might have occurred as a result of using the app. One week after the use period had ended, participants were asked to answer the survey again, to check for long-term effects. The whole email communication can be found in Appendix C.
During the two-week period of use, the app also collected data about the number of completed lessons, the number of uninstalled apps and the amount of time participants spent using FoxIT. If participants had uninstalled an app, they were presented a brief survey the next time they used FoxIT, asking whether they had actually uninstalled an app and if they had, for what reasons. The data collection feature, which also made it necessary to ask for particular permissions for the FoxIT app, was only implemented for study reasons and immediately removed from the app after the study was finished. Participants received no monetary compensation. Instead, five Amazon vouchers à 40€ were drawn among participants.

5.3.4 Questionnaires

All survey questions were presented in German. The items are based upon previously validated instruments whenever available. If not stated otherwise, the items are based on a 5-point Likert scale (1=strongly disagree; 5=strongly agree). To ensure reliability and validity of the measures, item difficulty and item-total correlation were checked for every item and internal consistency for every subscale. Items with a difficulty smaller than .20 or greater than .80 were dropped from the analysis; so were items with an item-total correlation smaller than .30. Also, items whose exclusion improved the internal consistency of the according scale significantly were excluded. The number of items that were included in the analysis is displayed in parentheses. Since the internal consistency could only be calculated separately for the three surveys, I will only report the lowest value for Cronbach's α.
Privacy Knowledge. Eleven multiple choice items were used to assess privacy knowledge. The knowledge items were drawn from the quiz parts of the privacy lessons. Participants could achieve a maximum score of 44.
Privacy Awareness. Eighteen (seven) items were used for the assessment of privacy awareness ($\alpha \geq .62$). The items were inspired by those used by Kang et al. [105].
Privacy Behavior. Five (four) items were used to assess privacy conditions on the smartphone ($\alpha \geq .66$), three (two) items for assessing the use of security measures ($\alpha \geq .58$) and five (four) items to measure

the management of privacy settings on social network sites ($\alpha \geq .96$). Three items were used to measure how participants inform themselves about privacy ($\alpha \geq .83$) in the first survey; an additional item relating to the app use was applied in the second and third survey. Another four items were used to assess how participants prompted others to protect their data ($\alpha \geq .88$). The items are based in part on Milne et al. [161] and Kang et al. [105]. Further, two items were used to ask participants whether and for what reasons they had uninstalled an app, if any uninstalling activity was observed during the study. However, these items were not included in the surveys, but displayed in FoxIT the next time the respective participant started the app.

5.3.5 Ethical Considerations

Ethical requirements with respect to participants' informed consent and data privacy were in line with the ethical guidelines provided by the Technische Universität Darmstadt. Participants were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, the surveys were implemented in SoSciSurvey [131], which stores all data in Germany and is thus subject to strict EU data protection law. Contact data, namely an email address, was stored in a separate data file, used for a lottery and subsequently deleted. The usage data was stored on servers of the Technische Universität Darmstadt, which are also subject to EU data protection law.

5.3.6 Results

A repeated measures MANOVA[13] showed significant differences for privacy knowledge, privacy awareness and behavior (privacy conditions on the smartphone, getting informed about privacy, prompting others to protect their data) across the three surveys, indicating an effect of FoxIT use (see table 43). No significant differences were found for the use of security measures and the management of privacy settings on social network sites.

Regarding actual behavior, 10 out of 31 participants uninstalled at least one app during the two weeks use period. Seven participants uninstalled only one app, and one participant uninstalled two, four and eight apps, respectively. However, only six participants reported to have uninstalled these apps for privacy reasons.

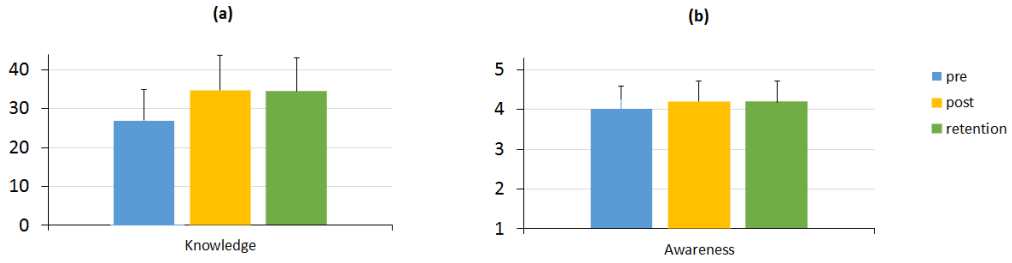

Figure 15: Privacy knowledge score (a) and privacy awareness (b) before using FoxIT (pre), after using FoxIT (post), and one week after the use period had ended (retention).

Privacy Knowledge. Post-hoc tests using Bonferroni correction showed a significant increase in privacy knowledge between the first and the second ($p < .001$) as well as the first and the third survey ($p < .001$). No differences were found between the second and the third survey (see fig. 15a).

Privacy Awareness. For privacy awareness, post-hoc tests showed a significant increase between the first and the second survey ($p < .05$, see fig. 15b).

[13] The assumptions of normality and homogeneity of variances were satisfied. Since the assumption of sphericity was violated, Greenhouse-Geisser corrections were applied.

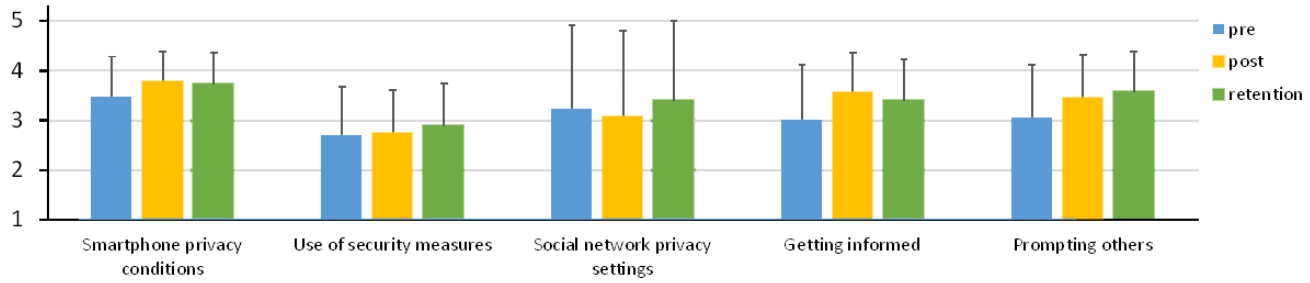

Figure 16: Privacy behavior before using FoxIT (pre), after using FoxIT (post), and one week after the use period had ended (retention).

Table 43: Results of the repeated measures MANOVA.

	df	F-value	Sig.	partial η^2
Knowledge	1.34, 40.34	40.02	$< .001^{***}$	0.57
Awareness	2, 60	3.90	$.025^{*}$	0.12
Smartphone privacy conditions	1.53, 45.83	4.27	$.03^{*}$	0.13
Use of security measures	2, 60	0.90	.41	0.03
Social network privacy settings	2, 60	1.12	.33	0.04
Getting informed	1.48, 44.24	7.55	$.004^{**}$	0.20
Prompting others	1.47, 44.14	7.33	$.004^{**}$	0.20

Privacy Behavior. Post-hoc tests showed significant differences for participants getting actively informed about privacy between the first and the second survey ($p < .01$). Significant differences were also shown for participants prompting others to protect their data between the first and the third survey ($p < .05$); differences between the first and the second survey closely failed significance ($p = .051$, see fig. 16).

5.4 Discussion

After using FoxIT for two weeks, participants in the field study showed higher values regarding knowledge about privacy related topics as well as an increased privacy awareness. They further reported to have improved the privacy conditions on their smartphone, actively informed themselves about privacy and also prompted others to protect their data. After a retention period of one week, privacy knowledge was still increased, indicating the potential for FoxIT use to lead to long-term effects. In fact, the frequency of prompting others to protect their data only differed significantly before using the app and after the retention period, although the differences between the pre- and post-use survey only closely failed significance. This delayed effect is plausible, considering participants first had to inform themselves about the topic as well as to change their own behavior before being knowledgeable enough to convince others to do the same. I found no long-term effects for participants getting actively informed about privacy. However, "getting informed" is sort of a finite activity and participants might have felt sufficiently informed after the period of use and thus made no additional effort to improve their knowledge. Privacy awareness, on the other hand, was actually supposed to be enhanced in the long term. Yet, considering the small sample size, the insignificant results might as well be caused by a lack of statistical power, since I applied the rather strict Bonferroni correction to the post-hoc tests. However, a selection of privacy consequences as identified in chapter 4 should be included in FoxIT to increase privacy awareness more permanently.
Participants did not report to use security measures more frequently or to have changed their privacy settings on social network sites after having used FoxIT. These results indicate that FoxIT supports a rather direct examination of privacy related topics, by increasing knowledge and awareness as well as

prompting participants to inform themselves and others about privacy. Since the main focus of FoxIT is on smartphone privacy, it is not surprising that the management of smartphone privacy conditions is the only concrete behavior participants changed due to FoxIT use. Although the lessons also cover topics related to social network privacy settings or security measures like encryption or passwords, this seems not sufficient to effectively cause a change in behavior.
In fact, the privacy behavior relating to the management of privacy settings on social network sites seems to be somewhat worse after using FoxIT, although the differences are not statistically significant. This might be because participants had a better understanding of how privacy settings work after using FoxIT and thus corrected the evaluation of their own privacy settings instead of actually changing their privacy settings on social networks. However, since the social network privacy setting value is slightly higher after the retention period, compared to the initial value, participants either adjusted their privacy settings somewhat delayed during the retention period or did rather quickly forget their newly gained knowledge about privacy settings and simply went back to their initial evaluation.
Overall, these results indicate that FoxIT in its current design seems promising in terms of increasing mobile users' privacy behavior on the smartphone, whereas it is not appropriate to increase privacy behavior beyond the mobile context. Furthermore, it should be noted that it is not sufficient to motivate users to always choose the most privacy-friendly alternative. Instead, they should be empowered to make informed decisions concerning their privacy. However, the approach to raise awareness about privacy issues (e.g., conduct an analysis of the current smartphone privacy conditions) and provide knowledge about privacy topics (e.g., implement knowledge lessons) seems to be suitable to support mobile users in making informed decisions.

5.4.1 Limitations

The present study suffers from several limitations that should be kept in mind when drawing conclusions based on the results. The study was carried out relying on a convenience sample with 19 out of 31 participants being undergraduate students. Thus, the sample is most likely skewed (i.e., younger, higher educated and eventually over-averagely tech-savvy) compared to the general population. Furthermore, since some participants knew the investigators carrying out the study, the results might suffer from social desirability bias as participants may have been afraid to stop using the app or say negative things about it, which could have hurt their friend's feelings. Further evaluation studies should be based on more heterogeneous and independent samples to allow for generalization.
Except for the number of apps being uninstalled during the study period, self-reported data was used to assess actual behavior. This data might be biased because participants euphemized their privacy efforts or simply did not recall their true privacy settings on the smartphone or on social network sites. Future studies are needed to verify the self-reported privacy behavior. Although it was decided to conduct a field study to evaluate FoxIT in a natural setting for maximizing ecological validity, this study design lacks the internal validity of a controlled lab study. It was not possible to control how participants informed themselves about privacy related topics beyond the use of FoxIT, either actively or passively, e.g., through media reports. However, participants were asked during the study if they had actively informed themselves. Still, I have no knowledge of any privacy-related events which were reported on in the media during the evaluation period.

5.4.2 Implications

The study results suggest that the improvement of mobile users' privacy through a knowledge and awareness enhancing application seems to be a promising approach. Contrary to most smartphone-based privacy enhancing tools proposed by other researchers, the content was not included in existing applications (e.g., the Play Store app installation interface), but in a separate app, so users can freely decide when they want to use it. This approach was chosen to make sure users are motivated to deal with privacy topics when they are using the tool. The great number of completed lessons, as well as the increased interest in privacy related topics indicate that the participants were indeed highly motivated to learn about privacy.

Thus, when providing a certain amount of information, it might be a good idea to conduct explicit privacy interventions instead of integrating content in existing frameworks.
I thus suggest the development of a dedicated privacy intervention. Following the example of FoxIT, I would implement this intervention as an app, thereby offering users the possibility to deal with it flexibly during their day, as most people carry their phone with them constantly.
FoxIT successfully increased people's privacy knowledge and their mobile privacy behavior, but failed to enhance privacy behavior in other domains, e.g., regarding the privacy settings in social networks. As FoxIT users could conveniently change their smartphone settings via a link implemented in the app, it might be necessary to apply further motivational elements to also prompt privacy enhancing actions in domains not associated with the smartphone. I describe the development of a concept for such motivational elements in the following section. As the results presented in chapter 6 suggest that people primarily aim to feel autonomous, competent, stimulated, and related to others when using digital applications, the motivational elements will be chosen in order to address the fulfillment of these psychological needs.
The evaluation of FoxIT further showed that privacy awareness could only be increased short-term. A more permanent increase of privacy awareness might be achieved by including more information about possible privacy consequences in the privacy lessons, as identified exemplary for the context of smart environments in chapter 4.

5.5 Motivational Elements

A popular framework for the development of motivational elements, which can be applied in interactive, technology-based products, is that of "persuasive technologies". The concept of persuasive technologies was first described by B.J. Fogg [73]. According to his definition, these are interactive technologies that aim to change the attitude or behavior of the respective user. Different mechanisms are applied, but all of them are characterized by the fact that no coercion is exerted and the influence is conscious. Persuasive technologies differ from, for example, nudges and advertising in that on the one hand a hidden influence can take place, and on the other hand no explicit interaction has to take place, whereas with persuasive technologies the influence must always take place through a conscious interaction with the respective technology.
The Persuasive Systems Design Model (PSD model) by Oinas-Kukkonen and Harjumaa [169] represents an empirical further development of this concept. They describe twenty-eight persuasive mechanisms that are assigned to the following categories:

- Support the user in fulfilling the primary task (e.g., by tailoring the information provided to the needs and characteristics of the respective recipient or by breaking down complex behaviours into small, easily achievable steps)
- Feedback and dialogue support (e.g., through suggestions for specific behaviours or rewards for desired behaviour)
- Increasing the credibility of the system (e.g., through the transfer of expertise or references to recognised external sources)
- Social support (e.g., through cooperation with others or social comparison)

The PSD model is shown in table 44.

Table 44: PSD model as described by Oinas-Kukkonen and Harjumaa [169]

System principle	Design principle
Primary Task Support	*Reduction:* A system that reduces complex behavior into simple tasks helps users perform the target behavior, and it may increase the benefit/cost ratio of a behavior.

Continued on next page

Table 44 – *Continued from previous page*

System principle	Design principle
	Tunneling: Using the system to guide users through a process or experience provides opportunities to persuade along the way. *Tailoring:* Information provided by the system will be more persuasive if it is tailored to the potential needs, interests, personality, usage context, or other factors relevant to a user group. *Personalization:* A system that offers personalized content or services has a greater capability for persuasion. *Self-monitoring:* A system that keeps track of one's own performance or status supports the user in achieving goals. *Simulation:* Systems that provide simulations can persuade by enabling users to observe immediately the link between cause and effect. *Rehearsal:* A system providing means with which to rehearse a behavior can enable people to change their attitudes or behavior in the real world.
Dialogue Support	*Praise:* By offering praise, a system can make users more open to persuasion. *Rewards:* Systems that reward target behaviors may have great persuasive powers. *Reminders:* If a system reminds users of their target behavior, the users will more likely achieve their goals. *Suggestion:* Systems offering fitting suggestions will have greater persuasive powers. *Similarity:* People are more readily persuaded through systems that remind them of themselves in some meaningful way. *Liking:* A system that is visually attractive for its users is likely to be more persuasive. *Social role:* If a system adopts a social role, users will more likely use it for persuasive purposes.
System Credibility Support	*Trustworthiness:* A system that is viewed as trustworthy will have increased powers of persuasion. *Expertise:* A system that is viewed as incorporating expertise will have increased powers of persuasion. *Surface credibility:* People make initial assessments of the system credibility based on a firsthand inspection. *Real-world feel:* A system that highlights people or organizations behind its content or services will have more credibility. *Authority:* A system that leverages roles of authority will have enhanced powers of persuasion. *Third-party endorsements:* Third-party endorsements, especially from well-known and respected sources, boost perceptions on system credibility. *Verifiability:* Credibility perceptions will be enhanced if a system makes it easy to verify the accuracy of site content via outside sources.
Social support	*Social learning:* A person will be more motivated to perform a target behavior if (s)he can use a system to observe others performing the behavior.

Continued on next page

Table 44 – *Continued from previous page*

System principle	Design principle
	Social comparison: System users will have a greater motivation to perform the target behavior if they can compare their performance with the performance of others. *Normative influence:* A system can leverage normative influence or peer pressure to increase the likelihood that a person will adopt a target behavior. *Social facilitation:* System users are more likely to perform target behavior if they discern via the system that others are performing the behavior along with them. *Cooperation:* A system can motivate users to adopt a target attitude or behavior by leveraging human beings' natural drive to co-operate. *Competition:* A system can motivate users to adopt a target attitude or behavior by leveraging human beings' natural drive to compete. *Recognition:* By offering public recognition for an individual or group, a system can increase the likelihood that a person/group will adopt a target behavior.

Based on the PSD model, systematic literature analyses have since been carried out mainly in the health sector [132, 130, 157, 177, 241, 249], but also with regard to environmental awareness [202]. The results suggest that the combination of as many mechanisms as possible from the three areas of support in fulfilling the primary task, feedback and dialogue support, and social support offers the best prospects of success. With regard to the concrete persuasive mechanisms, the most common positive effects were observed for the mechanisms reduction (breaking down complex behaviors into small, easily achievable steps), personalization, simulation (of desired behavior), adaptation (tailoring the information provided to the needs and characteristics of the recipient), memories (of desired behaviors), and suggestions (for desired behaviors).

5.5.1 Ideas for Implementation

Some of the design principles described above are already implemented in FoxIT. These are:

- Reduction: The information is split into smaller junks of courses and lessons.
- Tunneling: Users have to finish a lesson to unlock another lesson.
- Rewards: Users receive digital coins in the form of acorns and mushrooms by completing courses. They can further win trophies for showing certain behaviors, such as completing half of the courses.
- Suggestions: Users are prompted to perform privacy enhancing actions, such as checking their mobile privacy settings or adjusting their social networks privacy settings.
- Expertise: A lot of information, which covers different levels of expertise, is presented in the lessons.

Another idea for the application of the reduction design principle is to include a feature that allows users to define different goals for more privacy-friendly behavior, such as using encrypted messengers, adjusting privacy settings, or paying by cash.
Other design principles could be implemented as follows (see Appendix C for graphical prototypes):

- Tailoring: Show lessons dependent on the user's expertise, behavioral goals, or digital devices/applications/systems used

- Personalization: Include user name and avatar, include opportunity to individualize the app's design and adjust other features (e.g., the frequency of reminders) to personal needs and preferences
- Self-monitoring: Provide a graphical feedback mechanism for the achievement of the behavioral goals, implement a leveling system that allows users to level up when they complete lessons or achieve certain behavioral goals
- Praise: Show praising messages for successful behavior
- Reminders: Show push notifications to remind users of their behavioral goals. This could also be combined with suggestions by, e.g., showing users a notification when they apply an unwanted behavior such as using an unencrypted messenger and prompt them to use an encrypted messenger instead.
- Liking: Further improve the design of the app
- Social role: Include a coach, either the fox or a new virtual character
- Trustworthiness: Phrase the lessons as neutral as possible to avoid bias due to personal preferences, e.g., regarding the use of particular applications
- Credibility: Include sources for every statement
- Real-world feel: Highlight the app developers in an imprint
- Authority: Highlight the academic background in which the app was developed
- Verifiability: Make the sources for the knowledge content easily accessible
- Social comparison: Include leader boards, show notifications such as "20% of your contacts use [name of a privacy-friendly messenger]"
- Normative influence: Include a feature to invite others to use the app
- Social facilitation: Show notifications such as "20% of your contacts achieved [particular behavioral goal] today"
- Competition: Include leader boards and a leveling system, display the levels of contacts

Other design principles should not be pursued further, since they are not promising according to meta analyses carried out in other domains than privacy behavior [132, 130, 157, 177, 241, 249, 202] and do not fit to the app's concept. These are: Simulation, Rehearsal, Social learning, Cooperation, and Recognition.

5.6 Conclusion

The evaluation of FoxIT (see section 5.3) showed that it is promising to conduct an explicit privacy intervention that people can use at their own terms and conditions instead of integrating information in existing applications, e.g., an app store or social network, and presenting it when people lack time and motivation to deal with this information. As participants in the FoxIT evaluation were motivated to adjust their mobile privacy settings – which was facilitated by providing a direct link and explanation of these settings in FoxIT – but not their privacy behavior in other domains, it seems to be necessary to include further motivational elements in such a privacy-enhancing app. I outlined the implementation of such motivational elements based on the Persuasive Systems Design Model [169] in section 5.5. Further, information about possible consequences of using privacy-threatening technologies and services should be included in the lessons to increase lay users' privacy risk awareness. An exemplary list of such privacy consequences associated with living in smart environments is identified in section 4.1.

6 Reasons for Using Privacy-Threatening Technologies and Implications for Privacy Protection[15]

In addition to motivating users and providing them with knowledge regarding how to protect their privacy, it is also important to consider why they tend to use privacy-threatening devices and services in the first place. I identified four reasons for this usage in the interview study described in chapter 3: (1) Social pressure, (2) To keep oneself and others up-to-date, (3) Convenience, and (4) To express one's opinion. As the participants of the interview study frequently referred to social networks and messengers, and the sample considered in the study was rather small, I will consider this topic in more depth in this chapter.

6.1 Theoretical Background

According to Hassenzahl and Roto [95], users pursue two kinds of goals when using interactive products: do-goals and be-goals. While do-goals focus on the pragmatic aspect (i.e., they describe what the user wants to do/accomplish by using the product), be-goals concentrate on the hedonic aspect (i.e., they describe what the user wants to be/feel like by using the product). They describe the example of making a phone call (do-goal), which can satisfy completely different be-goals, depending on whom one calls (e.g., a spouse or a business partner). The authors refer to the ten psychological needs identified as being most important for people's well-being by Sheldon et al. [198] as promising candidates for describing the be-goals people aim to achieve when using interactive products:

- Autonomy: feeling that one's activities are self-chosen and self-endorsed
- Competence: feeling that one is effective in one's activities
- Relatedness: feeling close with others
- Self-actualization-Meaning: feeling that one is moving toward an ideal version of oneself
- Pleasure-stimulation: feeling pleased and stimulated
- Security: feeling that one's life is in order and predictable
- Popularity-Influence: feeling like one has the ability to make new friends and influence others
- Luxury: feeling that one is owning or being able to buy what one desires
- Self-esteem: feeling confident of oneself and personally worthy
- Physical thriving: feel physically well

In a subsequent study, Hassenzahl et al. [94] investigated seven of the ten primary psychological needs (money-luxery, self-esteem and physical thriving were excluded due to theoretical considerations) and indeed found that the level of need fulfillment produced by the interaction with a product was related to positive affect.
Based on this theoretical model, I conducted three studies, which are described in the following sections.

6.2 Identification of Do-goals and Be-goals – Quantitative Approach

I conducted two survey studies in order to identify the do-goals and be-goals users pursue by interacting with potentially privacy-threatening devices and services.

[15] based in part on the papers "Sina Zimmermann and Nina Gerber. Why Do People Use Digital Applications? A Qualitative Analysis of Usage Goals and Psychological Need Fulfillment. In: i-com 18.3 (2019), pp. 271–285" [263] and "Nina Gerber, Paul Gerber, and Maria Hernando. Sharing the 'Real Me' – How Usage Motivation and Personality Relate to Privacy Protection Behavior on Facebook. In: Human Aspects of Information Security, Privacy and Trust. Ed. by Theo Tryfonas. Cham: Springer International Publishing, 2017, pp. 640–655" [80]

6.2.1 Study I

The first survey study follows a qualitative approach with the aim to develop a categorization of do-goals for nine different use cases:

- Social networks
- Messengers
- Cloud services
- Digital assistants
- Game consoles
- Smart TVs
- E-Commerce
- Customer loyalty programs
- Market research studies

Recruitment and Participants. To recruit participants, the questionnaire link was sent to 270 German student mailing lists and distributed on social networks. A total of 217 participants completed the survey, of which 139 (64 %) were female and 76 (35%) male (2 –1% – did not specify their gender), ranging in age from 18 to 56 years (M=24.8, SD=6.3). Two Amazon coupons á 50€ and five Amazon coupons á 20€ were drawn among participants.

Study Procedure. All questions were implemented in SoSciSurvey [131] and presented in German. It took participants about 8 minutes to complete the whole survey (SD=2.8 minutes). Participants were asked independently for each use case to indicate which, e.g., social networks they used. They were provided with twenty text boxes and instructed to enter one social network per box, beginning with the one they use most frequently. Participants where then asked about the reasons or purposes they used social networks for and prompted to enter all reasons they were aware of. They were given an example of a possible reason to prompt them to describe the reasons as detailed as possible (e.g., "A possible reason could be 'To inform friends and family about my experiences while I'm travelling'."). This time, they were provided with twenty text boxes each on the left and on the right side with corresponding headlines and the instruction to enter a purpose for which they used social networks on the left and the corresponding social network they used for this purpose on the right side. The same approach was applied for the remaining use cases.

Evaluation Methodology. The responses were analyzed using open coding based on a grounded theory approach after Strauss and Corbin [214, 215]. Overall, I identified 93 categories of do-goals and various sub-subcategories (see Appendix D for the sub-categories).

Ethical Considerations. Ethical requirements with respect to participants' informed consent and data privacy were in line with the ethical guidelines provided by the Technische Universität Darmstadt. Participants were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, the surveys were implemented in SoSciSurvey [131], which stores all data in Germany and is thus subject to strict EU data protection law. Contact data, namely an email address, was stored in a separate data file, used for a lottery and subsequently deleted.

Results. Participants reported to use social networks primarily for obtaining information (e.g., about friends' and families' activities and experiences, about news and world affairs, about events), for contact purposes (e.g., keep in touch, get in touch, networking), to be entertained (e.g., by watching videos or pictures), to communicate (via chat or text messages), and to inform others (e.g., about one's experiences, events, or specific topics; see table 45).

Table 45: Social networks

Do-goal	N	%
Obtain information	220	35.8
Contact with others	120	19.5
Be entertained	49	8
Communicate	44	7.2
Inform others	42	6.8
View content	27	4.4
Exchange views/information	22	3.6
Share data	21	3.4
Make arrangements	20	3.3
Be inspired	12	2
Manage data	7	1.1
Have fun	4	0.7
Exchange data	3	0.5
Search for information	2	0.3
Buy things	2	0.3
Listen to music	1	0.2
Test out functions	1	0.2
Receive data	1	0.2
Participate in studies	1	0.2
Kill time	1	0.2
Sell things	1	0.2
Other	14	2.3
Total	615	100

Table 46: Messengers

Do-goal	N	%
Make arrangements	234	30.5
Communicate	219	28.6
Contact with others	128	16.7
Exchange views/information	74	9.6
Share data	44	5.7
Obtain information	20	2.6
Exchange data	15	2
Inform others	12	1.6
Be entertained	11	1.4
Have fun	3	0.4
View content	3	0.4
Receive data	1	0.1
Manage data	1	0.1
Other	2	0.3
Total	767	100

Table 47: Cloud services

Do-goal	N	%
Share data	96	24.6
Save files	74	19
Exchange data	71	18.2
Manage data	55	14.1
Access data from anywhere	29	7.4
Organize joint work	25	6.4
Receive data	21	5.4
Work together on documents	17	4.4
Other	2	0.5
Total	390	100

Messengers were reported to be used mostly for making arrangements (e.g., make appointments, about work or projects, plan activities), for communicating (e.g., in writing, verbally, to save money by avoiding phone calls), for contact purposes (e.g., keep in touch, get in touch), and for exchanging (e.g., information, about study contents; see table 46).

Participants reported to use cloud services mainly for sharing data (e.g., study materials, pictures), for saving files (e.g., backup, save documents), for exchanging data with others (e.g., study materials, pictures), and for managing data (e.g., synchronize data across devices; see table 47).

Digital assistants were reported to be used primarily for operating particular applications (e.g., set a timer, weather forecasts, write notes, making calls), and searching for information (e.g., navigating; see table 48).

Participants reported to use game consoles mostly for playing games (e.g., old/retro games, party games, SingStar, sports games), for being entertained, for having fun, and for viewing content (e.g., via DVD, Netflix; see table 49).

SmartTVs were reported to be used primarily for viewing content (e.g., TV series, films, videos; see table 50).

Table 48: Digital assistants

Do-goal	N	%
Operate particular applications	13	28.9
Search for information	12	26.7
Make entries without having to operate the device	5	11.1
Have fun	3	6.7
Operate device conveniently	3	6.7
Get help with operation of the device	2	4.4
Communicate	2	4.4
Test out functions	2	4.4
Be entertained	2	4.4
Show off the device	1	2.2
Total	45	100

Table 49: Game consoles

Do-goal	N	%
Play games	103	49.5
Be entertained	28	13.5
Have fun	23	11.1
View content	19	9.1
Relax	8	3.8
Pause, deflect	5	2.4
Experience success	4	1.9
Spend one's free time	3	1.4
Experiences with friends	2	1
Kill time	2	1
Participation in studies	1	0.5
More convenient operation	1	0.5
Other	9	4.3
Total	208	100

Table 50: Smart TVs

Do-goal	N	%
View content	40	81.6
Listen to music	3	6.1
Save files	2	4.1
Operate device conveniently	2	4.1
Receive data	1	2
Play games	1	2
Total	49	100

Table 51: E-Commerce

Do-goal	N	%
Buy things	763	99.6
Sell things	3	0.4
Total	766	100

Table 52: Customer loyalty programs

Do-goal	N	%
Receive bonuses	72	48
Gain financial benefits	63	42
Get service benefits	8	5.3
Use out of habit	2	1.3
Buy things	2	1.3
Obtain information	2	1.3
Communicate demand, influence supply	1	0.7
Total	150	100

Participants reported to use E-Commerce services and applications mainly for buying things (e.g., special products, to save money, to shop conveniently, to save time, have a wide choice, buy locally unavailable products), and only very rarely to sell things (e.g., used products; see table 51).
Participants stated to participate in customer loyalty programs primarily for receiving bonuses (e.g., vouchers, products), and for gaining financial benefits (e.g., discounts, cash; see table 52).
The main reasons for my participants to participate in market research studies are receiving compensation (e.g., participate in lotteries, get money), helping others (e.g., college students, researchers), supporting science, and being interested in the topic of investigation; see table 53.

6.2.2 Study II

The second survey study follows a quantitative approach, with the aim to investigate the importance of the do-goals identified in the first study, as well as the be-goals proposed in the literature [198, 95, 94] for the use of social networks, messengers, cloud services, digital assistants, game consoles, E-commerce, and the participation in consumer loyalty programs and market research studies.
Recruitment and Participants. Participants were recruited via the "clickworker" [88] panel. A total of 246 participants completed the survey, of which 112 (46%) were female and 134 (54%) male, ranging in age from 18 to 70 years (M=36.07, SD=11.46). Participants received a compensation of 3.50€ for their participation.
Study Procedure. All questions were implemented in SoSciSurvey [131] and presented in German. It took participants about 21 minutes to complete the whole survey (SD=6.6 minutes). Participants were asked independently for each use case to indicate how often they used, e.g., social networks (on a scale from 1–never to 5–very frequently). They were then asked to indicate how often they pursued the different do-goals identified in the first study[16] (again on a scale from 1–never to 5–very frequently). Finally, they were asked to indicate on a 5-Point-Likert scale (from 1–strongly disagree to 5–strongly agree) whether they were feeling like the ten psychological needs described by Sheldon et al. [198] were fulfilled through using, e.g., social networks. I used the Needs Scale developed by Diefenbach, Lenz and Hassenzahl [55] to assess need fulfillment.

[16] I only included the do-goals that were mentioned by more than just a few people in the first study to maintain the duration of the study at an appropriate level.

Table 53: Market research studies

Do-goal	N	%
Get compensation	49	37.4
Help others	20	15.3
Support science	13	9.9
Participation out of interest in the topic	12	9.2
Exert influence	8	6.1
Be entertained	5	3.8
Increase self-awareness	5	3.8
Have fun	4	3.1
Support market research	3	2.3
Satisfy curiosity	3	2.3
Receive bonuses	2	1.5
Receive test products	2	1.5
Participate in studies	1	0.8
Kill time	1	0.8
Other	3	2.3
Total	131	100

Ethical Considerations. Ethical requirements with respect to participants' informed consent and data privacy were in line with the ethical guidelines provided by the Technische Universität Darmstadt. Participants were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, the surveys were implemented in SoSciSurvey [131], which stores all data in Germany and is thus subject to strict EU data protection law.

Results. Participants reported to use social networks regularly for various reasons, but most often for watching videos and being entertained (see table 54), whereas messengers were reported to be used most often for keeping in touch with friends and communicating cheaply with others (see table 55). In line with this, participants reported to fulfil a broad range of needs when using social networks (see fig. 17), whereas the use of messengers was mainly associated with feeling related (see fig. 18). However, participants also indicted to feel more related with others than being stimulated when using social networks.

Cloud services were reported to be used primarily for saving documents and pictures, accessing files from anywhere, and synchronizing files across devices (see table 56). In line with this, the feelings reported to be mostly associated with the use of cloud services were competence and autonomy (see fig. 19).

Digital assistants were reported to be used mainly to check them out and to search for particular information, such as directions for navigation (see table 57). Consequently, the use of digital assistants was mainly related to feeling stimulated, competent and autonomous, although none of the psychological needs was reported to be fulfilled thoroughly by the use of digital assistants (see fig. 20).

Participants reported to use game consoles primarily to be entertained, but also to relax, spend free time, play alone, and to distract themselves (see table 58). In line with this, the main feeling reported to be associated with the use of game consoles is stimulation (see fig. 21).

Smart TVs were reported to be used most often to watch movies and series, either in general or because they offer the possibility to watch these contents flexibly in terms of time (see table 59). Consequently, participants reported to mainly feel stimulated and autonomous when using smart TVs (see fig. 22).

E-Commerce services and applications were reported to be used mostly in order to have a wide choice and to compare and purchase products (see table 60). The use of E-Commerce services and applications was reported to be related to feeling autonomous, but also stimulated and luxurious (see fig. 23).

Participants further reported to participate in customer loyalty programs due to the possibility to save money and get a discount on their purchases (see table 61), whereas participation in market research studies

Table 54: Social networks

Do-goal	N	M	SD
Watch videos	227	3.77	1.194
Be entertained	226	3.60	1.230
View pictures	228	3.52	1.207
Inform myself about certain topics	227	3.39	1.216
Keep in touch with friends	225	3.35	1.345
Communicate with friends	225	3.31	1.339
Keep in touch with acquaintances	225	3.21	1.280
Contact people already known to me	225	3.20	1.267
Maintain contact with people living far away	226	3.19	1.317
Inform myself about activities/experiences of my friends	226	3.16	1.303
Inform myself about personal news from other people	226	3.13	1.257
Inform myself about the news / world affairs	225	3.10	1.326
Inform myself about events	226	3.08	1.309
Keep in touch with “old” friends I don’t meet often	226	3.08	1.304
Network with other people	225	3.03	1.280
Share pictures with other people	225	2.88	1.364
Keep in touch with my family	224	2.86	1.429
Inform me about strangers	226	2.80	1.252
Inform me about my family’s activities/experiences	225	2.77	1.398
Inform other people about my experiences	225	2.71	1.337
Plan activities with other people	224	2.64	1.305
Make appointments with other people	225	2.56	1.308
Inform other people about my experiences during a trip	224	2.48	1.372
Inform me about offers and novelties of companies	222	2.47	1.235
Inform other people about events	223	2.39	1.286
Get in touch with unknown/new people	224	2.38	1.254
Inform me about vacancies	223	2.19	1.260
Exchange information with other persons about study contents/organisation or work contents/organisation	221	2.13	1.253
Make arrangements about work/projects	222	2.12	1.238
Inform me about study contents/organisation or work contents/organisation	223	2.11	1.274

was reported to be undertaken in order to make money, support science, and help scientific researchers and college students (see table 62). No particular psychological need seems to be fulfilled by participating in customer loyalty programs (see fig. 24), while participation in market research studies seems to trigger feelings of autonomy, popularity-influence, and stimulation (see fig. 25).

6.3 Identification of Do-goals and Be-goals – Qualitative Approach

To gain a more thorough understanding, especially regarding the importance of be-goals in terms of using digital applications, I describe the results of an additional interview study including a card sorting task. To keep the length of the study in a reasonable time frame, only five of the nine use cases considered in the online surveys described in section 6.2 were included in the interviews.

In the following, I will liberally use quotations from the article published in “i-com” (2019) without explicitly marking each quote.

Table 55: Messengers

Do-goal	N	M	SD
Keep in touch with friends	229	4.01	0.996
Communicate cheaply with other people	230	3.92	1.132
Communicate in writing with other people	229	3.71	1.227
Keep in touch with acquaintances	229	3.67	1.065
Arrange appointments for meetings with friends	228	3.67	1.087
Exchange information with other people	229	3.66	1.127
Plan joint activities with other people	228	3.56	1.111
Share personal news with other people	227	3.54	1.126
Maintain contact with people living far away	228	3.48	1.243
Keep in touch with the family	229	3.47	1.293
Share pictures with other people	228	3.46	1.211
Send greetings to other people (e.g. during a trip, on a birthday)	229	3.45	1.182
Share pictures with other people	229	3.44	1.204
Keep in touch with “old” friends I don’t meet so often	229	3.34	1.203
Share funny content with other people	229	3.32	1.287
Find out about friends’ activities	229	3.26	1.184
Inform other people about my own experiences	229	3.21	1.147
Make small talk	229	3.13	1.293
Contact other people	230	3.07	1.293
Arrange appointments for meetings with the family	228	3.01	1.271
Exchange information about work/projects	226	2.54	1.226
Make arrangements about the work/projects	227	2.41	1.242
Exchange information with other people about study contents/organisation or work contents/organisation	225	2.38	1.314
Make phone calls	228	2.38	1.216
Agree on study contents/organization or work contents/organization	225	2.25	1.262
Find out about study contents/organisation or work contents/organisation	224	2.25	1.273
Arrange professional appointments	226	2.00	1.231

Table 56: Cloud services

Do-goal	N	M	SD
Save documents	154	3.30	1.382
Access my files from anywhere	153	3.18	1.462
Save pictures	154	3.09	1.434
Synchronize files across multiple devices	154	3.04	1.525
Receive documents	153	2.96	1.418
Receive pictures	155	2.79	1.506
Create a Back Up of my files	154	2.76	1.513
Share documents with other people	153	2.71	1.365
Exchange documents with other people	152	2.68	1.349
Share large files/quantities of files with other people	154	2.67	1.495
Share pictures with other people	152	2.65	1.406
Work on documents together with other people	153	2.48	1.415
Save study/work materials	151	2.41	1.511
Organize the joint work with other people	152	2.31	1.406
Receive study/work materials	151	2.30	1.432
Exchange study/work materials with other people	152	2.28	1.373

Table 57: Digital assistants

Do-goal	N	M	SD
Check it out	88	3.00	1.278
Search for particular information (e.g., directions)	91	2.93	1.281
Operate device easily	88	2.75	1.324
Be entertained/have fun	88	2.63	1.307
Make entries without having to operate the device (e.g., in a car)	88	2.52	1.414
Let me be helped with the operation of the device	88	2.27	1.239
Set the timer	87	2.24	1.438

Table 58: Game consoles

Do-goal	N	M	SD
Have fun	128	3.85	1.255
Relax	127	3.38	1.321
Spend free time	128	3.32	1.322
Distract me/take a break	128	3.27	1.350
Let me entertain myself alone	128	3.23	1.433
Play with friends	128	2.97	1.414
Experience success	128	2.90	1.339
Be entertained together with friends	127	2.89	1.376
Play sports games	128	2.67	1.415
Experience things with friends	128	2.66	1.353
Play party games with other people	126	2.54	1.401
Watch movies/series on DVD or BluRay	128	2.52	1.375
Play “old” games (e.g., SuperMario Kart) with other people	127	2.51	1.379
Use streaming services (e.g., Netflix, Amazon Prime)	128	2.31	1.510
Play SingStar with friends	128	1.70	1.213

Table 59: Smart TVs

Do-goal	N	M	SD
Watch movies	111	3.56	1.425
Watch series	110	3.45	1.463
Watch videos	113	3.32	1.441
Watch missed movies/series	111	3.15	1.460
Listen to music	113	2.61	1.423

Table 60: E-Commerce

Do-goal	N	M	SD
Have a wide choice	236	4.25	0.981
Compare prices	235	4.12	0.977
Purchase particular products	236	4.12	0.986
Buy comfortably as products are delivered	236	3.94	1.084
Buy locally unavailable products	235	3.92	1.028
Buy comfortably as I save my way to the city/shop	236	3.85	1.188
Save money	236	3.79	1.102
Save time as the way to the city/business is no longer necessary	236	3.78	1.151
Get products delivered quickly	236	3.78	1.151
Save time by purchasing products in a more targeted way	236	3.77	1.152
Get a lot of information (e.g., through reviews) and thus be able to make well-founded decisions	236	3.72	1.149
Buy products if this would not be possible offline (e.g., due to opening hours etc.).	236	3.62	1.195
Make multiple purchases from a single customer account	235	3.23	1.376
Buy exceptional, unique products	235	3.16	1.211
Buy products secondhand	236	2.93	1.278
Pay with vouchers	236	2.83	1.359
Fulfil ecological and fair trade criteria when purchasing	234	2.22	1.143

Table 61: Customer loyalty programs

Do-goal	N	M	SD
Save money	148	3.72	1.344
Get discount on my purchase	146	3.61	1.411
Get money back	148	3.16	1.590
Get service benefits	148	3.15	1.421
Get products as bonuses	147	3.07	1.525
Get vouchers	148	3.05	1.451
Pay with points	148	3.02	1.523

Table 62: Market research studies

Do-goal	N	M	SD
Make money	229	4.06	1.011
Support science	229	3.56	1.132
Help scientific researchers	230	3.49	1.174
Help college students	230	3.41	1.257
Improve the service in question	229	3.37	1.173
Support market research	230	3.31	1.235
Learn interesting things about the respective topic	230	3.26	1.197
Improve supply	230	3.23	1.173
Have fun	230	2.96	1.202
Satisfy curiosity	230	2.85	1.271
Be entertained	230	2.60	1.228
Learn new things about myself	230	2.54	1.343
Participate in lotteries	230	2.35	1.251

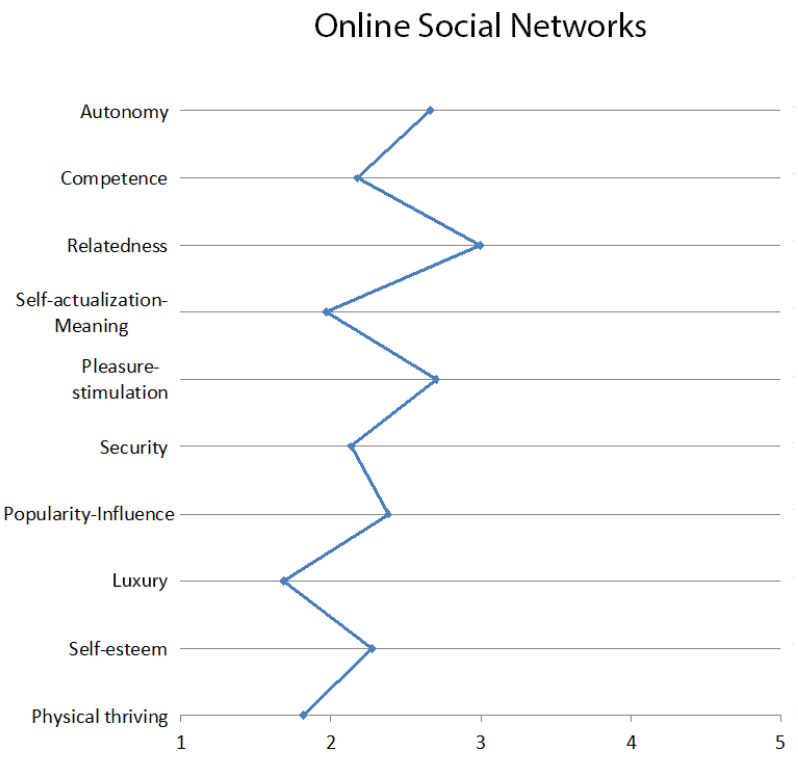

Figure 17: Needs associated with using Online Social Networks.

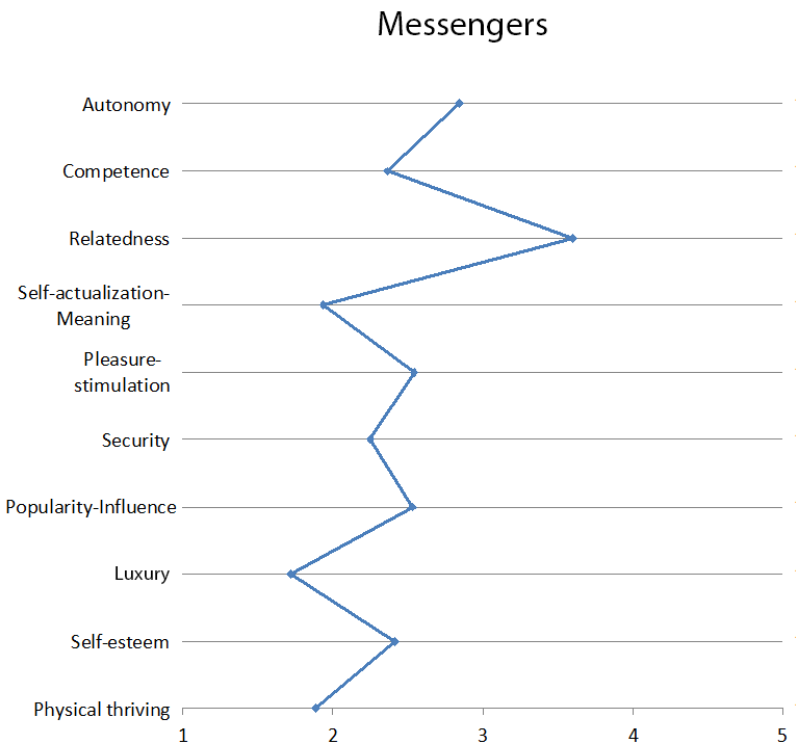

Figure 18: Needs associated with using messengers.

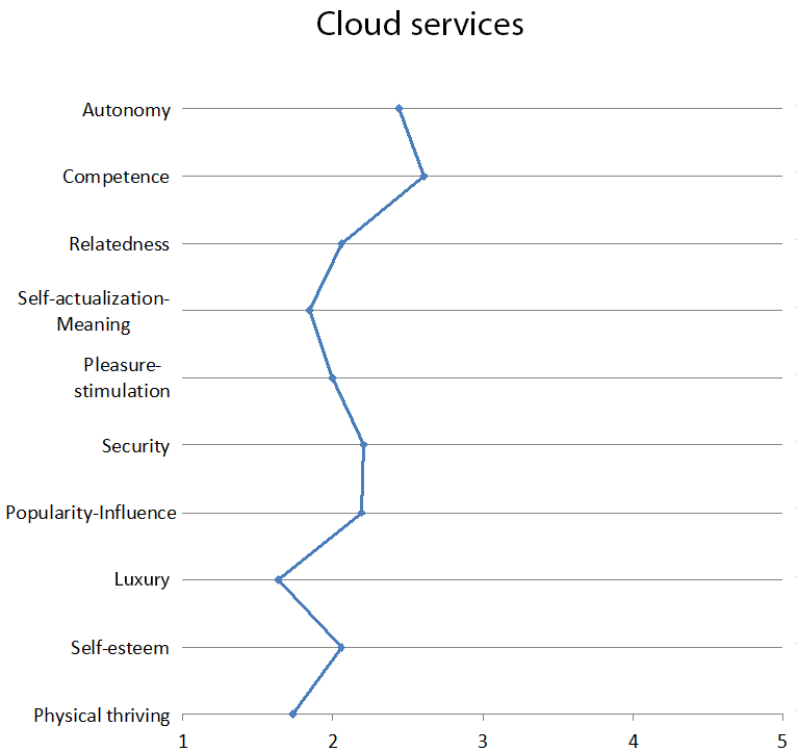

Figure 19: Needs associated with using cloud services.

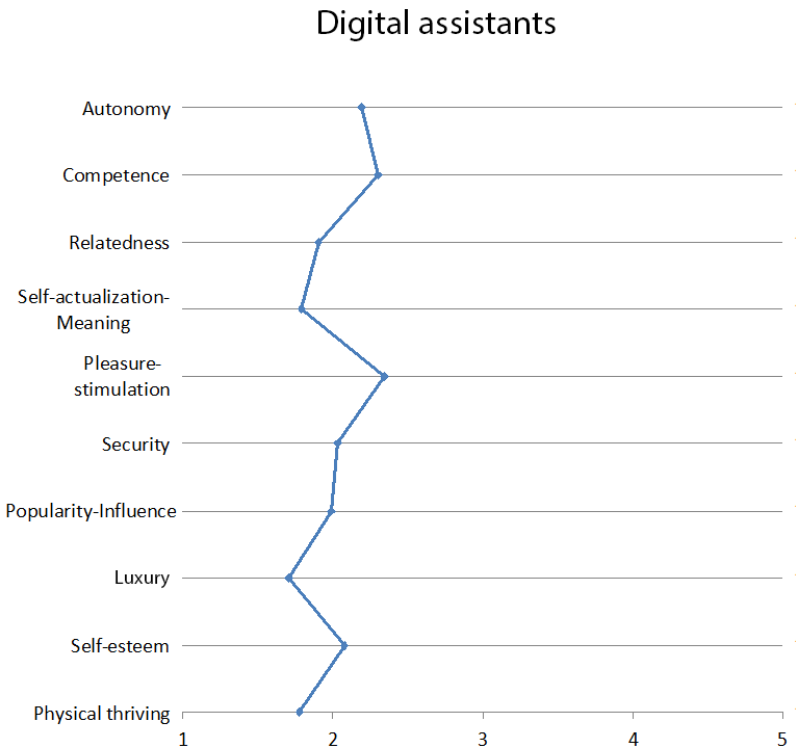

Figure 20: Needs associated with using digital assistants.

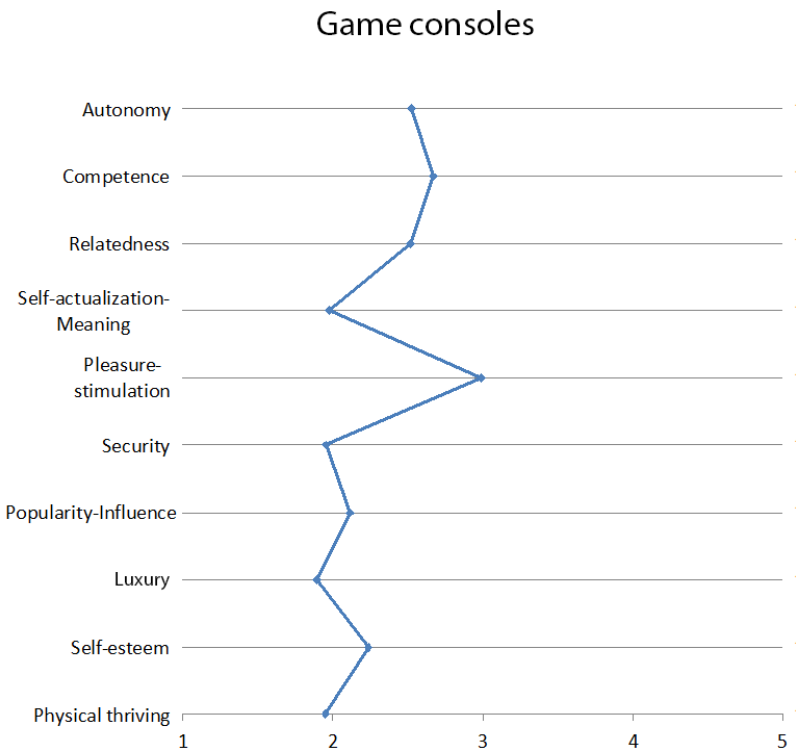

Figure 21: Needs associated with using game consoles.

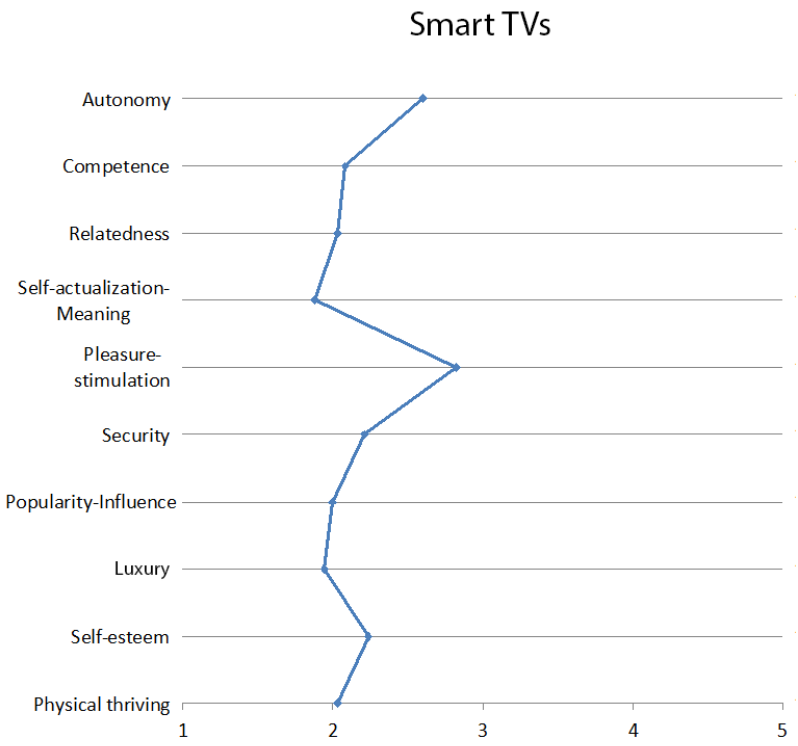

Figure 22: Needs associated with using smart TVs.

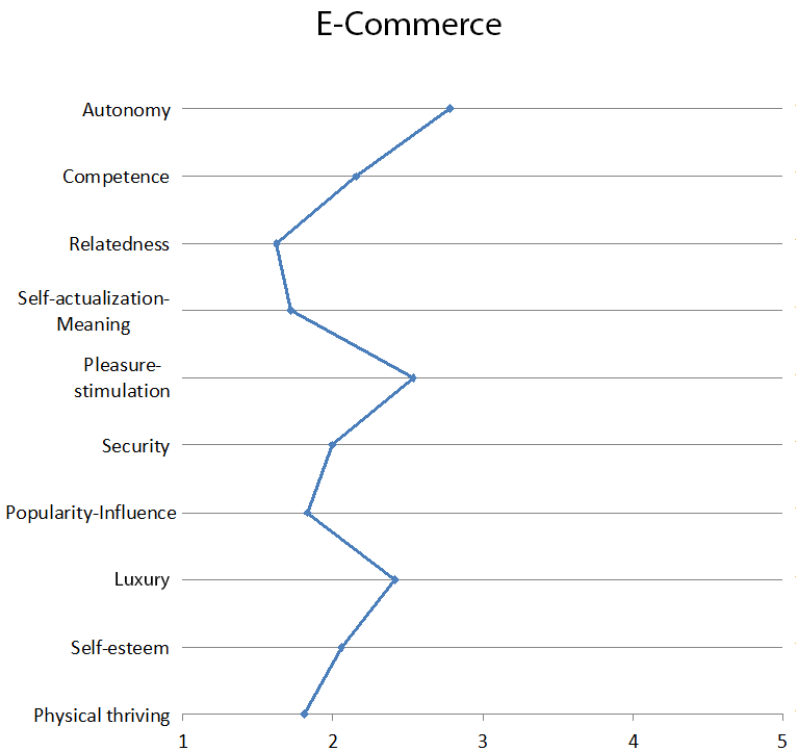

Figure 23: Needs associated with using E-commerce services.

Figure 24: Needs associated with using costumer loyalty programs.

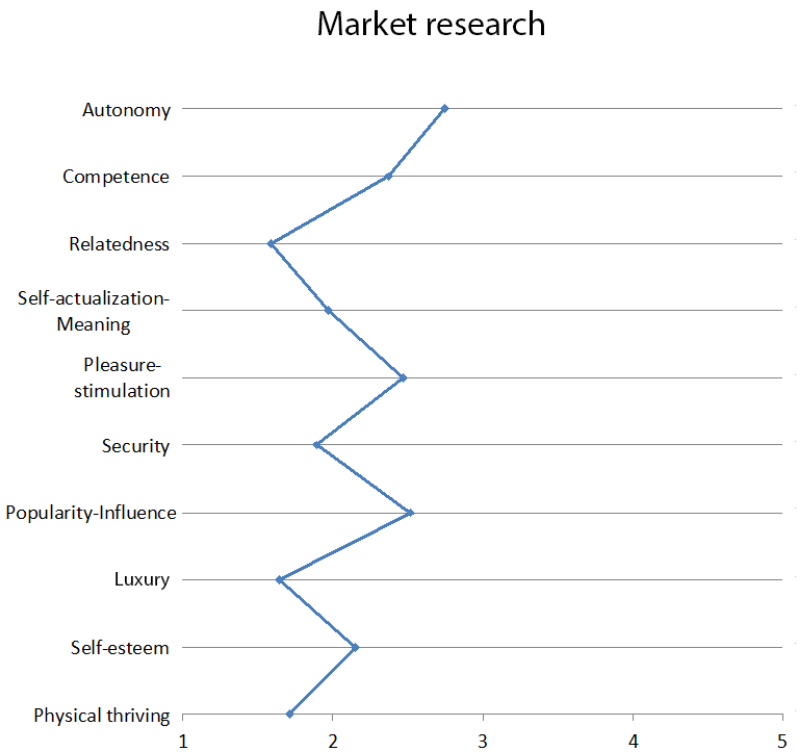

Figure 25: Needs associated with participating in market research studies.

6.3.1 Methodology

The interviews took between 38 and 67 minutes, with an average of 49 minutes. Three pilot interviews were conducted to check the soundness of the interview guide and process. The interview guidelines were improved iteratively, based on the feedback of pre-study participants and own impressions during the pilot interviews.

Recruitment and Participants. Participants were recruited by inviting friends and family members who might be interested in participating. In addition, an invitation email was sent via the mailing list that is used to promote studies among under-graduate psychology students at the Technische Universität Darmstadt. People interested in participating were told the interview topic would be their usage of digital applications in order to prevent biasing participants towards the topic of usage goals (do-goals) or psychological need fulfillment (be-goals). Undergraduate students received course credits, whereas non-student participants participated voluntarily without receiving any compensation.

Seventeen people participated in the study (11 female, 6 male) whose age ranged between 19 and 28 years (M=22.88, SD=2.47). Except for three participants, all participants were undergraduate or graduate students of psychology or psychology in IT. None of the participants were familiar with the concept of the ten psychological needs postulated by Sheldon et al. [198].

Study Procedure. The interviews comprised four parts:

Welcome and general instructions: Participants were welcomed and provided with information about the study. They then signed the consent form, which allowed recording of the interview. Afterwards, they were informed in more detail about the study procedure.

Use of digital applications (messengers, social networks, cloud services, digital assistants and Smart TVs): Participants were asked whether they used each of the digital applications considered in this study.

If they reported to use an application, they were asked what, e.g., social network, they used, for which reasons, in which situations, for which contents, and –if applicable–together with whom. They were also asked to name benefits and dis-advantages of using the respective digital application. They were further asked whether they have ever uninstalled an application in the past, and if they did, why.

If they reported not to use an application, they were asked why or in which specific situation they refrain from using it or why they have uninstalled the application in the past. Again, they were also asked to name benefits and disadvantages of using the digital application.

Presentation of the ten psychological needs: Prior to the card sorting task, the ten psychological needs postulated by Sheldon et al. [198] were explained to the participants. For this purpose, each psychological need was printed on a card showing the name of the psychological need and a brief explanation text.

Card sorting task: Finally, participants conducted a ranking of the ten psychological needs with regard to how important these needs are for their usage of a particular digital application. Participants were told that they only had to include those psychological needs that they considered to be relevant for using the respective application, i.e., psychological needs that were not considered to be relevant were excluded from the ranking. The ranking could be adjusted later on, in case participants realized retrospectively there was a psychological need missing or of greater importance than they had initially assumed. Additionally, participants were asked to explain their rankings.

Evaluation Methodology. The interviews were transcribed and responses were analyzed using open coding following the grounded theory approach [214, 215]. The final codebook includes seven main categories, i.e., reasons for using each digital application (messengers, social networks, cloud services, digital assistants, and Smart TVs), and concerns and reasons for refraining from using digital applications.

Ethical Considerations. Ethical requirements for research involving human participants are provided by an ethics commission at the Technische Universität Darmstadt. All relevant ethical requirements regarding research with personal data were met. Participants were first informed about the procedure of the study, after which they could decide to proceed or stop the interview. They were further told that they could stop the interview at any time without stating reasons and in this case all data collected so far would be deleted. They were further assured that the collected data would only be used for research purposes, their

identity would not be linked to their responses, and their data would only be handled by members of my research group and never passed on to third parties.

6.3.2 Results

First, I describe the responses of the interview part that focuses on why people use the different digital applications considered in this study, i.e., their do-goals. Then I present the results of the card sorting task, which indicate how important the different psychological needs (i.e., be-goals) are for participants' use of these digital applications.

Messengers. Almost all participants reported to use messengers to communicate, exchange news, and to stay in touch, particularly with people abroad ("My family is often scattered all over the world, hence [I use messengers to] keep in contact" (P17)). Several participants also stated that they used messengers to communicate with a working group, for information exchange in general, and for organizational contents, such as arranging appointments.

Social Networks. Many participants reported to use social networks in order to stay up-to-date with friends abroad ("Gaining insight into the life of people, which I have met abroad, without communicating constantly" (P8)), keep in touch, for communication in general, and to establish contact with acquaintances of whom the participants do not have any further contact information. Many participants also reported to use social networks to look at posted images or posted news, and to be entertained and amused.

Furthermore, many participants reported self-portrayal to be an important reason for using social networks ("In principle, Instagram is used for self-portraying" (P2)).

Cloud Services. Most participants reported to use cloud services mainly in a professional context, i.e., for storing educational material and documents concerning their studies, for exchanging files in groups, and for the organization of their work. Moreover, almost all participants reported to use cloud services to share files and enabling other people to access their files, especially if they want to share these with a large amount of people.

Digital Assistants. Although less participants reported to use digital assistants, some participants emphasized benefits of using digital assistants, such as the opportunity to make fast, voice-based entries and thus convenience due to using voice-based entries instead of using the keyboard. Some participants also stated to use or to have used digital assistants for fun, i.e., by asking Siri funny things ("At the time when I got my iPhone, I asked Siri a few things just for fun" (P9), "It was a funny gadget, but not very useful" (P15)).

Smart TVs. Most participants mentioned the comfortable and easy use of streaming services or the possibility to watch videos as the major reason to use a Smart TV. Some participants also emphasized the benefit of being independent of television programs and having the opportunity to stream shows and movies one has missed watching via media libraries. Some participants even reported to have bought a Smart TV because they wanted to own an extraordinary device ("Smart TVs are more expensive [...], anyway I feel great as a result of owning a Smart TV" (P17)).

Card Sorting. The top 3 psychological needs associated with the use of the digital applications considered are depicted in fig. 26. Overall, relatedness, pleasure-stimulation, autonomy and competence were reported to be the most important needs associated with the use of all digital applications considered in this study. While relatedness is the most important psychological need related to the use of messengers and social networks, it is not among the three most important needs associated with using cloud services, digital assistants, and Smart TVs. This is not surprising, considering that messengers and social networks were primarily designed for the purpose of interacting with other people. Pleasure-stimulation, on the other hand, is an important psychological need for the use of all digital applications investigated, except for cloud services, which indeed seem to be primarily used for task fulfillment instead of pleasure. Further, the regular communication with other people via messengers seems to give people a feeling of security. The use of social networks, however, is rather associated with personal grow, i.e., self-actualization-meaning. Due to the small sample size the results regarding digital assistants and Smart TVs should be handled with caution.

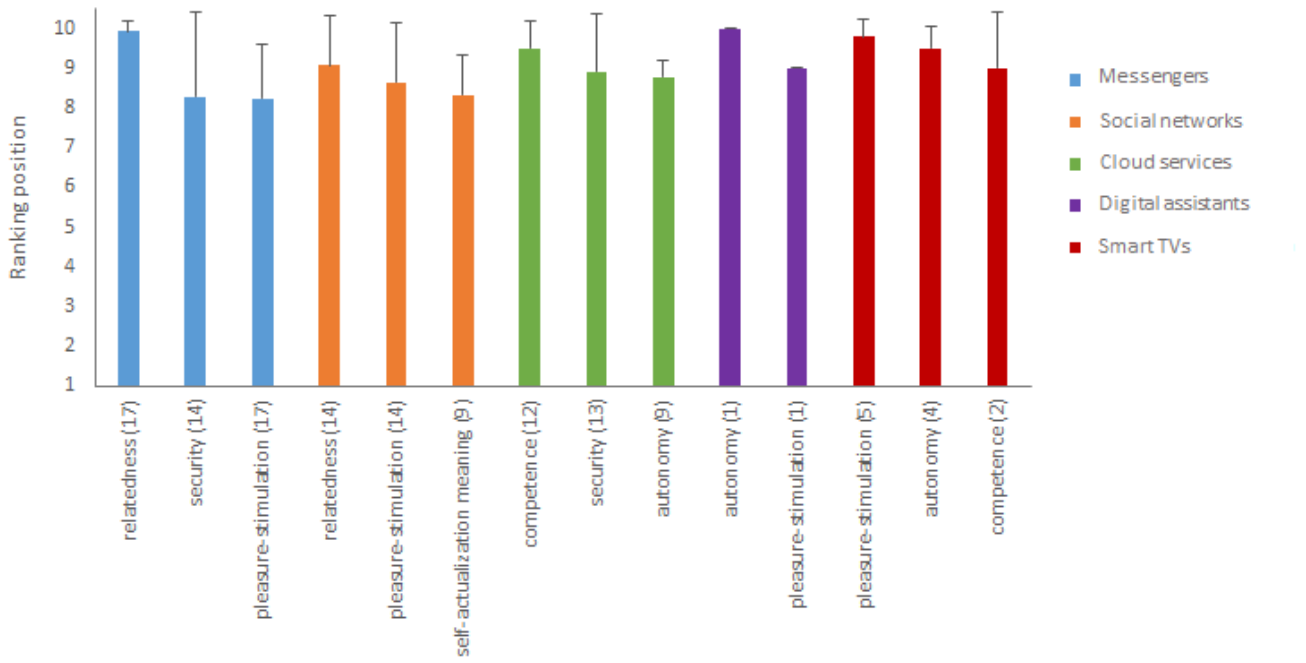

Figure 26: Most important psychological needs for each digital application.

Privacy concerns and reasons to refrain from using digital applications. Participants frequently reported to be concerned about data abuse ("In the end, they might even sell data to health insurance companies or other insurance companies and hence you can't take out insurance [...]" (P9)), eavesdropping on data ("I don't need a messenger spying on data on my cell phone" (P1), "I'm using Telegram for private discussions since I get somewhat paranoid about someone unauthorized eaves-dropping" (P14)) or unauthorized collection of their data ("One more device that records movements and decisions, somehow collects data or is at least connected [to the Internet]" (P8)). Regarding the use of Smart TVs, some participants also reported to be concerned about privacy infringement, particularly since these devices usually include a microphone and a camera which could be misused for recording them without their permission ("All devices with built-in microphone and camera can be hacked, consequently your privacy is threatened" (P13)). Moreover, some participants named (personalized) advertisements as a negative consequence of using digital applications, often associated with the use of social networks ("[...] Facebook is using data for commercial purposes, this has to be confirmed by accepting the general terms and conditions, thus much advertisement data will be collected" (P4)).
Some participants also reported to refrain from using various digital applications to protect their privacy ("Until now, I'm not using digital assistants, since I am concerned that such applications always listen" (P1)). One participant even stated to refrain from using social networks such as Facebook due to the belief that it is unethical to earn money by selling data ("People earn money in this way, I don't like the way they earn money, it is not ethical" (P7)).

6.3.3 Limitations

This study suffers from several limitations, which should be kept in mind when drawing conclusions based on the results. First, the results are based on a small sample size, especially concerning the card sorting task, which only those participants conducted who reported to actively use the respective digital application. This led to a very small sample size concerning the use of digital assistants and Smart TVs and therefore threatens the validity of the results for these applications. Second, since most participants were students of psychology, the sample is most likely skewed, i.e., younger, higher educated and mostly female, which is not representative for the general population. Third, participants were allowed to include all psychological

needs that they considered to be important when using the respective application, in the card sorting task, independent of whether this need is actually fulfilled by using the application. Thus, each psychological need could also be expressed as something participants would wish to be satisfied by using the application. Hence, it was difficult to distinguish afterwards which needs participants considered to be fulfilled by using the application and which ones participants would wish to be fulfilled. Further, each participant has their own concept of the psychological needs, even though all participants were presented the same definitions of the psychological needs. Hence, different concepts could have led to different rankings between the participants.

6.4 Relationship between Needs and Privacy Protection Behavior on Facebook

Although according to the results of the interview study described in section 6.3, their privacy concerns do not seem to stop people from using messengers, social networks, and cloud services, it is expected that they deploy certain strategies to protect their privacy when using these devices and services (see chapter 3). This has been repeatedly shown in prior studies especially for the use of social networks [52, 54, 254], being the service with the most extensive set of possibilities for privacy management. However, it is unclear whether the be-goals people pursue while using social networks relate to their deployment of certain privacy protection strategies. As such a relationship would implicate the use of approaches which are tailored to the be-goal or need they aim to fulfil for supporting users in their privacy protection efforts, I conducted a survey study to answer the following research questions:

RQ4d: Do Facebook users with strict and those with lax privacy settings differ pertaining to the needs/be-goals that motivate them to use Facebook (i.e. (a) autonomy, (b) competence, (c) relatedness, (d) meaningfulness, (e) pleasure-stimulation, (f) security and (g) popularity-influence)?

RQ4e: Do Facebook users who deploy certain privacy protection strategies besides the management of privacy settings and those who do not differ pertaining to the needs/be-goals that motivate them to use Facebook (i.e. (a) autonomy, (b) competence, (c) relatedness, (d) meaningfulness, (e) pleasure-stimulation, (f) security and (g) popularity-influence)?

Facebook was chosen since it is by far the most popular social network within the western hemisphere nowadays [2]. Physical thriving and money-luxury were not considered in this study, since these were the needs considered least important for the use of social networks in the interview study and the card sorting task (see section 6.3). As self-esteem was also not reported to be one of the most important needs for the use of social networks, I decided to use the questionnaire developed by Diefenbach et al. [55] to assess need fulfilment related to the use of interactive products. This questionnaire focuses only on the seven needs that have repeatedly shown to be important for people regarding the use of interactive products, thus, self-esteem is also not considered in this study.
In the following, I will liberally use quotations from my article published in "Human Aspects of Information Security, Privacy and Trust" (2017) without explicitly marking each quote.

6.4.1 Related Work

A number of studies have dealt with the deployment of different privacy protection strategies by Facebook users. For example, Debatin et al. [52] showed that Facebook users who had recently experienced a personal privacy invasion were more likely to alter their privacy settings compared to users who just heard about a privacy invasion experienced by other users. Young and Quan-Haase [254] found that university students mainly adopted privacy protection strategies that restricted access to their personal data for different members of the Facebook community, rather than strategies that would allow them to control data access for third parties. Furthermore, they showed that university students do not use fictitious information as protection strategy, since this would lead to confusion among friends and peers. Another study by Staddon,

Acquisti and LeFevre [212] concerning the use of privacy protection strategies on Facebook not only showed that the controlling of post visibility is strongly correlated with the deletion of posts, but also that users who value privacy features most generally show more privacy actions.
Furthermore, the results of Peters, Winschiers-Theophilus and Mennecke [174] indicate that US users would rather remove friends from their contact list than change their privacy settings to restrict the visibility of their data, whereas Namibian users refuse from the deletion of friends due to the concern of being rude. Therefore, 50% of the participants reported that they restricted some friends from seeing all of their posts. They further showed that US users tend to update their privacy settings usually when they are looking for or after they found a new job.
Beyond culture, other demographic factors seem to influence privacy protection behavior as well. Female users are more likely to have a friends-only Facebook profile [216] and tend to use a more diverse set of technological privacy tools (i.e. protection tools implemented in the social network site itself) than males [246, 148], maybe because women generally have more privacy concerns related to safety (e.g., stalking) and therefore transfer their protection strategies to the online context. When it comes to teenagers, however, Feng and Xie [69] found that females are indeed more likely to set their profile to private and adopt more privacy-setting strategies, but do not express more privacy concerns. Their results further suggest that older teenagers tend to implement more privacy protection strategies (e.g., deleting someone from their friends list, deleting older posts, block people, untag photos), whereas younger adults are more likely to show a wider use of technological privacy tools than older adults [148], maybe due to greater knowledge of and skills in using these technologies.
Ross et al. [186] suggest that the motivation someone has to use Facebook (e.g., to communicate, seek social support, be entertained) might also be useful in understanding Facebook usage behavior. Using factor analysis, Sheldon [200] identified six motives for using Facebook: relationship maintenance, passing time, interacting in a virtual community, entertainment, coolness and companionship. Facebook usage for reasons of relationship maintenance was associated with a greater number of Facebook friends, whereas usage for entertainment purposes and passing time significantly predicted frequent change of one's Facebook profile. Further research on this topic [211] showed that Facebook users with high levels of self-disclosure were more satisfied with Facebook's ability to entertain and pass time. Furthermore, Hollenbaugh and Ferris [97] found that Facebook usage for exhibitionism and relationship maintenance is associated with larger amounts of disclosed personal information. They also showed that usage for relationship maintenance is associated with disclosing more breadth of information in Facebook, whereas the depth of information disclosure was found to be related to the usage motivation "interacting in a virtual community". The results of Waters and Ackerman [239] suggest that Facebook users disclose their data to share information with others, to store information and being entertained, to keep up with trends and to show off. On the other hand, Krasnova et al. [122] found evidence for an association between self-disclosure on Facebook and relying on the convenience for maintaining relationships, building new relationships and enjoyment.

6.4.2 Methodology

I conducted an online survey with 280 German Facebook users. All questions were implemented in SoSciSurvey [131] and presented in German. It took participants about 30 minutes to complete the whole survey.
Recruitment and Participants. To recruit participants, the questionnaire link was sent to 270 German student mailing lists. Of the respondents, 71.8% were female and 27.1% were male (1.1% did not specify their gender), ranging in age from 18 to 45 years (M=22.84, SD=3.76). Five Amazon coupons á 20€ were drawn among participants. Psychology students from the Technische Universität Darmstadt received course credits.
Questionnaire. Various items were used to assess need fulfillment, privacy settings, other privacy protection strategies and demographics. To increase reliability and validity, items are based upon previously validated instruments whenever available. Item formulation prompted participants to answer as accurately as possible. To achieve this goal, formulations like "What do you think..." or "Could you please estimate..." were avoided, and where possible it was spoken in terms of facts ("How often do you..." or "How many

times do you...” etc.). Additionally, items that asked for content that could not be easily found by the participants included click-path indications to point to where the content of the item could be found (e.g. for item PS03 “Home → Click on the lock symbol on the top right → ‘Who can see my stuff?”’). Two filtering questions were used to exclude participants who do not use Facebook on a regular basis and those who use it as part of their working activity and not for private purposes. Five items were used to assess the participants’ gender, age, level of education, nationality and duration of Facebook usage.

To assess need fulfillment trough Facebook usage, I used the Needs Scale developed by Diefenbach, Lenz and Hassenzahl [55]. The Needs Scale evaluates the extent to which an interactive product (e.g. Facebook) fulfills the seven postulated needs that are associated with the use of interactive products (autonomy, competence, relatedness, meaningfulness, pleasure-stimulation, security and popularity-influence). Items corresponding to each need are presented as continuation of the sentence “When using the product, I generally feel that...”. All items were measured on a 5-Point Likert scale (with 1=“strongly disagree” and 5=“strongly agree”).

Personality traits were assessed using the BFI-10 scale, a brief version of the Big Five Inventory developed by Rammstedt and John [181]. In this 10-item version, each Big Five personality construct is assessed with two items. All items were measured on a 5-Point Likert scale (with 1=“strongly disagree” and 5=“strongly agree”). The results regarding personality are not considered in this chapter, but can be found at Gerber et al. [80].

Thirteen items were used to measure participants’ privacy settings. The answer options matched the privacy setting options available on Facebook at the time of questionnaire development (12/20/2015). Four items corresponding to the deployment of other privacy protection strategies were developed in order to evaluate to which extent users do protect their private information from undesired (public) access. The items used to assess privacy settings (PS) as well as other privacy protection strategies (OS) are presented in table 63.

Table 63: Items used to assess privacy settings (PS) and the deployment of other privacy protection strategies (OS)

Nr.	Item
PS01	Is it possible to find your profile via Google or other search engines? Yes (6) No (0)
PS02	Have you ever changed the default privacy settings on Facebook? Yes (6) No (0) I don’t know (0)
PS03	Who can see your Facebook profile and its contents? Only you (6) User-defined (selected people and groups) (3) Only your Friends on Facebook (3) Friends except Acquaintances (3) Anyone on or off Facebook (0)
PS04	Do you have to agree first if other people try to tag you in a post/photo/video? Yes (6) No (0)
PS05	Who is able to see your e-mail address? Your Friends (4) Friends of Friends (2) Everyone (0)

Continued on next page

Table 63 – *Continued from previous page*

Nr.	Item
	Data not provided on Facebook (6)
PS06	Who is able to see your telephone number? *(answer options see PS05)*
PS07	Who is able to see your current location? Only you (6) User-defined (selected people and groups) (4) Your Friends on Facebook (4) Friends of Friends (2) Anyone on or off Facebook (0) Data not provided on Facebook (6)
PS08	Who is able to see your birthplace? *(answer options see PS07)*
PS09	Who is able to see your date of birth? *(answer options see PS07)*
PS10	Who is able to see your relationship status? *(answer options see PS07)*
PS11	Who is able to see your family relations? *(answer options see PS07)*
PS12	Who is able to see your employer? *(answer options see PS07)*
PS13	Who is able to see your educational institution? *(answer options see PS07)*
OS01	Do you use the blocking feature? Yes No
OS02	Have you ever deleted a post on your time wall to prevent other people from reading it? Yes No
OS03	Have you ever provided incomplete or fictitious information on Facebook on purpose to prevent other people from collection information about you? Yes No
OS04	Have you ever deleted a tag on a photo or video of you? Yes No

Evaluation Methodology. For statistical analysis, a score between zero and six points was assigned to every answer option of the privacy setting items (see table 63). Depending on their answers, a privacy setting score was calculated for every participant by summing up the individual answer scores. The calculated privacy setting scores range from 15 to 78 points, with 78 being the maximum reachable. Table 64 summarizes the distribution of the scores across participants.

To calculate a score for the deployment of other privacy protection strategies besides the management of privacy settings, another score was calculated by summing up the positive answers for each protection strategy. The calculated protection strategy scores range from 0 to 4 points (M=2.16, SD=1.13), with 4 being the highest possible value.

Ethical Considerations. Ethical requirements with respect to participants' informed consent and data privacy were in line with the ethical guidelines provided by the Technische Universität Darmstadt. Participants were assured that their data would not be linked to their identity and that the responses would only be used for study purposes. Furthermore, the surveys were implemented in SoSciSurvey [131], which stores all data in Germany and is thus subject to strict EU data protection law. Contact data, namely an email address, was stored in a separate data file, used for a lottery and subsequently deleted.

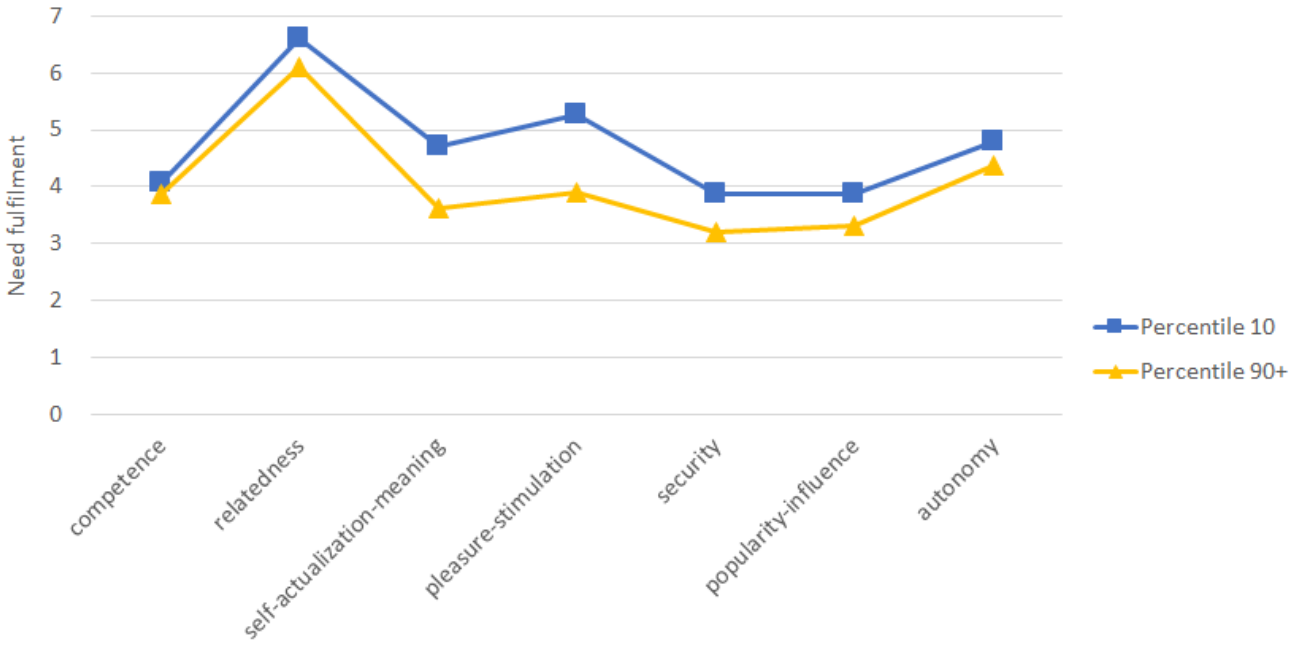

Figure 27: Need Profiles for percentile 10 and percentile 90+ of the privacy setting scores.

6.4.3 Results

Linear regression analysis was used to test RQ4d, i.e., whether Facebook users with strict and those with lax privacy settings differ pertaining to the needs/be-goals that motivate them to use Facebook. All seven needs were entered as predictors, whereas the privacy setting score was used as dependent variable. The resulting regression model exhibited an adjusted R^2 of .049, thereby explaining a total of 5% in the variance of privacy setting management ($F=3.039$, $p<.05$). However, only meaningfulness was found to be of significant predictive power ($\beta=-.274$, $t=-3.36$, $p<.001$), with higher values of self-actualization-meaning indicating the usage of lax privacy settings.

To further investigate the relationship between privacy settings and needs/be-goals, I compared the need values for the participants with very lax privacy settings ($\leq$ 10%, i.e. percentile 10) to the values for those with very strict privacy settings ($\geq$ 90%, i.e. percentile 90+). Therefore, a multivariate analysis of variance (MANOVA) was conducted, with the seven needs serving as dependent variables and the percentile membership as independent variable.

As can be seen in table 65 the participants with very strict privacy settings showed significantly different values for meaningfulness and pleasure-stimulation compared to those with very lax privacy settings. Fig. 27 illustrates the need profiles of both groups.

Analog to RQ4d, a linear regression analysis was conducted to test RQ4e, i.e., whether Facebook users who deploy certain privacy protection strategies besides the management of privacy settings and those who do not differ pertaining to the needs that motivate them to use Facebook. Again, all seven needs were entered as predictors, whereas the protection strategy score was used as dependent variable. The resulting regression model held no significant prediction power ($F=0.247$, $p=.973$).

6.4.4 Discussion

The goal of this study was to investigate whether the be-goals users pursue relate to the management of privacy settings as well as the deployment of other protection strategies in Facebook. The results showed that Facebook users with rather lax privacy settings have a greater feeling of being meaningful and stimulated when using Facebook than users with rather strict privacy settings. However, no association could be found between needs/be-goals and the deployment of other protection strategies.

Table 64: Distribution of privacy setting scores

N	280	Percentiles								
Mean	58.66	P10	P20	P30	P40	P50	P60	P70	P80	P90
SD	11.39									
Minimum	15	41	51	55	57	61	63	67	68	71
Maximum	78									

Table 65: Results of the MANOVA testing the differences of need values for users with very strict and very lax privacy settings. Note: *p < .05; **p < .01; ***p < .001

	df	F-value	Sig.	partial η^2
Autonomy	1, 65	0.62	.44	.009
Competence	1, 65	0.09	.77	.001
Relatedness	1, 65	0.60	.44	.009
Self-actualization-Meaningfulness	1, 65	6.48	.01*	.091
Pleasure-stimulation	1, 65	10.61	.002**	.140
Security	1, 65	2.02	.16	.030
Popularity-influence	1, 65	1.99	.16	.03

None of the three fundamental needs associated with the use of a specific medium (i.e. autonomy, competence and relatedness) [60] showed a significant relationship with privacy protection behavior on Facebook. Considering the fact that the wish to be related to significant others poses one of the central usage motivations for social networks (e.g., [104, 189, 201]), its lacking association with privacy protection behavior is noteworthy. Indeed, the results indicate that Facebook users have the possibility of being socially integrated and feeling related to significant others without giving up their privacy on Facebook. The desire to feel meaningful and be stimulated, on the other hand, goes along with the use of rather lax privacy settings. This could be due to the fact that users seek for stimulation by sharing a huge amount of content with as many other Facebook users as possible, thereby increasing the chance that someone likes, comments or further shares this content. The association between having lax privacy settings and fulfilling the need to feel meaningful, i.e. being the "real self" and moving further to an ideal version of this self, is somewhat more difficult to interpret. It may be that a Facebook user perceives oneself as his or her "real self" to a greater extent if this self is shared with as many other users as possible. At the same time, this form of self-disclosure prevents other people from getting a false picture of the particular user due to a lack of information. Looking at the need profiles in its entirety, another possible explanation could be that users with a more moderate need profile tend to have stricter privacy settings because as specific needs gain significant importance during the usage of Facebook, other considerations like privacy take a back seat and hence, users pay less attention to their privacy settings.

The results hold several implications for privacy researchers as well as designers of privacy friendly applications. First of all, when speaking about privacy, it is important to consider the context in which personal data is provided by a user. Designers of privacy friendly applications or interventions that aim to increase a user's privacy self-protection should bear in mind that users have various motivations to share their data, for example to feel related to significant others, but also to feel meaningful or to be stimulated. If an alternative privacy-friendly application cannot provide the intended gratification, users will continue to use the established, privacy-threatening applications. Equally, privacy researchers have to consider the needs that the investigated user aims to fulfill, as they seem to explain some of the variance in privacy settings management.

Limitations. Like any survey trying to assess actual behavior, this study has various limitations that should be kept in mind when drawing conclusions based on the results. Since I did not verify the self-reported privacy behavior, it is quite possible that participants did euphemize their privacy efforts or simply did not recall their true privacy settings. However, I tried to avoid the last point by instructing the participants to check on their actual privacy settings if they were not sure about them, and added click-paths that point to where the particular content could be found. Nonetheless, I do not know how often participants use the particular protection strategies like blocking another user, and under which circumstances they do so. Further research is needed to gain a deeper understanding of the situational and motivational factors that influence the deployment of certain protection strategies.
Furthermore, I limited this study to the context of Facebook usage. Although Facebook is the most popular social network nowadays, I do not know if the results can be generalized to other privacy related contexts like the installation of smartphone apps or the encryption of email communications. Since most participants stem from university populations, the sample is most likely skewed (i.e. younger, higher educated and eventually over-averagely tech-savvy), compared to the general population. Further studies should be based on more heterogeneous samples to allow for generalization.

6.5 Conclusion

Especially relatedness, pleasure-stimulation, autonomy, and competence seem to be important for the use of messengers, social networks, cloud services, digital assistants, and Smart TVs. Although several participants expressed privacy concerns such as fear of data abuse or eavesdropping on data in the interview study, the fulfillment of do- and -be-goals seem to trump these concerns in many cases. Regarding digital assistants and Smart TVs, however, many participants reported to be concerned about privacy infringement in the interview study, e.g., since they feared to be eavesdropped on. This might be due to the fact that both applications include a microphone and some Smart TVs also include a camera, which could always be recording. Developers thus should at least increase transparency regarding when and why the digital application is recording. Besides this, the possibility of advanced privacy management is needed, e.g., the option to deactivate recording when it is not intended.
In the survey study described in section 6.4, I investigated 280 German Facebook users and found that the be-goals of users significantly predict the management of privacy settings. The use of lax settings is associated with a greater feeling of being meaningful and stimulated when using Facebook. Product designers and privacy researchers therefore should consider the context in which users provide personal data, i.e. what motivates them to share their data in the first place. Only if privacy studies and interventions account for these important factors, it is possible to not only gain a complete picture of but also to influence the privacy behavior of users. The be-goals identified in the studies described in section 6.2 and section 6.3 should thus be considered in the development of a privacy-enhancing solution such as described in chapter 5, e.g., by suggesting users to rely on alternative solutions to feel related to others, such as communicating via encrypted messengers instead of social networks or unencrypted messengers.

7 Discussion

I chose a multidimensional approach in order to shed light on the complex phenomenon of people's privacy attitude and behavior, which often contradict, a phenomenon which is referred to as "privacy paradox". This dichotomy between people's privacy attitude (that is often characterized by severe concerns about the handling of their private data) and their often careless privacy behavior (that frequently contradicts these expressed concerns) has received considerable attention during the last decade, but has not been fully explained yet.

7.1 Goal 1: Identify explanation approaches for the privacy paradox

The first goal of this thesis was thus to identify explanation approaches for the privacy paradox that have been proposed in the literature in order to ground this thesis in prior work and extend the existing findings in a reasonable manner. As the privacy paradox is a complex phenomenon that has been looked at by researchers from different fields who apply different research approaches (i.e., top-down by considering general theories of human behavior or bottom-up from a data-driven point of view), I propose two research questions to meet this goal: RQ1a: Which theoretical explanations have been proposed for the privacy paradox? and, assuming that the privacy paradox evolves because privacy attitude and behavior are affected by different factors, RQ1b: Which factors influence users' privacy attitude and behavior?[17]

I conducted a literature review to answer these research questions and meet the first goal. Regarding RQ1a, I identify the seven most popular theoretical explanations approaches that have been proposed in the literature. To answer RQ1b, I collate the effect sizes for all factors related to privacy attitude, intention, and behavior identified in empirical studies, including these that lacked statistical power in the respective studies. A closer look at these effect sizes found across different studies provides strong evidence for the privacy calculus model and the influence of social factors on privacy behavior. Further research is needed to evaluate how prior experiences with privacy infringement influence privacy attitude, intention, and behavior. Also, more studies are needed to determine the actual influence of how users subjectively control the disclosure and processing of their data, and to closer evaluate the risk and trust model, quantum theory and the possible explanation of the privacy paradox as a methodological artefact. Moreover, the results indicate that demographic variables should not be subject to further research, as these were frequently found to only weakly predict privacy attitude, behavioral intention, and behavior.

However, although a multiplicity of studies that investigate user privacy in some way have been conducted, it is difficult to draw overall conclusions. This is due to the fact that the constructs considered in these studies frequently slightly differ (e.g., one study focuses on privacy concerns, the next on website privacy concerns, and another on context specific privacy concerns). It often remains unclear how these constructs relate to each other: Privacy intention, e.g., could describe exactly the same construct as privacy willingness, but it may also be that these two constructs differ in some way. Thus, to facilitate a fruitful exchange among researchers, the research community should agree on a shared definition of privacy attitude, intention, and behavior and the underlying sub-constructs such as privacy concerns or perceived privacy risk, and further specify the relationship between these variables.

In conclusion, no "clear winner" can be identified that influences privacy attitude, intention, or behavior. Thus, further research is needed to explain the complex phenomenon of user privacy. Drawing on the privacy calculus model, I decide to further investigate which factors affect the users' decision to protect or share their data with the aim to increase user privacy protection. Based on the literature review results, I identify three factors that are among the most important factors for a user's decision to protect their privacy or share their data, respectively, and that are not system-specific and thus can be influenced on the user's side: (1) awareness of privacy issues, (2) knowledge of and ability to use protection solutions, and (3) protection obstacles, such as benefits associated with data disclosure.

[17] As many studies do not consider actual behavior but behavioral intention, I also considered this variable.

7.1.1 Contribution

The literature review serves as a basis for researchers to identify which factors should be investigated in more depth, either because they are significantly related to the three privacy variables, or because prior studies failed to analyze these factors with sufficient statistical power. Hence, the first contribution of this thesis is to provide a framework for privacy researchers to guide the direction of their research. Further, the literature review significantly contributes to showing the "big picture" of user privacy by bringing together findings from a broad set of studies as well as theoretical considerations. Researchers, but also privacy activists or product designers can build on the results in their decision to include or focus on specific aspects when designing an intervention or a technology or service which aims to motivate privacy-friendly behavior.

7.2 Goal 2: Understand factors that are important for users' decision to protect their digital privacy

As I aim to support users in protecting their privacy, the second goal of this thesis is to gain a deeper understanding of the factors that are important for a user's decision to protect their privacy. Based on the literature review conducted in the first part of the thesis, I identified three factors that are important for a user's decision to protect their privacy or share their data, respectively, and that are not specific for the technology or service used (such as trust towards the website or retention period), but can be influenced on the users' side: (1) awareness of privacy issues, (2) knowledge of and ability to use protection solutions, and (3) protection obstacles, such as benefits associated with data disclosure.
However, these factors were identified based on quantitative studies, applying either regression models or SEM. Thus, based on the literature review, I can only infer that these factors are related to the decision for or against privacy protection, but lack understanding on how to influence these factors in order to support people in protecting their privacy. To address this issue, I propose three research questions. First, I aim to investigate to what extend lay users are aware of privacy issues: RQ2a: What are people's mental models of possible consequences arising from sharing and not protecting their private data?
Second, I focus on the extend to which users are able and possess knowledge about how to implement protection solutions: RQ3a: What strategies do people apply to protect their data?
The third factor deals with obstacles for privacy protection, e.g., benefits associated with sharing data by using data-collecting technologies and services: RQ4a: What are obstacles for privacy protection and for what reasons do people still use privacy-threatening devices and services?
To answer these research questions and understand the three factors that influence the decision for or against privacy protection more thoroughly, I conducted qualitative in-depth interviews with 24 German lay users. The results indicate that lay users lack awareness of privacy risks beside personalized advertisement and financial loss (RQ2a). Thus, it seems necessary to inform lay users about possible consequences of data sharing, as current frameworks designed to guarantee a responsible treatment of user privacy, such as the GDPR, rely on users proving informed consent for the collection and processing of their data. The third part of this thesis thus focuses on how lay users can be informed about these possible privacy consequences. Although participants reported to apply several protection strategies, all of the described strategies fall into the category of "behavioral" protection strategies as described by Oomen and Leenes [170], e.g., not sharing sensitive data (RQ3a). No participants reported to apply Privacy Enhancing Technologies (PETs), indicating a lack of knowledge about these technical protection solutions. Some participants directly referred to a lack of knowledge about how to protect their privacy. Hence, it seems crucial to support lay users in increasing their knowledge about possible, in particular technology-based, protection solutions. The fourth part of this thesis pursues this approach.
Participants refrain from applying protection solutions or using privacy-friendly alternatives since these are too cumbersome to use, too complicated to understand, or due to the contradictory behavior of other people. On the other hand, they disclose data by using privacy-threatening technologies to reach other people, participate in their life, or share their opinion with others, as well as out of convenience (RQ4a).

Contrary to earlier research ([205, 183, 231]), these results indicate that the main obstacles for privacy protection are related to usability and social factors. As there are ongoing efforts in the community to increase the usability of PETs and privacy-friendly alternatives, I focus on why users continue to use privacy-threatening technologies and services despite their usability in the fifth part of this thesis.

7.2.1 Contribution

The interview results provide a more thorough understanding of the factors that significantly influence a user's decision to protect their privacy or provide their data. They indicate that in order to allow lay users to make an informed decision about their privacy, as it is assumed by legal frameworks such as the GDPR, measures have to be taken to increase their awareness of privacy issues, i.e., inform them about possible consequences that can result from data sharing. Apart from the focus groups conducted by Karwatzki et al. [108], to my best knowledge, there is a lack of studies dealing with which privacy consequences lay users are aware of without prompting them by showing them pre-defined lists and simply assessing their perception of these consequences. Furthermore, these studies usually remain rather abstract and only refer to issues such as identity theft, without describing the actual influence on the user. The consequences provided by individual participants in the interview study can thus serve as a starting point for researchers or activists who aim to run awareness campaigns or conduct awareness raising interventions.
Further, the results contribute to the discussion on possible theoretical explanation approaches for the privacy paradox by showing that lay users do not suffer from an "illusion of control", a theory which states that users share data because they assume that they remain in control about what information are shared with whom. Moreover, the results show that lay users successfully apply certain behavioral strategies for privacy protection, but need to be supported in the field of technical protection solutions. It has been proposed that younger users are more capable of using technical protection solutions [148]. However, as my sample is rather young and no participant reported to use any technical protection solutions, with some of them being aware of this issue and deliberately uttering the wish to be better informed about these solutions, it seems that it is not sufficient to hope that problems with technical protection solutions will vanish once most lay users are digital natives. Instead, privacy researchers, privacy activists, or the government have to take out measures to increase lay users' understanding of technical protection solutions, first by informing them about the existence of these solutions and then supporting them in using the solutions.
The results regarding RQ4a highlight the importance of increasing the usability of PETs and privacy-friendly alternatives. They further indicate that designers of such technologies should consider how social factors contribute to the use or abandonment of their products, as, e.g., the decision of a user to refrain from sharing pictures in social networks remains futile if other people are constantly sharing pictures of her or him. Thus, users aiming for privacy protection should be encouraged to talk with their contacts about this topic, and technical solutions could, e.g., include a functionality which allows users to send a request to respect their privacy to their contacts or automatically detect when information about them is shared by other people.

7.3 Goal 3: Investigate how users' awareness of privacy issues can be increased

To address users' lack of awareness of privacy risks, they should be informed about possible consequences that could arise from using potentially privacy-threatening services and technologies. The third part of this thesis focuses on how this can be done. An obvious approach might be to confront users with possible consequences of data sharing, such as identified in the interview study. However, people have been found to base their decisions on perceived risk instead of actual risk [227, 195]. The first step must thus be to understand how users perceive different kinds of privacy risks. Prior research has shown that unfamiliarity with a technology can lead to lower risk perceptions [74], whereas other studies indicate that unknown technologies are considered to be more risky [63, 77].
The study described in Gerber et al. [83] thus considers how lay users evaluate different kinds of privacy risk scenarios that are associated with the use of established and new technologies (Online Social Net-

works (OSN), smart home and smart health devices), thereby relying on the established definition of risk perception as the perceived probability of adverse consequences and the perceived severity of those [227, 150]. The results suggest that abstract privacy risk scenarios (e.g., describing the collection and analysis of data or referring rather vaguely to possible harm) are considered to be more likely, but less severe than specific privacy risk scenarios, which describe concrete consequences that can result from data sharing. Risk communication aiming for a reasonably high risk perception should thus not focus on vague or single specific privacy risks, but could, for example, provide a list of concrete privacy consequences to increase the recipients' evaluation of how likely one of these consequences might actually arise for themselves. Hence, RQ2b is: What are possible privacy consequences that could result from living in smart environments?
I conducted a literature review to identify such a set of concrete privacy consequences that can be used for risk communication.

7.3.1 Contribution

The third part of the thesis mainly contributes to the field of privacy risk communication. The results described in Gerber et al. [83] indicate that approaches for risk communication should not focus on single consequences of data sharing, e.g., as it is currently implemented on cigarette boxes. As single consequences are considered to be rather unlikely, risk communication should refer to real-world examples of those privacy consequences as well as combine a set of possible consequences to increase the perceived probability of one of these consequences actually applying to the recipient. I provide a basis for researchers, activists, or governmental actors who aim to develop such risk communication approaches, e.g., in the form of public awareness campaigns, by exemplary identifying possible consequences of living in smart environments. This is a highly relevant area for such approaches of risk communication, as the market for smart environments is increasing, and people are less familiar with the concept of such complex environments than, e.g., with social networks, which have often been a topic in the media in terms of privacy issues. To the best of my knowledge, this thesis provides the first list of such consequences that have been collected in a systematic approach and comprises a broad set of examples.

7.4 Goal 4: Increase users' privacy protection knowledge and ability

Lacking knowledge about and understanding of how to apply protection solutions can be addressed by supporting users in their handling of these solutions. I propose to implement this support in a smartphone app, as most people carry their smartphone around all day and an app does not necessarily rely on an Internet connection, and thus, the app should be accessibly almost anytime, which would presumably not be the case for, e.g., a computer program or a website. Further, users should be more motivated to deal with privacy-related topics if they decide to use an app that pursues this particular goal, compared to interventions which focus on situations in which privacy is only a secondary goal, like, e.g., by presenting users additional information when they are trying to install a new app in the app store.
I describe the development and evaluation of a first concept for this app in a field study with 31 participants to answer the following research questions:
RQ3b: Does using the app lead to an increase in knowledge about privacy related topics?
RQ3c: Does using the app lead to a change in privacy awareness?
RQ3d: Does using the app lead to a change in privacy behavior, that is, do participants...
...improve the privacy conditions on their smartphone?
...increase their use of security measures?
...deploy stricter privacy settings on social network sites?
...actively inform themselves about privacy?
...prompt others to protect their data?
Participants of the field study show increased values of knowledge about various privacy related topics, including the application of PETs (RQ3b), even after a retention period of one week. Privacy awareness was slightly increased after using the app, but the effect wore off after the one week retention period (RQ3c). Privacy behavior was enhanced only in some aspects (RQ3d): Participants were found to have improved

the privacy conditions on their smartphone, actively informed themselves about privacy, and prompted others to protect their data. Still, they did not deploy stricter privacy settings on social network sites or increase their use of security measures.
The results provide support for the idea to develop a dedicated application for assisting users in protecting their privacy. Since the information texts and gamification elements included in the app, as well as an analysis of the permissions requested by the apps installed on the user's smartphone succeed in enhancing participants' mobile privacy (which was explicitly facilitated by the app), but fail to improve their privacy protection in other domains, I suggest to include further motivational elements and outline the application of these elements based on the Persuasive Systems Design Model [169]. Since privacy awareness could only be increased short-term, I conclude that the final app should not only provide knowledge and support regarding the use of privacy protection solutions, but should also increase users' awareness of privacy risks by informing them about the possible privacy consequences identified in chapter 4.

7.4.1 Contribution

The forth part of the thesis provides insights on how a privacy enhancing solution can successfully be implemented. Especially in the field of mobile privacy and app permissions, prior research has focused on how visualizations of data flows or information about app permissions can be implemented in existing technologies such as the app store or the smartphone permission manager, and thus shown at the time users make a decision about installing a particular app. Although these solutions provide additional information, they do not take into account that users often pursue the main goal of installing or using an app at this point in time and thus privacy protection remains a secondary goal [124]. The evaluation results for the FoxIT app indicate that it is a promising approach to embed specific information, e.g., about app permissions, in a broader context by providing additional information about privacy topics, and combining these information with a gamification concept in a dedicated application that users can consciously choose to deal with whenever they feel is an appropriate time. Furthermore, while persuasive technologies have been successfully applied in several domains like healthy or environmental-friendly behavior, it is still largely unknown in the usable security and privacy community. Privacy or security enhancing interventions often focus on usability, but fail to take user experience and long-term motivation into account. Since the protection of privacy is a long-term task, and, as described in the privacy calculus model, users often have to weigh costs against benefits, it seems viable to provide the same support to users aiming to protect their privacy as to people who, e.g., aim to eat healthier. I thus call for a greater consideration of user motivation and long-term support in the privacy field and outline the implementation of an app that realizes this goal on several levels.

7.5 Goal 5: Identify reasons for users to keep using privacy-threatening technologies and investigate implications for privacy protection

Albeit the interview study already deals with why users keep using privacy-threatening technologies and services, I take a closer look at this topic in the fifth part of this thesis, as the participants in the interview study frequently referred to social networks and messengers and the sample only consisted of 24 participants. In order to investigate a broader range of technologies and services, and gain a deeper understanding of users' motivations, I propose two research questions. According to Hassenzahl and Roto [95], users pursue do-goals and be-goals when using interactive products, with the first focusing on the pragmatic aspect (i.e., what the user wants to do/accomplish by using the product), and the latter on the hedonic aspect (i.e., what the user wants to be/feel like by using the product). Thus, I investigate users' do-goals associated with a diverse set of technologies and services: RQ4b: What do users want to accomplish by using potentially privacy-threatening devices and services, i.e., Online Social Networks (OSN), messengers, cloud services, digital assistants, game consoles, smart TVs, E-Commerce applications, as well as participating in customer loyalty programs and market research studies? as well as their be-goals: RQ4c: What do users want to feel like by using potentially privacy-threatening devices and services, i.e., Online Social Networks (OSN),

messengers, cloud services, digital assistants, game consoles, smart TVs, E-Commerce applications, as well as participating in customer loyalty programs and market research studies?
I conducted two survey studies with 217 and 246 participants, respectively, as well as an additional interview study, to confirm and extend the result of the first interview study described in chapter 3. I considered various (potentially privacy-threatening) services and applications in these studies and found that users pursue a multiplicity of do-goals (describing what people want to accomplish by using a product) when using the considered technologies (RQ4b), but mainly strive to feel related, competent, autonomous, and stimulated when using these technologies (RQ4c).
I conducted another survey study with 280 Facebook users to investigate whether and how the be-goals (describing how people want to feel by using a product) that users pursue when they use Facebook relate to the application of privacy protection strategies: RQ4d: Do Facebook users with strict and those with lax privacy settings differ pertaining to the needs/be-goals that motivate them to use Facebook (i.e., (a) autonomy, (b) competence, (c) relatedness, (d) meaningfulness, (e) pleasure-stimulation, (f) security and (g) popularity-influence)? and RQ4e: Do Facebook users who deploy certain privacy protection strategies besides the management of privacy settings and those who do not differ pertaining to the needs/be-goals that motivate them to use Facebook (i.e., (a) autonomy, (b) competence, (c) relatedness, (d) meaningfulness, (e) pleasure-stimulation, (f) security and (g) popularity-influence)? The results suggest a relationship between the management of privacy settings and particular be-goals, with Facebook users having rather lax privacy settings reporting a greater feeling of being meaningful and stimulated when using Facebook than users with rather strict privacy settings (RQ4d). No relationship was found between the deployment of other protection strategies and users be-goals (RQ4e).
The results from all four studies indicate that a solution for supporting privacy protection should – whenever possible – be tailored to the specific needs of the user. A privacy enhancing app as described above should thus consider the respective do- and be-goals people typically pursue when using a particular service or application when suggesting the user possible privacy-friendly alternatives, or a more privacy-friendly way to handle the respective service or application.

7.5.1 Contribution

The fifth part of this thesis contributes to the understanding of what costs users actually weigh against the benefits of privacy protection. While there have been several approaches to understand what motivates the use of social network sites (e.g., [199, 147, 186]), to the best of my knowledge, this is the first set of studies which comprehensively identifies users' do-goals and be-goals associated with the use of various services and technologies. The resulting list of these goals can serve as an orientation for product designers, as well as designers of privacy interventions, as users will most likely not refrain from using privacy-threatening devices and services if such an intervention does not consider how their goals can be met in other ways. Furthermore, researchers can built on the findings in their efforts to fully understand people's privacy behavior, e.g., by referring to the identified goals as costs of privacy protection when empirically investigating the privacy calculus model.

7.6 Limitations

Especially the described user studies suffer from several limitations. First, they either rely on participants recruited via a panel, or on an academic sample. These types of samples are most likely both biased in terms of age, academic background, and technical expertise, in the sense that participants might be younger, higher educated and overly tech-savvy.
Second, the study design applied influences the validity and thoroughness of the study results. (Quantitative) survey studies allow the investigation of a larger and more diverse sample, thereby enhancing the external validity of the obtained results. Qualitative Interview studies, on the other hand, provide the opportunity to reflect in more depth on the considerations and perceptions of the investigated participants, which, in turn, strengthens the conclusions drawn on participants' answers, and thus enhances the internal

validity. Both study concepts exhibit different strengths and weaknesses, however, I tried to apply a reasonable combination of large-scale quantitative and more in-depth qualitative studies in order to maximize the advantages of both approaches.

Third, although the literature review draws on studies conducted with participants from various countries with different cultural backgrounds, most of these studies focus on US-American users. My user studies, on the other hand, only include participants who lived in Germany at the time the study was conducted. Hence, the results might not generalize to people from different cultural backgrounds. I will discuss this issue in more detail in the following subsection.

7.7 Influence of Culture

The possible influence of cultural specifics on privacy perception and privacy behavior should be kept in mind for the interpretation of the described user studies and the design of privacy enhancing solutions. Most research on this topic relies on US-American users. A number of studies has shown that US-American and German users differ, at least to some extent, in their privacy concepts. However, the nature of this differences is still ambiguous due to conflicting results: For example, Whitman [240] argues that the definition of privacy depends on people's culture, with Europeans (more precisely: Germans and Frenchmen) relating privacy protecting to the protection of their dignity, and US-Americans to the freedom to manage their own life without interference from the government, especially in their home.

In line with this, a study conducted by Krasnova et al. [121] indeed shows that Germans consider the possibility of someone using their posts on social media to embarrass them to be considerably more severe than US-Americans. However, Germans also find it more severe if their posts are used against them by "somebody" or shared with third parties. US-Americans, on the other hand, think it is more likely that their information is by used by "someone" to harm or embarrass them, compared to the German participants.

Yet, researchers disagree if Europeans are more or less concerned about privacy risks in general than US-Americans due to the different legal situations. A popular line of argumentation is that Europeans are less concerned about their privacy since the use of their data is closely protected by law. A survey conducted in 2008, when the Safe Harbour Agreement [16] regulated the handling of European consumers' data by European and US-American companies, provided evidence for this view. When the GDPR became enforceable in May 2018, Europeans' data became subject to even stricter regulations and thus if this effect really holds true, Europeans should now be even less concerned about privacy risks.

Still, another point of view is that since the violation of strict European data protection laws is often accompanied by detailed media reports [185], Europeans are more aware of possible privacy issues than US-Americans. There is also empirical evidence for this assumption: For example, Krasnova et al. [121] and Karl et al. [107] found that German users are more worried about their privacy in Online Social Networks than US-American users. Trepte et al. [225] found that Facebook users from countries with high values of uncertainty avoidance (e.g., Germans), find it more important to avoid privacy risks, as these are often unspecific and hard to grasp (and, consequently, associated with uncertainty).

However, further research is needed to clarify the differences between European and US-American users, and, more precisely, to decide who is more aware of and worried about privacy issues. It is, however, likely that the actual differences are more nuanced, and users from different cultures rely on different concepts of privacy, as indicated, e.g., by Whitman [240].

Less studies focus on cross-cultural differences between European users. Cecere, Le Guel, and Soulié [43] investigated privacy concerns regarding social media in twenty-seven European countries and found that participants from North and East Europe seem to be less concerned about the possibility of their data being abused, compared to participants from South and Central Europe. The authors argue that these differences might be grounded in the communistic history of East European countries, which is still reflected in their institutional legacy, and thus inhabitants of these countries are more accustomed to governmental control. Lancelot Miltgen et al. [162] also identified differences between Eastern and Southern Europeans,

with East European participants feeling more forced to disclose private data, and South European users feeling that they could decide more autonomously about the disclosure of private data.

7.8 Conclusion and Future Work

This thesis starts out with investigating what explanations (theoretical and empirical) have already been proposed for the privacy paradox in the literature and how the combination of these explanations can provide further insights into the phenomenon. The empirical results provide strong evidence for the privacy calculus model and the influence of social factors on privacy behavior. Further research is needed to evaluate the influence of prior experiences with privacy infringement and perceived control about the disclosure and processing of the disclosed data as well as the risk and trust model, quantum theory and the possible explanation of the privacy paradox as a methodological artefact. I provide on overview of the empirical results, which can guide researchers to include or exclude variables in their studies on privacy behavior, attitude, or intention. Future work should focus on how variables that have repeatedly been found to have a strong influence on user privacy relate to each other by including all variables in a comprehensive model. A first approach for this can be found at P. Gerber [86]. Researchers are further encouraged to conduct studies on the variables which could not be confirmed or rejected as relevant for user privacy due to lacking statistical power in prior studies.

Since the results also show that motivation to protect one's privacy or privacy concerns do often not result in increased protection behavior, I aim to support users in protecting their privacy. For this purpose, I focus on three factors that have been shown to influence a user's decision to protect their privacy or share their data in earlier research: Their risk awareness, knowledge about and ability to use protection solutions, and obstacles for protection. I find that most lay users lack awareness of possible consequences that can result from data sharing, e.g., by using data-collecting devices and services, and that approaches to raise their awareness of possible risks should probably (1) refer to real-world examples of privacy consequences and (2) include a set of possible consequences to maximize perceived probability and severity. I identify such a list of consequences for the example of smart environments. Future research is needed to identify the ideal combination of these consequences and real-world examples for risk communication. Further, it should be investigated how this risk communication should take place to maximize its effects (e.g., in public campaigns run by the government, in specific interventions developed by privacy researchers, as part of the curriculum in school classes, etc.).

I further describe the development and evaluation of an example of such a privacy intervention, which aims to enhance privacy knowledge. While the concept of a dedicated knowledge-enhancing app, which also includes gamification elements, seems to be promising, further motivational elements should be included to extend the users' privacy protection to various domains and to ensure long-term success. I outline the implementation of such motivational elements based on the Persuasive Systems Design Model (PSD model) [169]. Although I focus on elements that have been identified as promising in other domains, the technical implementation of these elements should be followed by additional empirical evaluations. Furthermore, the topics for the app's information texts were selected with the idea of putting together an interesting and informative collection to test the app concept instead of already finding a comprehensive compilation of all topics. It is thus necessary to revise and extend the implemented information texts, which is a constant task that I have been pursuing since the evaluation study was conducted. As the app content is growing, further evaluation studies should be conducted, if possible, over a longer period of time and with a more heterogeneous sample. It would also be worthwhile to collect qualitative feedback, and investigate individual app features in a controlled experimental setting.

The final part of this thesis comprises a list of users' do- and be-goals related to the use of a broad set of privacy-threatening technologies and services. This lists serves as a starting point for designers of PETs or privacy-friendly alternatives. Further research is needed to investigate how the different goals can be addressed in the design of specific product features. I present a first study that investigates the relationship between usage motivation and the deployment of privacy protection strategies for the example of Facebook as the most popular social network. Privacy researchers are encouraged to investigate this relationship in

more depth for a broader range of application areas. Moreover, drawing on the privacy calculus model, future studies could focus on how users weigh the benefits of using privacy-threatening services and devices (i.e., the identified do- and be-goals) against their privacy concerns and intentions.
Overall, this thesis contributes to the understanding of the privacy paradox by summarizing and combining the research already conducted on this topic. It further provides an approach to support users in their efforts for privacy protection by increasing their awareness of privacy risks, their knowledge about privacy and particularly the use of privacy protection solutions, and by offering new insights into how protection obstacles can be addressed in privacy interventions and privacy-friendly alternatives.

Appendix A

Quality Assessment

Study	1	2	3	5	6	7	8	9	10	11	12	13	14	15	16	17
[253]	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N	NA	N	Y	Y
[167]	Y	Y	N	Y	Y	N	Y	N	N	N	Y	N	NA	N	N	N
[230]	Y	Y	Y	Y	Y	N	Y	N	Y*	N	Y	N	NA	N	Y	Y**
[127]	Y	Y	N	Y	Y	N	Y*	N	Y*	N	Y	N	Y	NA	Y	Y
[220]	Y	Y	Y	Y	Y	N	Y	Y*	Y*	N	Y	Y	NA	N	Y	Y
[57]	Y	N	N	Y	Y	N	Y	Y	N	Y	Y	N	N	N	Y	Y
[232]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	NA	N	Y	Y
[137]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N
[138]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N
[152]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	NA	Y	Y	Y
[134]	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y
[103]	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y*	N	Y	Y
[164]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
[142]	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
[69]	Y	Y	Y	Y	Y	N	Y*	N	N	N	Y	Y	Y*	N	Y	Y
[136]	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
[109]	Y	Y	N	Y	Y	N	Y	Y	Y*	Y	Y	N	NA	N	Y	Y
[250]	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	NA	N	Y	Y
[245]	Y	Y	Y	Y	Y	N	Y*	N	N	N	Y	Y	Y*	N	Y	Y
[118]	Y	Y	NA	Y	Y	NA	Y	Y	NA	Y	N	NA	NA	N	Y	Y
[21]	Y	Y	Y	Y	Y	N	Y	Y*	Y	N	Y	Y	NA	N	Y	Y
[26]	Y	Y	N	Y	Y	N	Y	Y	Y*	Y	Y	N	NA	N	Y	Y
[196]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
[248]	Y	Y	Y	Y	Y	N	N	Y	N	N	Y	Y	Y*	N	Y	Y
[233]	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	N	NA	N	Y	Y
[171]	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y	NA	N	Y	Y
[133]	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	NA	N	Y	Y
[258]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
[3]	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	NA	N	Y	N
[120]	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N	NA	N	Y	Y
[30]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	NA	N	Y	Y
[163]	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y
[31]	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	N	N	N	Y	Y
[32]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	NA	N	Y	Y
[258]	Y	Y	Y	Y	Y*	N	Y	N	Y	N	Y	N	NA	N	Y	N
[90]	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	NA	N	Y	Y
[204]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y
[114]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	Y	Y

Figure 28: Quality assessment of the considered studies. Note: *fulfilled in part, **study 1 and 3: Y, study 2: N.

Quality Criterions

Sources:
Original form: Malhotra, M. and Grover, V. (1998), "An assessment of survey research in POM: from constructs to theory," Journal of Operations Management, Vol. 16 No. 4, pp. 407–425 [155]
Clarification/comment: Sommestad, T., Hallberg, J. Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: A systematic review of quantitative studies", Information Management & Computer Security, Vol. 22, No. 1, pp. 42–75 [209]

General

1. Is the unit of analysis clearly defined for the study?
Original form: A formal statement defining the unit of analysis was needed for a positive assessment on this attribute. Justification of why that unit of analysis was selected.
Clarification/comment: In the reviewed studies the unit of analysis was an employee in almost all cases. In all studies the unit of analysis was clearly defined.
2. Does the instrumentation consistently reflect that unit of analysis?
Original form: The items in the questionnaire would need to be at the same level of aggregation as the unit of analysis. For example, to ensure consistency, questions pertaining to overall business strategy must have strategic business unit as the unit of analysis. In contrast, manufacturing strategy related study could have the plant as the unit of analysis.
Clarification/comment: When the construct concerned a subjective property of an employee, which they often did, it was assessed if the questions were formulated this way. For example, a negative assessment was made if a respondent was asked "Does the security mechanisms work well?" for a construct called "perceived response efficacy" (because the question is not phrased as something perceived). All questions would need to be positively assessed.
3. Is the respondent(s) chosen appropriate for the research question?
Original form: The person most knowledgeable at the selected unit of analysis must be the preferred respondent. It would be inappropriate for instance, to survey plant employees on organizational constructs for a multi-plant organization.
Clarification/comment: In most cases the questions concerned an individual employee which made the respondent suitable. However, a negative assessment was made if arbitrary employees were asked question of objective nature which are outside of their expected competence, e.g., if a security policy is optimal.

Measurement Error

5. Are multi-item variables used?
Original form: Multiple items or questions would have to be used as opposed to a single item question to define a construct of interest. A positive assessment was made if both multi-item and single item variables were used in the study.
Clarification/comment: None.
6. Is content validity assessed?
Original form: Content validity would need to be assessed through prior literature, or opinion of experts who are familiar with the given construct.
Clarification/comment: A negative assessment was made if the constructs was not discussed at all for the majority of the constructs.
7. Is field-based pretesting of measures performed?
Original form: A positive assessment was made only if the study formally stated the inclusion of this step in cleaning up the survey instrument and establishing its relevance.
Clarification/comment: Studies that included a pre-test of pilot involving respondents somewhat representative to the population (e.g., students) received a positive assessment.
8. Is reliability assessed?

Original form: Cronbach's Alpha analysis or test–retest analysis would be needed for a positive assessment.
Clarification/comment: A positive assessment was made regardless if the reliability was assessed before (.e.g., in a pilot) or after data collection was made.

9. Is construct validity assessed?

Original form: Construct validity (discriminant/convergent) analysis in the form of exploratory factor analysis, item-construct correlation, etc., would be needed for a positive assessment.
Clarification/comment: None.

10. Is pilot data used for purifying measures or are existing validated measures adapted?

Original form: A positive assessment was made if constructs and their associated items were evaluated on the basis of pretesting before the collection of actual data. Alternatively, constructs which were well defined and tested in prior studies could also be used.
Clarification/comment: The validity would need to be evaluated using a field-based pretesting (cf. item number 7). However, no formal/statistical evaluation was required.

11. Are confirmatory methods used?

Original form: Confirmatory factor analysis (e.g., using LISREL) results would need to be reported to establish construct validity.
Clarification/comment: This should be a test made of the measurement instruments validity prior to its use and the test should confirm its correctness.

Sampling Error

12. Is the sample frame defined and justified?

Original form: A discussion of sample frame was needed for a positive assessment.
Clarification/comment: The discussion would need to describe the sample frame to a level of detail that makes it possible to produce a similar sample. Since it is difficult to define the parameters that are needed to replicate the study (it depends on beliefs concerning extraneous variables) the criterion was applied leniently. At a minimum, however, it should be stated which country and type of organization that the sample frames includes and is not enough to explain who answered the questionnaire without detailing who was invited.

13. Is random sampling used from the sample frame?

Original form: Sampling procedures (random or stratified) would need to be discussed for a positive assessment.
Clarification/comment: A positive assessment was also made if all samples within the sample frame were invited.

14. Is the response rate over 20%?

Original form: A formal reporting of response rate over 20% was needed for a positive assessment.
Clarification/comment: In case interest to participate in the study and answer the questionnaire was assessed before the final invitation was sent the response rate for those reporting interest was used.

15. Is non-response bias estimated?

Original form: A formal reporting of non-response bias testing was needed for a positive assessment.
Clarification/comment: None.

Internal Validity Error

16. Are attempts made to establish internal validity of the findings?

Original form: At the very minimum, a discussion of results with the objective of establishing cause and effect in relationships, elimination of alternative explanations, etc., was needed for a positive assessment. Statistical analysis for establishing internal validity (like structural equation modeling) was considered as desirable, but not critical.
Clarification/comment: In case the study confirmed all of the hypotheses it tested the motivation of these hypotheses was considered sufficient.

Statistical Conclusion Error

17. Is there sufficient statistical power to reduced statistical conclusion error?
Original form: At least a sample size of 100 and an item to sample size ratio of more than 5 were needed for a positive assessment.
Clarification/comment: None.

Relationships Between the Main Predictor Variables

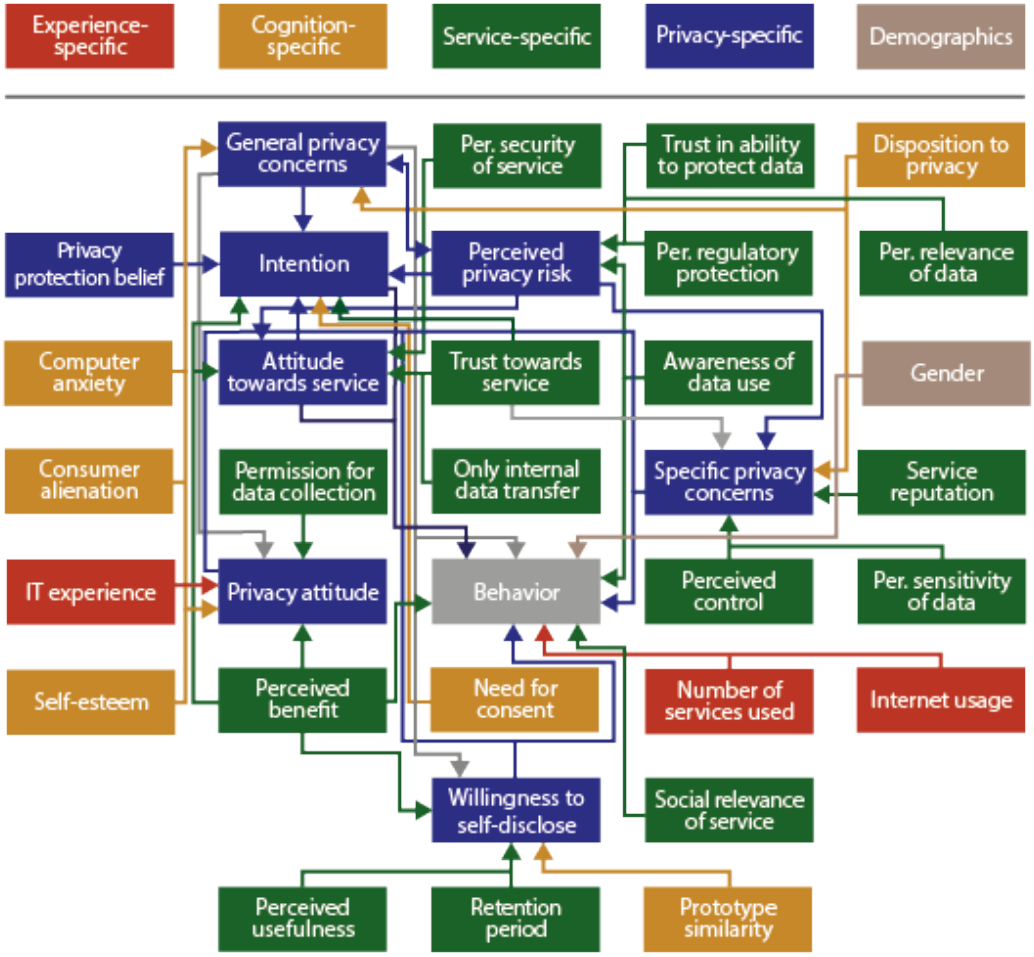

Figure 29: Relationships between the main predictor variables.

Appendix B

Interview Guidelines

Use of Digital Communication Channels

- Do you use technology to communicate with your peers?

Use of Privacy-Relevant Applications and Services

- Do you use...

  - Social networks
  - Apps: Messenger, games, navigation, shopping, etc.
  - Cloud services
  - Online shopping (products, services)
  - Online banking
  - Providers for online payment (e.g., PayPal)
  - Reward programs (Payback, "points collection-systems" & costumer cards)
  - New national identity card: digital functions (online authentication, fingerprints, etc.)
  - Digital assistants: GoogleNow, Cortana, Siri, etc.
  - SmartTV (If yes, is it connected to the Internet? What features do you use (apps, automatic recording, etc.)?
  - Consoles (If yes, is it connected to the Internet? What features do you use (gaming only, surfing, voice-chat, video sharing, shopping, etc.)?

- Do you participate in...
  - Research studies
  - Market research

Data Privacy Attitude and Behavior

- What is your opinion on data privacy? What does it mean for you?
- Social norm: What are your peers' opinions about it?
- Does data privacy play a role at your work place?
- Media perception:
  - How do you perceive the treatment of the topic data privacy in the media?
  - And regarding current events?
  - Do you think this topic is covered by the media appropriately?
  - Do you consider yourself informed sufficiently through the media?
  - How do your friends / family perceive the coverage of this topic in the media?
  - Do you think that the so-called "Snowden-Effect" influenced your / your friends' / family's opinion?
- Personalized services: What do you think about such services? (GoogleNow, product recommendation, Facebook suggested posts, etc.)
- Possible consequences: Which consequences could result from sharing your data?
- Have you experienced such consequences in the past?
- Do you take any precautions to protect your privacy / data? Which ones?
- Are there any specific data which you consider more important to protect than other? Are there any data that you would not protect at all?
- Are there enterprises / companies which you trust / distrust?

- What are your motives for protecting your data from...
  - Friends / Acquaintances / Family
  - Specific companies (Google, Facebook, etc.)
  - Specific organizations (NSA, state, police, etc.)
- Reflection behavior-intention regarding data privacy: Do you always act as you intend regarding data privacy or are there exceptions?

Appendix C

Email Communication With Participants of the Field Study

Invitation

Dear Participants,
during the last few months, we developed an app dealing with the topic of digital privacy and privacy protection and we would be happy to welcome you as a study participant today and hence one of the first users of FoxIT!
The app deals with your handling of digital privacy and privacy protection and our app is supposed to support you regarding these topics during the study.
You can't do anything wrong, you learn interesting things and further, you have the opportunity to win one out of five 40€ Amazon vouchers!
First, please fill in this questionnaire: [Link]
This will take about 15 minutes. You will receive an email providing details about the study procedure and instructions for installing our app within the next few days.
Thank you for your participation, we highly appreciate your support of our work.
During the whole study period, you can reach us here: foxit@psychologie.tu-darmstadt.de. We are glad to help you with problems, questions or suggestions!
Your FoxIT Team

Download of the App

Dear participant,
recently, you completed a survey about digital privacy and privacy protection (If you did not manage to complete the survey so far, you can still do this for a little while. In case you did not receive or lose the last email, do not hesitate to contact us :)). Now, the next step will be to install the FoxIT app and use it during a period of 14 days. Please start using the app as soon as you can.
The next steps are described in the following section. If you should encounter any difficulties or uncertainties, you can reach us via foxit@psychologie.tu-darmstadt.de.
Procedure
1. First, please download the app on your smartphone using the following link. This requires that your operating system is Android.
`https://play.google.com/store/apps/details?id=com.foxyourprivacy.f0x1t`
2. Now the study starts! Use the app during the next 14 days.
3. In two weeks, we will send you the first evaluation survey. After that, you don't have to use the app anymore.
4. One week later, you receive a final survey. If you complete it, you're not only doing us a great favor, but you also automatically participate in a lottery of five 40€ Amazon vouchers.
Your FoxIT Team

App Update

Dear participant,
the study started a week ago and we already received some feedback about bugs or crashes. Thus, we developed an update which should fix most of the problems. We ask (and encourage) you to update your app to the current version (0.942).
To do so, you can use the search function in the PlayStore (or: `https://play.google.com/store/apps/details?id=com.foxyourprivacy.f0x1t`) and click "update".
You can find information about your app version in the "settings" menu on the lower left side. If there is no information displayed at all, you have a rather old version. ;)
To receive the newest version of the lessons, you can also update manually via "settings" -> "debugging" by clicking on the first 2 buttons.
However, this is carried out automatically every two days.
If you should encounter any problems or crashs after updating the app, we would be thankful for your feedback!
Have fun with using the app!
Your FoxIT team

Second Survey and Upload Database

Dear participant,
two weeks ago, you completed the first survey and downloaded the app „FoxIT". We hope you were able to learn some things and enjoyed using FoxIT.
Now the FoxIT usage period is over and we ask you to complete the following steps:
Please chose "export database" in the app settings -> debugging.
Please complete the second survey. This should take about 15 minutes. Click on this link to be forwarded to the questionnaire: [Link]
Thank you for your participation, we highly appreciate your support of our work.
If you have any questions/comments, you can always contact us here: foxit@psychologie.tudarmstadt.de
Your FoxIT team
PS: If you like, of course you can still use FoxIT after the study is finished.

Reminder Upload Database

Dear participant,
if you did not already do it, please don't forget to provide us with your usage data. If you are connected to the internet right now, go to the app settings -> debug and then click on "export database".
The information does not relate to you personally, but only contains general and anonymized data about the app usage.
Thank you very much!
Your FoxIT team

Third Survey

Dear participant,
first, we want to thank you for hanging on and supporting us in our study on digital privacy and privacy protection!
Finally, we ask you to complete one last questionnaire. Please use this link: [Link]
This should take about 15 minutes.

We hope you were able to gain some insight into the subject of digital privacy and received some useful information about this topic.

After completing the last questionnaire, you automatically participate in a lottery of five 40€ Amazon vouchers. We contact the winners of the lottery directly.

Again, we thank you very much for your participation!

If you have any questions/comments concerning the study, you can always contact us here: foxit@psychologie.tudarmstadt.de. You can also contact us if you are interested in the study results.

Your FoxIT team

Winners of the Raffle

Dear participant,

congratulations! You won one of the 40€ Amazon vouchers.

You can activate the voucher by using the following code: [Code]

We thank you very much for your participation and hope you enjoy your voucher.

Sincerely

Your FoxIT team

Graphical Prototypes

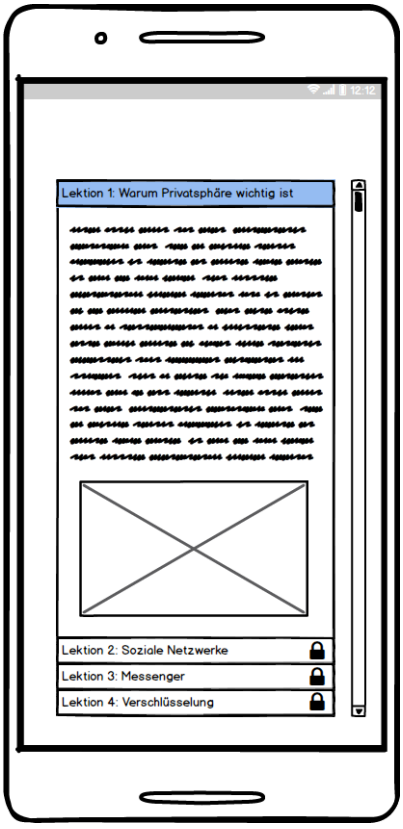

Figure 30: Tunneling.

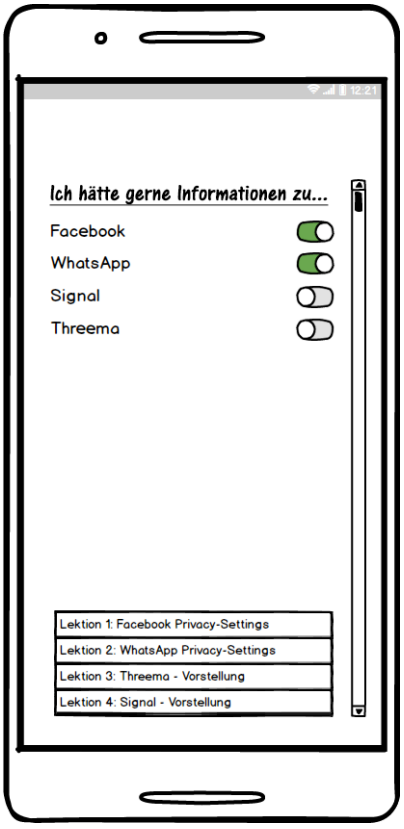

Figure 31: Tailoring.

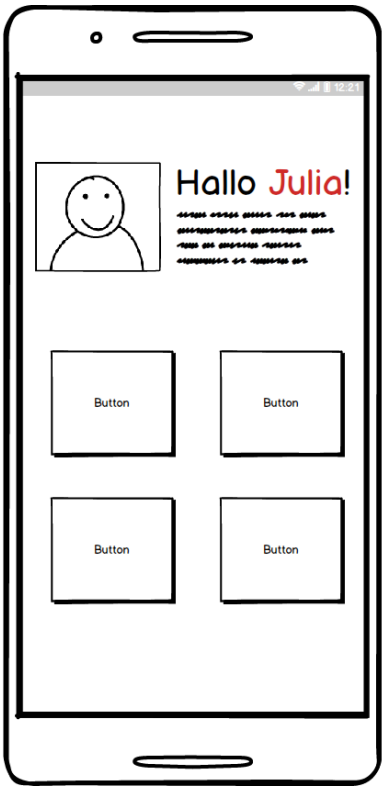

Figure 32: Personalization.

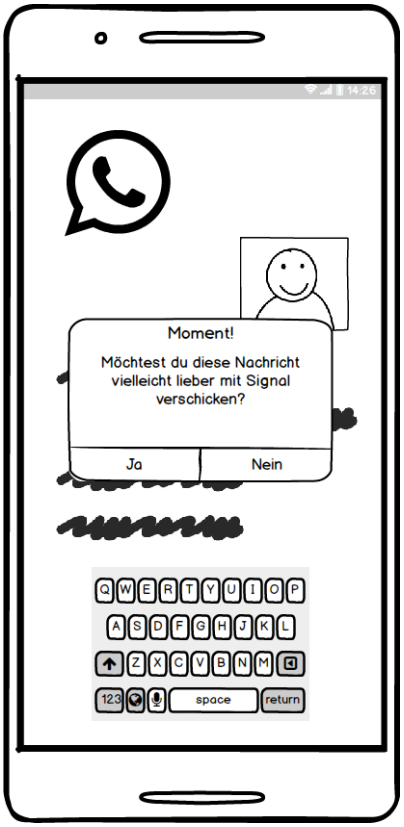

Figure 33: Reminders.

Figure 34: Praise.

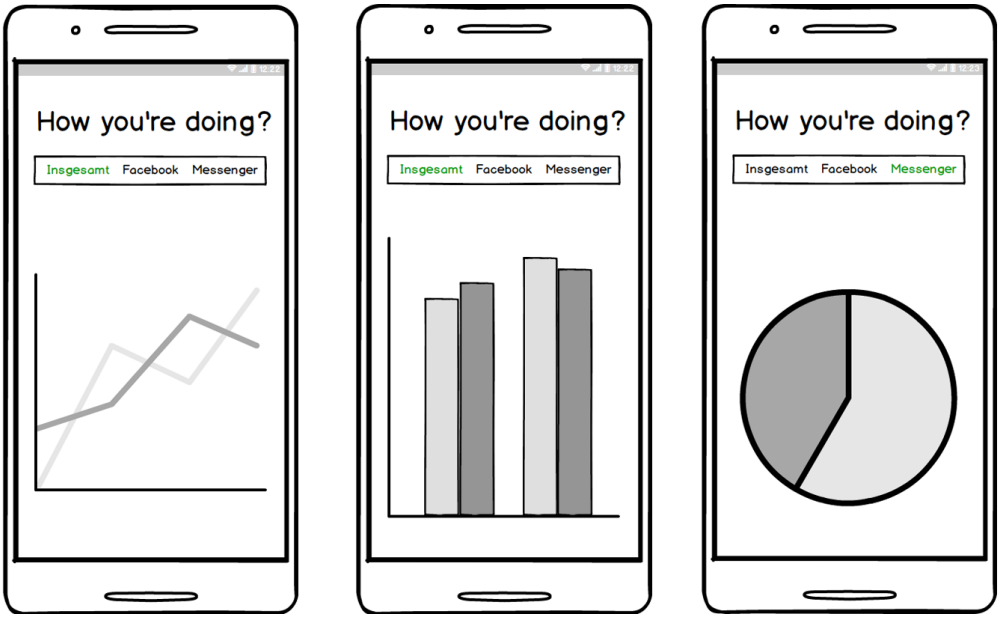

Figure 35: Self-monitoring.

Figure 36: Social role.

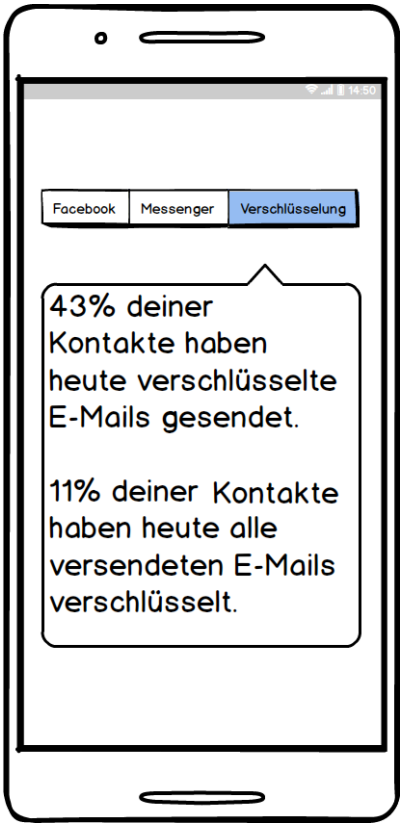

Figure 37: Social comparison.

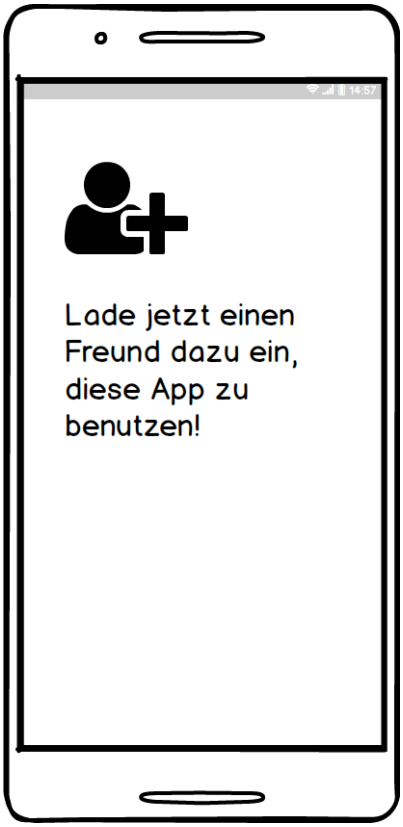

Figure 38: Normative influence.

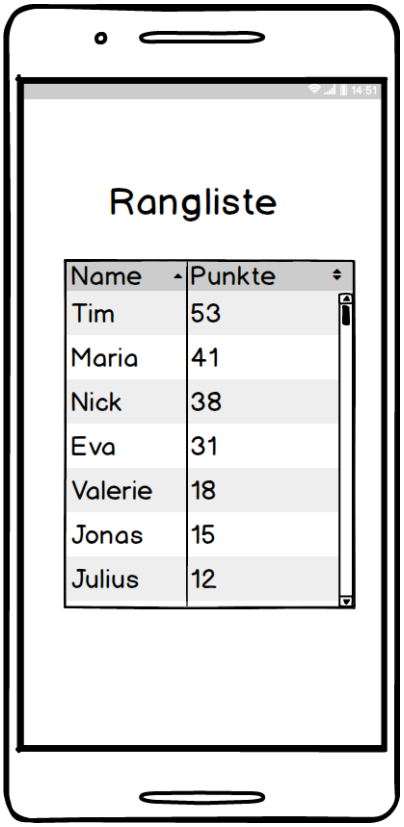

Figure 39: Competition.

Appendix D

Results of the Online Surveys Described in section 6.2

Table 66: Social Networks

Meta	Sub	N	%
Obtain information	About activities/experiences of the friends	43	23.8
	About news, world affairs	27	14.9
	About events	22	12.2
	On specific topics	18	9.9
	About activities of friends and family	16	8.8
	About study content / study organisation	15	8.3
	About celebrities	6	3.3
	About vacancies	5	2.8
	About personal news	5	2.8
	About offers and novelties of companies	4	2.2
	About strangers	4	2.2
	About association activities/events	2	1.1
	About local events	2	1.1
	About people	2	1.1
	About work/projects	1	0.6
	About apartments	1	0.6
	View pictures	1	0.6

Continued on next page

Table 66 – *Continued from previous page*

Meta	Sub	N	%
	Watch videos	1	0.6
	About activities/experiences of the family	1	0.6
	Others	5	2.8
Contact with others	Stay in touch	88	73.9
	- with friends	36	30.3
	- with people living far away	12	10.1
	- with acquaintances	10	8.4
	- with “old” friends you don’t meet so often anymore	6	5
	- with family members	6	5
	Get in touch	21	
	- with familiar people	8	6.7
	- with strangers	4	3.4
	Networking	9	7.6
	Send greetings	1	0.8
Be entertained	View pictures	2	40
	Watch videos	2	40
	About celebrities	1	20
Communicate	In writing	14	56
	With friends	10	40
	Save money	1	4
	Verbally	1	4
	About study content / study organisation	1	4
	Small talk	1	4
Inform others	About own experiences	19	52.4
	- while one is travelling	5	13.9
	About events	4	10.8
	On specific topics	3	8.1
	About association activities/events	1	2.7
	About meetings	1	2.7
	About study content / study organisation	1	2.7
	About vacancies	1	2.7
	Other	7	18.9
View content	View pictures	17	63
	Watch videos	7	25.9
	Funny contents	3	11.1
Exchange views/information	About study content / study organisation	11	57.9
	On specific topics	4	21.1
	Exchange information	3	15.8
	About personal news	1	5.3
Make arrangements	Plan activities	6	37.5
	Arrange appointments	5	31.3
	About work/projects	3	18.8
	About study content / study organisation	2	12.5
Manage data	Edit pictures	2	66.7
	Other	1	33.3
Exchange data	Exchange pictures	2	100

Continued on next page

Table 66 – *Continued from previous page*

Meta	Sub	N	%
Share data	Pictures	14	73.7
	Videos	2	10.5
	About work/projects	1	5.3
	Funny contents	1	5.3
	Other	1	5.3

Table 67: Messengers

Meta	Sub	N	%
Make arrangements	Arrange appointments	140	68
	- with friends	29	14.1
	- with family	3	1.5
	About work/projects	29	14.1
	Plan activities	19	9.2
	About study content / study organisation	8	3.9
	About everyday things	3	1.5
	About gifts	3	1.5
	In writing	1	0.5
	About events	1	0.5
	About association activities/events	1	0.5
	Other	1	0.5
Communicate	In writing	69	66.3
	Save money	9	8.7
	Verbally	9	8.7
	Small talk	5	4.8
	Scrambled	4	3.8
	About study content / study organisation	3	2.9
	Send greetings	3	2.9
	About everyday things	2	1.9
Contact with others	Stay in touch	87	80.6
	Contact somebody	13	12
	Send greetings	7	6.5
	Networking	1	0.9
Exchange views/information	Exchange information	25	55.6
	About study content / study organisation	7	15.6
	About personal news	7	15.6
	About work/projects	2	4.4
	On specific topics	2	4.4
	In writing	1	2.2
	About activities of friends/family	1	2.2
Share data	Pictures	26	66.7
	Funny contents	6	15.4
	Videos	2	5.1
	Voice messages	2	5.1
	Documents	2	5.1
	Music	1	2.6

Continued on next page

Table 67 – *Continued from previous page*

Meta	Sub	N	%
Obtain information	About activities of friends/family	5	33.3
	About study content / study organisation	4	26.7
	About association activities/events	2	13.3
	About celebrities	1	6.7
	About activities/experiences of the friends	1	6.7
	About activities/experiences of the family	1	6.7
	Other	1	6.7
Exchange data	Pictures	9	64.3
	Videos	3	21.4
	Funny contents	2	14.3
Inform others	About own experiences	4	57.1
	About everyday things	1	14.3
	Funny contents	1	14.3
	Other	1	14.3
Be entertained	Get images	2	50
	Share Pictures	2	50
View content	Pictures	2	66.7
	Funny contents	1	33.3
Receive data	Pictures	1	100
Manage data	Edit pictures	1	100

Table 68: Cloud services

Meta	Sub	N	%
Share data	Pictures	33	45.2
	Documents	19	26
	Large files/ large quantities	7	9.6
	Music	3	4.1
	Study materials	3	4.1
	About work/projects	2	2.7
	Videos	2	2.7
	Pictures	2	2.7
	To plan activities	1	1.4
	Books	1	1.4
Save files	Back Up	26	55.3
	Documents	8	17
	Study materials	5	10.6
	Pictures	4	8.5
	Books	2	4.3
	Music	1	2.1
	Large files/ large quantities	1	2.1
Exchange data	Study materials	23	43.4
	Pictures	16	30.2
	Documents	6	11.3
	About work/projects	4	7.5
	Networking	1	1.9
	Videos	1	1.9
	Music	1	1.9
	Large files/ large quantities	1	1.9
Manage data	Synchronize data	28	63.6
	Documents	5	11.4
	Study materials	5	11.4
	Get study materials	1	2.3
	Books	1	2.3
	Large files/ large quantities	1	2.3
	Pictures	1	2.3
	Other	2	4.5
Access data from anywhere	Documents	8	72.7
	Get study materials	2	18.2
	Study materials	1	9.1
Organize joint work	Plan activities	1	33.3
	About work/projects	2	66.7
Receive data	Study materials	7	36.8
	Pictures	5	26.3
	Documents	4	21.1
	Videos	2	10.5
	Other	1	5.3

Table 69: Digital assistants

Meta	Sub	N	
Operate particular applications	Set timer	4	30.8
	Weather forecast	2	15.4
	Write note	2	15.4
	Make phone call	2	15.4
	Navigate	1	7.7
	Other	2	15.4
Search for information	Navigation	3	100
Make entries without having to operate the device	In the car	2	66.7
	Other	1	33.3
Be entertained	Funny contents	2	100

Table 70: Game consoles

Meta	Sub	N	
Play games	Old games	13	44.8
	Party games	5	17.2
	SingStar	4	13.8
	Sports games	4	13.8
	With others	3	10.3
View content	Via DVD	4	23.5
	Via Netflix	4	23.5
	Via Blu-ray	3	17.6
	Films	3	17.6
	Via Amazon Prime Video	2	11.8
	Videos	1	5.9

Table 71: Smart TVs

Meta	Sub	N	%
View content	Series	12	31.6
	Movies	11	28.9
	Videos	10	26.3
	Missed content	3	7.9
	Save money	1	2.6
	Have a wide choice	1	2.6
Save files	Movies	1	50
	Series	1	50

Table 72: E-Commerce

Meta	Sub	N	%
Buy things	Special products	150	20.2
	Save money	139	18.7
	Shop conveniently	122	16.4
	Save time	64	8.6
	Have a wide choice	61	8.2
	Buy locally unavailable products	60	8.1
	Shop exceptionally, uniquely	36	4.8
	Shop beyond regular possibilities	26	3.5
	Used products	25	3.4
	Get fast delivery	13	1.7
	Carry out price comparisons	8	1.1
	Do several things with one account	7	0.9
	Get quickly available product	7	0.9
	Meet ecological / fair trade criteria	6	0.8
	Get lots of information, make well-founded decisions	5	0.7
	Pay by voucher	5	0.7
	Support providers	2	0.3
	About work/projects	1	0.1
	Synchronize data	1	0.1
Sell things	Used products	1	100
	Other	6	0.8

Table 73: Customer loyalty programs

Meta	Sub	N	%
Receive bonuses	Get vouchers	16	53.3
	Get products	8	26.7
	Get a discount	1	3.3
	Pay with points	1	3.3
	Other	4	13.3
Gain financial benefits	Get a discount	35	56.5
	Get money	9	14.5
	Save money	8	12.9
	Pay with points	5	8.1
	Get vouchers	5	8.1
Buy things	Special products	1	50
	Locally unavailable products	1	50
Obtain information	About offers and novelties of companies	2	100

Table 74: Market research studies

Meta	Sub	N	%
Get compensation	Participate in lotteries	35	77.8
	Get money	8	17.8
	Other	2	4.4
Help others	College students	10	66.7
	Researchers	4	26.7
	Other	1	6.7
Exert influence	Improve service	3	42.9
	Improve supply	3	42.9
	Other	1	14.3

Interview Guideline

Part I – Interview

Messengers: Do you use technology like messengers to communicate with others?
If yes:

- Which ones?
- Why / for which purpose?
- In which occasions?
- Which contents?
- With whom?
- Are there any differences regarding which messenger you use?
- Have you changed your use of messengers?
- When / for what reason did you stop using messengers?
- Did you uninstall messengers or stopped using a messenger?
- Which messenger and why?
- Which advantages do you see in the usage of messengers?
- Which disadvantages do you see in the usage of messengers?

If not:

- Why not?
- Why did you uninstall it?
- Which disadvantages do you see in the usage of messengers?
- Are there, nevertheless, any advantages in the usage of messengers?

Social networks: Do you use social networks?
If yes:

- Which ones?
- Why / for which purpose?
- In which occasions?
- With whom?
- Have you changed your use of messengers?
- Which advantages do you see in the usage of social networks?
- Which disadvantages do you see in the usage of social networks?

If not:

- Why did you stop using social networks?
- Why haven't you registered yourself?
- Which disadvantages do you see in the usage of social networks?
- Are there, nevertheless, any advantages in the usage of social networks?

Cloud services: Do you use cloud services?
If yes:

- Which ones?
- Why / for which purpose?
- In which occasions / in which not?
- Which advantages do you see in the usage of cloud services?
- Which disadvantages do you see in the usage of cloud services?

If not:

- Why not?
- Which disadvantages do you see in the usage of cloud services?
- Are there, nevertheless, any advantages in the usage of cloud services?

Digital assistants: Do you use digital assistants e.g. Siri, Google Now, Cortana, Alexa, ...?
If yes:

- Which one?
- Why / for which purpose?
- In which occasions?
- Which advantages do you see in the usage of digital assistants?
- Which disadvantages do you see in the usage of digital assistants?

If not:

- Why not?

- (Why did you disable your digital assistant?)
- Which disadvantages do you see in the usage of digital assistants?
- Are there, nevertheless, any advantages in the usage of digital assistants?

Smart TVs: Do you use a Smart TV? If yes:

- Why do you use a Smart TV?
- What are you doing with the Smart TV?
- Which advantages do you see in the usage of Smart TVs?
- In your opinion, which negative consequences can result from using Smart TVs?
- Which disadvantages do you see in the usage of Smart TVs?

If not:

- Why not?
- Which disadvantages do you see in the usage of Smart TVs?
- In your opinion, which negative consequences can result from using Smart TVs?
- Are there, nevertheless, any advantages in the usage of Smart TVs?

Part II – Ranking of the psychological needs [198]

The same questions were asked separately for each digital application:

- Why is it important to fulfill... (need)?
- What does (need) mean to you?
- What fulfills (need)?
- Which actions / events fulfill (need)?
- Can you give an example, where (need) is fulfilled?
- Is (need) already fulfilled or is it rather a wish than a need that is already fulfilled?

Literature

[1] IoT Analytics Research 2018. *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/. Accessed: 2019-07-08.

[2] Statista 2019. *Most famous social network sites worldwide as of April 2019, ranked by number of active users (in millions)*. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Accessed: 2019-06-22.

[3] Rana Abbas and Gustavo S. Mesch. *Cultural values and Facebook use among Palestinian youth in Israel*. In: *Computers in Human Behavior* 48 (2015), pp. 644–653. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2015.02.031.

[4] Ruba Abu-Salma et al. *Obstacles to the Adoption of Secure Communication Tools*. In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. 2017, pp. 137–153.

[5] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. *Privacy in e-commerce: examining user scenarios and privacy preferences*. In: *Proceedings of the 1st ACM conference on Electronic commerce*. ACM. 1999, pp. 1–8.

[6] Alessandro Acquisti. *Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior*. In: *Proceedings of the 2nd Annual Workshop on Economics and Information Security (WEIS)*. 2003.

[7] Alessandro Acquisti and Ralph Gross. *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. In: *Proceedings of the International Workshop on Privacy Enhancing Technologies*. Springer. 2006, pp. 36–58.

[8] Alessandro Acquisti and Jens Grossklags. *Privacy and rationality in individual decision making*. In: *IEEE Security Privacy* 3.1 (2005), pp. 26–33. ISSN: 1540-7993. DOI: 10.1109/MSP.2005.22.

[9] Alessandro Acquisti and Jens Grossklags. *What Can Behavioral Economics Teach Us About Privacy?* In: *Digital Privacy: Theory, Technology, and Practices*. Ed. by A. Acquisti et al. Boca Raton: Auerbach Publications, 2006, pp. 363–377.

[10] Paarijaat Aditya et al. *Brave New World: Privacy Risks for Mobile Users*. In: *Proceedings of the ACM MobiCom workshop on Security and privacy in mobile environments (SPME)*. 2014, pp. 7–12. ISBN: 9781450330756.

[11] Musheer Ahmed and Mustaque Ahamad. *Protecting Health Information on Mobile Devices*. In: *Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy (CODASPY)*. 2012, pp. 229–240. ISBN: 978-1-4503-1091-8. DOI: 10.1145/2133601.2133629.

[12] Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. *Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks*. In: *Proceedings of the Multimedia Privacy and Security Workshop (MPS) at the 24th ACM Conference on Computer & Communication Security (CCS)*. 2017, pp. 1–11. ISBN: 978-1-4503-5206-2. DOI: 10.1145/3137616.3137617.

[13] Ahlam Alami, Laila Benhlima, and Slimane Bah. *A Study of Security Requirements in Wireless Sensor Networks for Smart Home Healthcare Systems*. In: *Proceedings of the 3rd International Conference on Smart City Applications (SCA)*. 2018, 55:1–55:8. ISBN: 978-1-4503-6562-8. DOI: 10.1145/3286606.3286832.

[14] Bako Ali and Ali Ismail Awad. *Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes*. In: *Sensors* 18.3 (2018). DOI: https://doi.org/10.3390/s18030817.

[15] Hazim Almuhimedi et al. *Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging*. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 2015, pp. 787–796. ISBN: 9781450331456. DOI: 10.1145/2702123.2702210.

[16] Annie I. Antón, Julia B. Earp, and Jessica D. Young. *How Internet Users' Privacy Concerns Have Evolved Since 2002*. In: *IEEE Security & Privacy* 8.1 (2010), pp. 21–27. ISSN: 1540-7993. DOI: 10.1109/MSP.2010.38.

[17] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. *Privacy in the Age of Mobility and Smart Devices in Smart Homes*. In: *Proceedings of the ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust*. IEEE Computer Society, 2012, pp. 819–826. ISBN: 978-0-7695-4848-7. DOI: 10.1109/SocialCom-PASSAT.2012.108.

[18] B2B International with Kaspersky Lab. *Consumer Security Risks Survey. From Scared to Aware: Digital Lives in 2015*. https://apo.org.au/node/58440. Accessed: 2019-07-27. 2015.

[19] *Badgeville: Game mechanics*. http://badgeville.com/wiki/Game_Mechanics. Accessed: 2017-03-16.

[20] Young Min Baek. *Solving the privacy paradox: A counter-argument experimental approach*. In: *Computers in Human Behavior* 38 (2014), pp. 33–42. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2014.05.006.

[21] Young Min Baek, Eun-mee Kim, and Young Bae. *My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns*. In: *Computers in Human Behavior* 31 (2014), pp. 48–56. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2013.10.010.

[22] Rebecca Balebako and Lorrie Faith Cranor. *Improving App Privacy: Nudging App Developers to Protect User Privacy*. In: *IEEE Security & Privacy* 12.4 (2014), pp. 55–58. ISSN: 1540-7993. DOI: 10.1109/MSP.2014.70.

[23] Rebecca Balebako et al. *"Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones*. In: *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013, 12:1. ISBN: 978-1-4503-2319-2. DOI: 10.1145/2501604.2501616.

[24] Rebecca Balebako et al. *The Impact of Timing on the Salience of Smartphone App Privacy Notices*. In: *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)* (2015), pp. 63–74. DOI: 10.1145/2808117.2808119.

[25] Rebecca Balebako et al. *The privacy and security behaviors of smartphone app developers*. In: *Proceedings of the Workshop on Usable Security (USEC)*. Internet Society, 2014. ISBN: 1-891562-37-1. DOI: http://dx.doi.org/10.14722/usec.2014.23006.

[26] Gaurav Bansal, Fatemeh "Mariam" Zahedi, and David Gefen. *The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online*. In: *Decision Support Systems* 49.2 (2010), pp. 138–150. ISSN: 0167-9236. DOI: https://doi.org/10.1016/j.dss.2010.01.010.

[27] Mahmoud Barhamgi et al. *User-centric Privacy Engineering for the Internet of Things*. In: *IEEE Cloud Computing* 5.5 (2018). DOI: 10.1109/MCC.2018.053711666.

[28] David Barrera et al. *A Methodology for Empirical Analysis of Permission-based Security Models and Its Application to Android*. In: *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS)*. ACM, 2010, pp. 73–84. ISBN: 978-1-4503-0245-6. DOI: 10.1145/1866307.1866317.

[29] Daniel Bastos, Mark Shackleton, and Fadiali El-Moussa. *Internet of Things: A survey of technologies and security risks in smart home and city environments*. In: *Living in the Internet of Things: Cybersecurity of the IoT*. IET, 2018. DOI: 10.1049/cp.2018.0030.

[30] Laura Becker and Key Pousttchi. *Social networks: The role of users' privacy concerns*. In: *Proceedings of the 14th International Conference on Information Integration and Web-Based Applications & Services (IIWAS)*. 2012, pp. 187–195. DOI: 10.1145/2428736.2428767.

[31] Ardion Beldad, Menno De Jong, and Michaël Steehouder. *I Trust Not Therefore It Must Be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for e-Government Transactions*. In: *Computers in Human Behavior* 27.6 (2011), pp. 2233–2242. ISSN: 0747-5632. DOI: 10.1016/j.chb.2011.07.002.

[32] Ardion Beldad and Margareta Citra Kusumadewi. *Here's My Location, for your Information: The Impact of Trust, Benefits, and Social Influence on Location Sharing Application Use among Indonesian University Students*. In: *Computers in Human Behavior* 49 (2015), pp. 102–110. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2015.02.047.

[33] Xavier Bellekens et al. *Pervasive eHealth services a security and privacy risk awareness survey*. In: *International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. 2016. DOI: 10.1109/CyberSA.2016.7503293.

[34] Giles Birchley et al. *Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies*. In: *BMC Medical Ethics* 18 (2017). DOI: 10.1186/s12910-017-0183-z.

[35] danah m. boyd and Nicole B. Ellison. *Social Network Sites: Definition, History, and Scholarship*. In: *Journal of Computer-Mediated Communication* 13.1 (2007), pp. 210–230. ISSN: 1083-6101. DOI: 10.1111/j.1083-6101.2007.00393.x.

[36] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. *Misplaced Confidences: Privacy and the Control Paradox*. In: *Social Psychological and Personality Science* 4.3 (2013), pp. 340–347. DOI: 10.1177/1948550612455931.

[37] Laura Brandimarte et al. *Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis*. 2009. Poster, presented at iConference 2009.

[38] BreakAwayGames. *Virtual Dental Implant Trainer*. http://www.breakawaygames.com/{#}portfolio. Accessed: 2017-09-20.

[39] BreakAwayGames. *Vital Signs*. http://www.breakawaygames.com/vitalsigns/. Accessed: 2017-09-20.

[40] Chase Buckle. *Rethinking "Trust" in a New Era of Data Privacy*. https://blog.globalwebindex.com/chart-of-the-week/trust-data-privacy/. Accessed: 2019-07-08. 2018.

[41] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. *An analysis of malicious threat agents for the smart connected home*. In: *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2017, pp. 557–562. DOI: 10.1109/PERCOMW.2017.7917623.

[42] Die Bundesregierung. *Die Digitalstrategie der Bundesregierung*. https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/die-digitalstrategie-der-bundesregierung-1549554. Accessed: 2019-07-08. 2019.

[43] Grazia Cecere, Fabrice Le Guel, and Nicolas Soulié. *Perceived Internet privacy concerns on social networks in Europe*. In: *Technological Forecasting and Social Change* 96 (2015), pp. 277–287.

[44] Hichang Cho, Jae-Shin Lee, and Siyoung Chung. *Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience*. In: *Computers in Human Behavior* 26.5 (2010), pp. 987–995. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2010.02.012.

[45] Eun Kyoung Choe et al. *Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing*. In: *Human-Computer Interaction – INTERACT 2013*. Ed. by Paula Kotzé et al. Springer Berlin Heidelberg, 2013, pp. 74–91. ISBN: 978-3-642-40477-1.

[46] ChronicLogic. *Bridge Builder*. https://www.bridgebuilder-game.com/bbg-info.php. Accessed: 2017-09-20.

[47] Jason W. Clark et al. *"I Saw Images I Didn't Even Know I Had": Understanding User Perceptions of Cloud Storage Privacy*. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 2015, pp. 1641–1644. ISBN: 978-1-4503-3145-6. DOI: 10.1145/2702123.2702535.

[48] Joel E. Cohen. *Statistical Power Analysis for the Behavioral Sciences*. 2nd ed. New York, NY, US: Academic Press, 1987.

[49] Lizzie Coles-Kemp and Elahe Kani-Zabihi. *Practice Makes Perfect: Motivating Confident Privacy Protection Practices*. In: *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. 2011, pp. 866–871. DOI: 10.1109/PASSAT/SocialCom.2011.51.

[50] Drew Davidson, Matt Fredrikson, and Benjamin Livshits. *MoRePriv: Mobile OS Support for Application Personalization and Privacy*. In: *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*. ACM, 2014, pp. 236–245. ISBN: 978-1-4503-3005-3. DOI: 10.1145/2664243.2664266.

[51] Sourya Joyee De and Daniel Le Métayer. *Privacy Harm Analysis: A Case Study on Smart Grids*. In: *2016 IEEE Security and Privacy Workshops (SPW)*. 2016, pp. 58–65. DOI: 10.1109/SPW.2016.21.

[52] Bernhard Debatin et al. *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*. In: *Journal of Computer-Mediated Communication* 15.1 (2009), pp. 83–108. DOI: 10.1111/j.1083-6101.2009.01494.x.

[53] André Deuker. *Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services*. In: *Privacy and Identity Management for Life*. Ed. by Michele Bezzi et al. Springer, 2010, pp. 275–283. DOI: 10.1007/978-3-642-14282-6_23.

[54] Ratan Dey, Zubin Jelveh, and Keith Ross. *Facebook users have become much more private: A large-scale study*. In: *Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops*. 2012, pp. 346–352. DOI: 10.1109/PerComW.2012.6197508.

[55] Sarah Diefenbach, Eva Lenz, and Marc Hassenzahl. *Handbuch proTACT Toolbox. Tools zur User Experience Gestaltung und Evaluation*. http://germanupa.de/events/mensch-und-computer-2014/tutorials/experience-design-tools.html. Accessed: 2016-12-03.

[56] Tobias Dienlin and Miriam J. Metzger. *An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample*. In: *Journal of Computer-Mediated Communication* 21.5 (2016), pp. 368–383. ISSN: 1083-6101. DOI: 10.1111/jcc4.12163.

[57] Tobias Dienlin and Sabine Trepte. *Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors*. In: *European Journal of Social Psychology* 45.3 (2015), pp. 285–297. DOI: 10.1002/ejsp.2049.

[58] Digibyte. *ePrivacy: consultations show confidentiality of communications and the challenge of new technologies are key questions*. https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are. Accessed: 2019-07-08. 2016.

[59] Anthony Downs. *An Economic Theory of Democracy*. New York, NY, US: Harper & Brothers, 1958.

[60] Aine Dunne, Margaret-Anne Lawlor, and Jennifer Rowley. *Young People's Use of Online Social Networking Sites :a Uses and Gratifications Perspective*. In: *Journal of Research in Interactive Marketing* 4.1 (2010), pp. 46–58. DOI: https://doi.org/10.21427/D7WV31.

[61] William Enck et al. *TaintDroid: An Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones*. In: *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI)*. USENIX, 2010, pp. 393–407.

[62] Sai Mounika Errapotu et al. *SAFE: Secure Appliance Scheduling for Flexible and Efficient Energy Consumption for Smart Home IoT*. In: *IEEE Internet of Things Journal* 5.6 (2018), pp. 4380–4391. ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2866998.

[63] Fariborz Farahmand and Eugene H. Spafford. *Understanding insiders: An analysis of risk-taking behavior*. In: *Information Systems Frontiers* 15.1 (2013), pp. 5–15. ISSN: 1572-9419. DOI: 10.1007/s10796-010-9265-x.

[64] Franz Faul et al. *Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses*. In: *Behavior Research Methods* 41.4 (2009), pp. 1149–1160. ISSN: 1554-3528. DOI: 10.3758/BRM.41.4.1149.

[65] Adrienne Porter Felt, Serge Egelman, and David Wagner. *I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns*. In: *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. New York, NY, USA: ACM, 2012, pp. 33–44. ISBN: 978-1-4503-1666-8. DOI: 10.1145/2381934.2381943.

[66] Adrienne Porter Felt et al. *Android Permissions: User Attention, Comprehension, and Behavior*. In: *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS)*. New York, NY, USA: ACM, 2012, 3:1–3:14. ISBN: 978-1-4503-1532-6. DOI: 10.1145/2335356.2335360.

[67] Adrienne Porter Felt et al. *How to Ask for Permission*. In: *Presented as part of the 7th USENIX Workshop on Hot Topics in Security*. USENIX, 2012.

[68] Yang Feng and Wenjing Xie. *Explaining the Effect of Event Valence on Unrealistic Optimism*. In: *Psychology, Health & Medicine* 14.3 (2014), pp. 262–272. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2014.01.009.

[69] Yang Feng and Wenjing Xie. *Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors*. In: *Computers in Human Behavior* 33 (2014), pp. 153–162. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2014.01.009.

[70] Simone Fischer-Hübner and Hans Hedbom. *Benefits of privacy-enhancing identity management*. In: *Asia Pacific Business Review* 4.4 (2008), pp. 3–13.

[71] Drew Fisher, Leah Dorner, and David Wagner. *Short Paper: Location Privacy: User Behavior in the Field*. In: *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*. ACM, 2012, pp. 51–56. ISBN: 978-1-4503-1666-8. DOI: 10.1145/2381934.2381945.

[72] Christian Flender and Günter Müller. *Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited*. In: *Quantum Interaction*. Ed. by Jerome R. Busemeyer et al. Springer Berlin Heidelberg, 2012, pp. 148–159. ISBN: 978-3-642-35659-9.

[73] B. J. Fogg. *Persuasive Technology: Using Computers to Change What We Think and Do*. In: *Ubiquity* 2002 (2002). ISSN: 1530-2180. DOI: 10.1145/764008.763957.

[74] Batya Friedman et al. *Users' Conceptions of Risks and Harms on the Web: A Comparative Study*. In: *CHI '02 Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: ACM, 2002, pp. 614–615. ISBN: 1-58113-454-1. DOI: 10.1145/506443.506510.

[75] Huiqing Fu et al. *A field study of run-time location access disclosures on android smartphones*. In: *Proceedings of the Workshop on Usable Security (USEC)*. 2014. DOI: 10.14722/usec.2014.23044.

[76] Vaibhav Garg, Kevin Benton, and L. Jean Camp. *The Privacy Paradox: A Facebook Case Study*. In: *Proceedings of the 42nd Research Conference on Communication, Information and Internet Policy*. 2014.

[77] Vaibhav Garg and L. Jean Camp. *End User Perception of Online Risk under Uncertainty*. In: *Proceedings of the 45th Hawaii International Conference on System Sciences (HICCS)*. IEEE, 2012, pp. 3278–3287. DOI: 10.1109/HICSS.2012.245.

[78] James Paul Gee. *What video games have to teach us about learning and literacy.* In: *ACM Computers in Entertainment* 1.1 (2003).

[79] Abigail W. Geiger. *How Americans have viewed government surveillance and privacy since Snowden leaks.* https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/. Accessed: 2019-07-08. 2018.

[80] Nina Gerber, Paul Gerber, and Maria Hernando. *Sharing the 'Real Me' – How Usage Motivation and Personality Relate to Privacy Protection Behavior on Facebook.* In: *Human Aspects of Information Security, Privacy and Trust.* Ed. by Theo Tryfonas. Cham: Springer International Publishing, 2017, pp. 640–655. ISBN: 978-3-319-58460-7.

[81] Nina Gerber, Paul Gerber, and Melanie Volkamer. *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior.* In: *Computers & Security* 77 (2018), pp. 226–261. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.04.002.

[82] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. *Home Sweet Home? Investigating Users' Awareness of Smart Home Privacy Threats.* In: *Proceedings of An Interactive Workshop on the Human aspects of Smarthome Security and Privacy (WSSP), Baltimore, MD, August 12, 2018.* USENIX, Berkeley, CA, 2018.

[83] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. *Investigating People's Privacy Risk Perception.* In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 3 (2019), pp. 267–288.

[84] Nina Gerber, Verena Zimmermann, and Melanie Volkamer. *Why Johnny Fails to Protect his Privacy.* In: *Proceedings of the 4th European Workshop on Usable Security (EuroUSEC).* IEEE, 2019. DOI: 10.1109/EuroSPW.2019.00019.

[85] Nina Gerber et al. *FoxIT: Enhancing Mobile Users' Privacy Behavior by Increasing Knowledge and Awareness.* In: *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust (STAST).* ACM, 2018, pp. 53–63. ISBN: 978-1-4503-6357-0. DOI: 10.1145/3167996.3167999.

[86] Paul Gerber. *Privatsphäre, gibt?s da nicht 'ne App für? - Verbesserung von Privatsphäre-relevantem Verhalten durch bessere Informationen.* PhD thesis. Darmstadt: Technische Universität, 2017.

[87] Paul Gerber, Melanie Volkamer, and Karen Renaud. *The simpler, the better? Presenting the COPING Android permission-granting interface for better privacy-related decisions.* In: *Journal of Information Security and Applications* (2016). ISSN: 22142126. DOI: 10.1016/j.jisa.2016.10.003.

[88] clickworker GmbH. *clickworker Panel.* https://www.clickworker.com/. Accessed: 2017-09-20.

[89] Google. *System permissions.* https://developer.android.com/guide/topics/permissions/requesting.html{#}normal-dangerous. Accessed: 2017-03-16.

[90] Ellen Van Gool et al. *To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model.* In: *Computers in Human Behavior* 44 (2015), pp. 230–239. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2014.11.036.

[91] Marian Harbach, Sascha Fahl, and Matthew Smith. *Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness.* In: *2014 IEEE 27th Computer Security Foundations Symposium.* 2014, pp. 97–110. DOI: 10.1109/CSF.2014.15.

[92] Marian Harbach et al. *Using personal examples to improve risk communication for security & privacy decisions.* In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems (CHI).* ACM. 2014, pp. 2647–2656.

[93] Abduljaleel Al-Hasnawi, Ihab Mohammed, and Ahmed Al-Gburi. *Performance Evaluation of the Policy Enforcement Fog Module for Protecting Privacy of IoT Data.* In: *2018 IEEE International Conference on Electro/Information Technology (EIT).* 2018, pp. 0951–0957.

[94] Marc Hassenzahl, Sarah Diefenbach, and Anja Göritz. *Needs, affect, and interactive products – Facets of user experience*. In: *Interacting with Computers* 22.5 (2010), pp. 353–362. ISSN: 0953-5438. DOI: https://doi.org/10.1016/j.intcom.2010.04.002.

[95] Marc Hassenzahl and Virpi Roto. *Being and doing: A perspective on user experience and its measurement*. In: *Interfaces* 72 (2007), pp. 10–12.

[96] Ryan Heartfield et al. *A taxonomy of cyber-physical threats and impact in the smart home*. In: *Computers & Security* 78 (2018), pp. 398–428. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.07.011.

[97] Erin E. Hollenbaugh and Amber L. Ferris. *Facebook self-disclosure: Examining the role of traits, social cohesion, and motives*. In: *Computers in Human Behavior* 30 (2014), pp. 50–58. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2013.07.055.

[98] Peter Hornyack et al. *These Aren't the Droids You're Looking for: Retrofitting Android to Protect Data from Imperious Applications*. In: *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS)*. ACM, 2011, pp. 639–652. ISBN: 978-1-4503-0948-6. DOI: 10.1145/2046707.2046780.

[99] Gordon Hull. *Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data*. In: *Ethics and Information Technology* 17.2 (2015), pp. 89–101. ISSN: 1572-8439. DOI: 10.1007/s10676-015-9363-z.

[100] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. *A risk analysis of a smart home automation system*. In: *Future Generation Computer Systems* 56 (2016), pp. 719–733. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2015.09.003.

[101] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. *On the Risk Exposure of Smart Home Automation Systems*. In: *2014 International Conference on Future Internet of Things and Cloud*. 2014, pp. 183–190. DOI: 10.1109/FiCloud.2014.37.

[102] Shubham Jain and Janne Lindqvist. *Should I protect you? Understanding developers' behavior to privacy-preserving APIs*. In: *Proceedings of the Workshop on Usable Security (USEC)*. 2014. DOI: 10.14722/usec.2014.23045.

[103] Haiyan Jia et al. *Risk-taking As a Learning Process for Shaping Teen's Online Information Privacy Behaviors*. In: *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW)*. ACM, 2015, pp. 583–599. ISBN: 978-1-4503-2922-4. DOI: 10.1145/2675133.2675287.

[104] Adam N. Joinson. *Looking at, Looking Up or Keeping Up with People?: Motives and Use of Facebook*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2008, pp. 1027–1036. ISBN: 978-1-60558-011-1. DOI: 10.1145/1357054.1357213.

[105] Ruogu Kang et al. *"My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security*. In: *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2015, pp. 39–52.

[106] Marja Helena Kankaanranta and Pekka Neittaanmäki. *Design and Use of Serious Games, Intelligent Systems Control and Automation*. In: *Science and Engineering* 37 (2009). DOI: 10.1007/978-1-4020-9496-5.

[107] Katherine Karl, Joy Peluchette, and Christopher Schlaegel. *Who's Posting Facebook Faux Pas? A Cross-Cultural Examination of Personality Differences*. In: *International Journal of Selection and Assessment* 18.2 (2010), pp. 174–186. DOI: 10.1111/j.1468-2389.2010.00499.x.

[108] Sabrina Karwatzki et al. *Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence*. In: *European Journal of Information Systems* 26.6 (2017), pp. 688–715. ISSN: 1476-9344. DOI: https://doi.org/10.1057/s41303-017-0064-z.

[109] Mark J. Keith et al. *Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior*. In: *International Journal of Human-Computer Studies* 71.12 (2013), pp. 1163–1173. ISSN: 1071-5819. DOI: https://doi.org/10.1016/j.ijhcs.2013.08.016.

[110] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. *Privacy As Part of the App Decision-making Process*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2013, pp. 3393–3402. ISBN: 978-1-4503-1899-0. DOI: 10.1145/2470654.2466466.

[111] Patrick Gage Kelley et al. *A Conundrum of Permissions: Installing Applications on an Android Smartphone*. In: *Proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC)*. Springer-Verlag, 2012, pp. 68–79. ISBN: 978-3-642-34637-8. DOI: 10.1007/978-3-642-34638-5_6.

[112] Houssain Kettani and Robert M. Cannistra. *On Cyber Threats to Smart Digital Environments*. In: *Proceedings of the 2nd International Conference on Smart Digital Environment (ICSDE)*. ACM, 2018, pp. 183–188. ISBN: 978-1-4503-6507-9. DOI: 10.1145/3289100.3289130.

[113] Wazir Zada Khan, Mohammed Y. Aalsalem, and Muhammad Khurram Khan. *Communal Acts of IoT Consumers: A Potential Threat to Security and Privacy*. In: *IEEE Transactions on Consumer Electronics* 65.1 (2019), pp. 64–72. ISSN: 0098-3063. DOI: 10.1109/TCE.2018.2880338.

[114] Youngseek Kim and Melissa Adler. *Social scientists' data sharing behaviors: Investigating the roles of individual motivations, institutional pressures, and data repositories*. In: *International Journal of Information Management* 35.4 (2015), pp. 408–418. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.04.007.

[115] Barbara Kitchenham. *Procedures for Performing Systematic Reviews*. Tech. rep. Keele University, 2014.

[116] Predrag Klasnja et al. *"When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Everyday Wi-Fi Use*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. New York, NY, USA: ACM, 2009, pp. 1993–2002. ISBN: 978-1-60558-246-7. DOI: 10.1145/1518701.1519004.

[117] Bart P. Knijnenburg. *Privacy? I Can't Even! Making a Case for User-Tailored Privacy*. In: *IEEE Security & Privacy* 15.4 (2017), pp. 62–67.

[118] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. *Dimensionality of information disclosure behavior*. In: *International Journal of Human-Computer Studies* 71.12 (2013), pp. 1144–1162. ISSN: 1071-5819. DOI: https://doi.org/10.1016/j.ijhcs.2013.06.003.

[119] Spyros Kokolakis. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*. In: *Computers & Security* 64 (2017), pp. 122–134. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2015.07.002.

[120] Mehrdad Koohikamali, Natalie Gerhart, and Mohammadreza Mousavizadeh. *Location disclosure on LB-SNAs: The role of incentives on sharing behavior*. In: *Decision Support Systems* 71 (2015), pp. 78–87. ISSN: 0167-9236. DOI: https://doi.org/10.1016/j.dss.2015.01.008.

[121] Hanna Krasnova and Natasha F. Veltri. *Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA*. In: *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2010. DOI: 10.1109/HICSS.2010.307.

[122] Hanna Krasnova et al. *Online Social Networks: Why We Disclose*. In: *Journal of Information Technology* 25.2 (2010), pp. 109–125. DOI: 10.1057/jit.2010.6.

[123] Lydia Kraus, Ina Wechsung, and Sebastian Möller. *Using statistical information to communicate android permission risks to users*. In: *Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE. 2014, pp. 48–55.

[124] Oksana Kulyk et al. *Does This App Respect My Privacy? Design and Evaluation of Information Materials Supporting Privacy-Related Decisions of Smartphone Users*. In: *Workshop on Usable Security (USEC)*. 2019.

[125] Airi Lampinen et al. *We're in It Together: Interpersonal Management of Disclosure in Social Network Services*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2011, pp. 3217–3226. ISBN: 978-1-4503-0228-9. DOI: 10.1145/1978942.1979420.

[126] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. *Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers*. In: *Proceedings of the ACM on Human-Computer Interaction* 2.CSCW (2018), 102:1–102:31. ISSN: 2573-0142. DOI: 10.1145/3274371.

[127] Chung Hun Lee and David A. Cranage. *Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web sites*. In: *Tourism Management* 32.5 (2011), pp. 987–994. ISSN: 0261-5177. DOI: https://doi.org/10.1016/j.tourman.2010.08.011.

[128] Namyeon Lee and Ohbyung Kwon. *A Privacy-aware Feature Selection Method for Solving the Personalization-privacy Paradox in Mobile Wellness Healthcare Services*. In: *Expert Systems with Applications* 42.5 (2015), pp. 2764–2771. ISSN: 0957-4174. DOI: 10.1016/j.eswa.2014.11.031.

[129] Seonglim Lee et al. *The Impact of Perceived Privacy Benefit and Risk on Consumers' Desire to Use Internet of Things Technology*. In: *Human Interface and the Management of Information. Information in Applications and Services*. Ed. by Sakae Yamamoto and Hirohiko Mori. Cham: Springer International Publishing, 2018, pp. 609–619. ISBN: 978-3-319-92046-7.

[130] Tuomas Lehto and Harri Oinas-Kukkonen. *Persuasive Features in Web-Based Alcohol and Smoking Interventions: A Systematic Review of the Literature*. In: *Journal of Medical Internet Research* (2011). DOI: 10.2196/jmir.1559.

[131] Dominik J. Leiner. *SoSci Survey (Version 2.5.00-i)*. https://www.soscisurvey.de/. Accessed: 2017-09-20.

[132] Aniek J. Lentferink et al. *Key Components in eHealth Interventions Combining Self-Tracking and Persuasive eCoaching to Promote a Healthier Lifestyle: A Scoping Review*. In: *Journal of Medical Internet Research*. 2017. DOI: 10.2196/jmir.7288.

[133] Pedro Giovanni Leon et al. *What Matters to Users?: Factors That Affect Users' Willingness to Share Information with Online Advertisers*. In: *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013, 7:1–7:12. ISBN: 978-1-4503-2319-2. DOI: 10.1145/2501604.2501611.

[134] Han Li, Rathindra Sarathy, and Heng Xu. *The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors*. In: *Decision Support Systems* 51.3 (2011), pp. 434–445. ISSN: 0167-9236. DOI: 10.1016/j.dss.2011.01.017.

[135] Han Li, Rathindra Sarathy, and Heng Xu. *Understanding Situational Online Information Disclosure as a Privacy Calculus*. In: *Journal of Computer Information Systems* 51.1 (2010), pp. 62–71. DOI: 10.1080/08874417.2010.11645450.

[136] Kai Li, Zhangxi Lin, and Xiaowen Wang. *An empirical analysis of users' privacy disclosure behaviors on social network sites*. In: *Information & Management* 52.7 (2015), pp. 882–891. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2015.07.006.

[137] Yuan Li. *A Multi-level Model of Individual Information Privacy Beliefs*. In: *Electronic Commerce Research and Applications* 13.1 (Jan. 2014), pp. 32–44. ISSN: 1567-4223. DOI: 10.1016/j.elerap.2013.08.002.

[138] Yuan Li. *The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns*. In: *Decision Support Systems* 57 (2014), pp. 343–354. ISSN: 0167-9236. DOI: https://doi.org/10.1016/j.dss.2013.09.018.

[139] Hui Liang and Min Yong Shi. *Design and Implement a Computer Network Security Education Game on iOS for University Students*. In: *Applied Mechanics and Materials* 373-375 (2013), pp. 1815–1820. ISSN: 1662-7482. DOI: 10.4028/www.scientific.net/AMM.373-375.1815.

[140] Huigang Liang and Yajiong Xue. *Avoidance of Information Technology Threats: A Theoretical Perspective*. In: *MIS Quarterly* 33.1 (2009), pp. 71–90. ISSN: 0276-7783.

[141] Huigang Liang and Yajiong Xue. *Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective*. In: *Journal of the Association for Information Systems* 11.7 (2010), pp. 394–413.

[142] Chechen Liao, Chuang-Chun Liu, and Kuanchin Chen. *Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model*. In: *Electronic Commerce Research and Applications* 10.6 (2011), pp. 702–715. ISSN: 1567-4223. DOI: https://doi.org/10.1016/j.elerap.2011.07.003.

[143] Ilaria Liccardi, Joseph Pato, and Daniel J Weitzner. *Improving user choice through better mobile apps transparency and permissions analysis*. In: *Journal of Privacy and Confidentiality* 5.2 (2014).

[144] Ilaria Liccardi et al. *No technical understanding required: Helping users make informed choices about access to their personal data*. In: *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. 2014, pp. 140–150.

[145] Jialiu Lin et al. *Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing*. In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp)*. ACM, 2012, pp. 501–510. ISBN: 978-1-4503-1224-0. DOI: http://doi.acm.org/10.1145/2370216.2370290.

[146] Jialiu Lin et al. *Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings*. In: *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. 2014, pp. 199–212.

[147] Kuan-Yu Lin and Hsi-Peng Lu. *Why people use social networking sites: An empirical study integrating network externalities and motivation theory*. In: *Computers in Human Behavior* 27.3 (2011), pp. 1152–1161. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2010.12.009.

[148] Eden Litt. *Understanding social network site users' privacy tool use*. In: *Computers in Human Behavior* 29.4 (2013), pp. 1649–1656. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2013.01.049.

[149] Bin Liu et al. *Follow my recommendations: A personalized privacy assistant for mobile app permissions*. In: *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. 2016, pp. 27–41.

[150] Ragnar Löfstedt and Åsa Boholm. *The study of risk in the 21st century*. In: *The Earthscan Reader on Risk*. Earthscan, 2009. ISBN: 9781844076864.

[151] Dominique Machuletz, Stefan Laube, and Rainer Böhme. *Webcam Covering As Planned Behavior*. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2018, 180:1–180:13. ISBN: 978-1-4503-5620-6. DOI: 10.1145/3173574.3173754.

[152] Mary Madden et al. *Public Perceptions of Privacy and Security in the Post-Snowden Era*. In: *Pew Research Center* (2014), pp. 3–57. DOI: 202.419.4372.

[153] Kaitlin Mahar, Amy X. Zhang, and David Karger. *Squadbox: A Tool to Combat Email Harassment Using Friendsourced Moderation*. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2018, 586:1–586:13. ISBN: 978-1-4503-5620-6. DOI: 10.1145/3173574.3174160.

[154] Delfina Malandrino et al. *Privacy awareness about information leakage*. In: *Proceedings of the 12th ACM Workshop on privacy in the electronic society (WPES)* (2013), pp. 279–284. ISSN: 15437221. DOI: 10.1145/2517840.2517868.

[155] Manoj K. Malhotra and Varun Grover. *An Assessment of Survey Research in POM: From Constructs to Theory*. In: *Journal of Operations Management* 16.4 (1998), pp. 407–425.

[156] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*. In: *Information systems research* 15.4 (2004), pp. 336–355.

[157] John Matthews et al. *Persuasive Technology in Mobile Applications Promoting Physical Activity: a Systematic Review*. In: *Journal of Medical Systems* 40.3 (2016), p. 72. ISSN: 1573-689X. DOI: 10.1007/s10916-015-0425-x.

[158] Kathryn McMahon. *Tell the smart house to mind its own business!: Maintaining privacy and security in the era of smart devices*. In: *Fordham Law Review* 86.5 (2018), pp. 2511–2551.

[159] William Melicher et al. *(Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking*. In: *Proceedings on Privacy Enhancing Technologies* 2 (2016), pp. 135–154.

[160] Microsoft. *Visual Studio Achievements Program*. https://blogs.technet.microsoft.com/microsoft{_}blog/2012/01/18/visual-studio-achievements-program-brings-gamification-to-development/. Accessed: 2017-11-21. 2012.

[161] George R. Milne, Andrew J. Rohm, and Shalini Bahl. *Consumers' Protection of Online Privacy and Identity*. In: *The Journal of Consumer Affairs* 38.2 (2004), pp. 217–232. ISSN: 00220078, 17456606.

[162] Caroline Lancelot Miltgen and Dominique Peyrat-Guillard. *Cultural and generational influences on privacy concerns: a qualitative study in seven European countries*. In: *European Journal of Information Systems* 23.2 (2014), pp. 103–125.

[163] Caroline Lancelot Miltgen, Aleš Popovič, and Tiago Oliveira. *Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context*. In: *Decision Support Systems* 56 (2013), pp. 103–114. ISSN: 0167-9236. DOI: https://doi.org/10.1016/j.dss.2013.05.010.

[164] Caroline Lancelot Miltgen and H. Jeff Smith. *Exploring information privacy regulation, risks, trust, and behavior*. In: *Information & Management* 52.6 (2015), pp. 741–759. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2015.06.006.

[165] Curtiss Murphy. *Why Games Work and the Science of Learning*. In: *Selected Papers Presented at MODSIM World 2011 Conference and Expo*. 2012, pp. 383–392.

[166] Nintendo. *Fluidity*. https://www.nintendo.com/games/detail/r1QM8ZnIi2Gku-gAVPoAq3Rc-iL0t4hM. Accessed: 2017-11-21. 2010.

[167] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*. In: *Journal of Consumer Affairs* 41.1 (2007), pp. 100–126. DOI: 10.1111/j.1745-6606.2006.00070.x.

[168] Jason R. C. Nurse, Ahmad Atamli, and Andrew Martin. *Towards a Usable Framework for Modelling Security and Privacy Risks in the Smart Home*. In: *Proceedings of the International Conference on Human Aspects of Information Security, Privacy and Trust*. Springer, 2016, pp. 255–267.

[169] Harri Oinas-Kukkonen and Marja Harjumaa. *Persuasive Systems Design Key Issues, Process Model, and System Features*. In: *Communications of the Association for Information Systems* 24 (2009).

[170] Isabelle Oomen and Ronald Leenes. *Privacy Risk Perceptions and Privacy Protection Strategies*. In: *Policies and Research in Identity Management*. Ed. by Elisabeth de Leeuw et al. 2008, pp. 121–138.

[171] Yong Jin Park. *Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet*. In: *Computers in Human Behavior* 50 (2015), pp. 252–258. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2015.04.011.

[172] Yong Jin Park and S. Mo Jang. *Understanding Privacy Knowledge and Skill in Mobile Communication*. In: *Computers in Human Behavior* 38 (2014), pp. 296–303. ISSN: 0747-5632. DOI: 10.1016/j.chb.2014.05.041.

[173] Anand Paturi, Patrick Gage Kelley, and Subhasish Mazumdar. *Introducing privacy threats from ad libraries to android users through privacy granules*. In: *Proceedings of the Workshop on Usable Security (USEC)* (2015). DOI: http://dx.doi.org/10.14722/usec.2015.23008.

[174] Anicia N. Peters, Heike Winschiers-Theophilus, and Brian E. Mennecke. *Cultural influences on Facebook practices: A comparative study of college students in Namibia and the United States*. In: *Computers in Human Behavior* 49 (2015), pp. 259–271. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2015.02.065.

[175] Scott Plous. *The Psychology of Judgment and Decision Making*. New York, NY, US: McGraw-Hill Inc., 1993.

[176] Maija E Poikela and Felix Kaiser. *"It Is a Topic That Confuses Me"-Privacy Perceptions in Usage of Location-Based Applications*. In: *Proceedings of the 1st European Workshop on Usable Security (EuroUSEC)*. Internet Society, 2016.

[177] Jennifer Dickman Portz et al. *Persuasive features in health information technology interventions for older adults with chronic diseases: a systematic review*. In: *Health and Technology* 6.2 (2016), pp. 89–99. ISSN: 2190-7196. DOI: 10.1007/s12553-016-0130-x.

[178] Stefanie Pötzsch. *Privacy Awareness: A Means to Solve the Privacy Paradox?* In: *The Future of Identity in the Information Society*. Ed. by V. Matyáš et al. Vol. 298. Berlin, Heidelberg: Springer, 2009, pp. 226–236. ISBN: 978-3-642-03314-8. DOI: 10.1007/978-3-642-03315-5_17.

[179] Ismini Psychoula et al. *Users' Privacy Concerns in IoT Based Applications*. In: *Proceedings of the 4th IEEE International Conference on Internet of People (IoP)*. IEEE, 2018, pp. 1887–1894. DOI: 10.1109/SmartWorld.2018.00317.

[180] Lee Rainie et al. *Anonymity, Privacy, and Security Online*. http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx. Accessed: 2019-07-27. 2013.

[181] Beatrice Rammstedt and Oliver P. John. *Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German*. In: *Journal of Research in Personality* 41.1 (2007), pp. 203–212. ISSN: 0092-6566. DOI: https://doi.org/10.1016/j.jrp.2006.02.001.

[182] Ulf-Dietrich Reips and Frederik Funke. *Interval-level measurement with visual analogue scales in Internet-based research: VAS Generator*. In: *Behavior Research Methods* 40.3 (2008), pp. 699–704. ISSN: 1554-3528. DOI: 10.3758/BRM.40.3.699.

[183] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. *Why Doesn't Jane Protect Her Privacy?* In: *Privacy Enhancing Technologies*. Ed. by Emiliano De Cristofaro and Steven J. Murdoch. Cham: Springer International Publishing, 2014, pp. 244–262. ISBN: 978-3-319-08506-7.

[184] Libby Rittenberg and Timothy Trigarthen. *Principles of Microeconomics*. Washington, DC, US: Flat World Knowledge, Inc., 2012.

[185] Carsten Röcker. *Information Privacy in Smart Office Environments: A Cross-Cultural Study Analyzing the Willingness of Users to Share Context Information*. In: *Computational Science and Its Applications – ICCSA 2010. Lecture Notes in Computer Science, vol 6019*. Ed. by David Taniar et al. Berlin, Heidelberg: Springer, 2010, pp. 93–106. ISBN: 978-3-642-12189-0.

[186] Craig Ross et al. *Personality and motivations associated with Facebook use*. In: *Computers in Human Behavior* 25.2 (2009), pp. 578–586. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2008.12.024.

[187] Jungwoo Ryoo et al. *IoE Security Threats and You*. In: *2017 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2017, pp. 13–19. DOI: 10.1109/ICSSA.2017.28.

[188] Souad Sadki and Hanan El Bakkali. *Enhancing privacy on Mobile Health: An integrated privacy module*. In: *Proceedings of the 2014 International Conference on Next Generation Networks and Services (NGNS)*. IEEE, 2014, pp. 245–250. DOI: 10.1109/NGNS.2014.6990259.

[189] Fatima Saleh et al. *Social networking by the youth in the UAE: A privacy paradox*. In: *Proceedings of the 2011 International Conference and Workshop on Current Trends in Information Technology (CTIT)*. 2011, pp. 28–31. DOI: 10.1109/CTIT.2011.6107957.

[190] Shruti Sannon, Natalya N. Bazarova, and Dan Cosley. *Privacy Lies: Understanding How, When, and Why People Lie to Protect Their Privacy in Multiple Online Contexts*. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2018, 52:1–52:13. ISBN: 978-1-4503-5620-6. DOI: 10.1145/3173574.3173626.

[191] Dilshani Sarathchandra, Kristin Haltinner, and Nicole Lichtenberg. *College Students' Cybersecurity Risk Perceptions, Awareness, and Practices*. In: *Proceedings of the 2016 Cybersecurity Symposium (CYBERSEC)*. 2016, pp. 68–73. DOI: 10.1109/CYBERSEC.2016.018.

[192] Florian Schaub et al. *A design space for effective privacy notices*. In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. USENIX. 2015.

[193] Florian Schaub et al. *Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern*. In: *Proceedings of the Workshop on Usable Security (USEC)*. 2016. DOI: http://dx.doi.org/10.14722/usec.2016.23017.

[194] Michael Schiefer. *Smart Home Definition and Security Threats*. In: *Proceedings of the 9th International Conference on IT Security Incident Management IT Forensics*. 2015, pp. 114–118. DOI: 10.1109/IMF.2015.17.

[195] Bruce Schneier. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Berlin, Heidelberg: Springer, 2003. ISBN: 0387026207.

[196] Kathy S. Schwaig et al. *A model of consumers' perceptions of the invasion of information privacy*. In: *Information & Management* 50.1 (2013), pp. 1–12. ISSN: 0378-7206. DOI: https://doi.org/10.1016/j.im.2012.11.002.

[197] Norbert Schwarz et al. *Ease of Retrieval as Information: Another Look at the Availability Heuristic*. In: *Journal of Personality and Social Psychology* 61 (1991), pp. 195–202.

[198] Kennon M. Sheldon et al. *What Is Satisfying About Satisfying Events? Testing 10 Candidate Psychological Needs*. In: *Journal of Personality and Social Psychology* 80.2 (2001), pp. 325–339.

[199] Kennon Sheldon, Neetu Abad, and Christian Hinsch. *A Two-Process View of Facebook Use and Relatedness Need-Satisfaction: Disconnection Drives Use, and Connection Rewards It*. In: *Journal of personality and social psychology* 100 (2011), pp. 766–75. DOI: 10.1037/a0022407.

[200] Pavica Sheldon. *Student Favorite: Facebook and Motives for its Use Student Favorite: Facebook and Motives for its Use*. In: *Southwestern Mass Communication Journal* 23 (2008), pp. 39–55.

[201] Pavica Sheldon. *The Relationship Between Unwillingness-to-Communicate and Students' Facebook Use*. In: *Journal of Media Psychology: Theories, Methods, and Applications* 20 (2008), pp. 67–75. DOI: 10.1027/1864-1105.20.2.67.

[202] Nataliya Shevchuk and Harri Oinas-Kukkonen. *Exploring Green Information Systems and Technologies as Persuasive Systems: A Systematic Review of Applications in Published Research*. In: *Proceedings of the International Conference on Information Systems (ICIS)*. 2016.

[203] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. *Privacy Tipping Points in Smartphones Privacy Preferences*. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 2015, pp. 807–816. ISBN: 978-1-4503-3145-6. DOI: 10.1145/2702123.2702404.

[204] Dong-Hee Shin and Youn-Joo Shin. *Why do people play social network games?* In: *Computers in Human Behavior* 27.2 (2011), pp. 852–861. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2010.11.010.

[205] Fatemeh Shirazi and Melanie Volkamer. *What Deters Jane from Preventing Identification and Tracking on the Web?* In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society (WPES)*. ACM, 2014, pp. 107–116. ISBN: 978-1-4503-3148-7. DOI: 10.1145/2665943.2665963.

[206] Irina Shklovski et al. *Leakiness and creepiness in app space: Perceptions of privacy and mobile app use*. In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems (CHI)*. ACM, 2014, pp. 2347–2356. ISBN: 9781450324731. DOI: 10.1145/2556288.2557421.

[207] Paul Slovic et al. *The Affect Heuristic*. In: *Heuristics and Biases*. Ed. by T. Gilovich, W. D. Griffin, and D. Kahneman. Cambridge, UK: Cambridge University Press, 2002, pp. 397–420.

[208] H. Jeff Smith, Tamara Dinev, and Heng Xu. *Information Privacy Research: An Interdisciplinary Review*. In: *MIS Quarterly* 35.4 (2011), pp. 989–1016. ISSN: 0276-7783.

[209] Teodor Sommestad et al. *Variables influencing information security policy compliance: A systematic review of quantitative studies*. In: *Information Management & Computer Security* 22.1 (2014), pp. 42–75. DOI: 10.1108/IMCS-08-2012-0045.

[210] Daniel S. Soper. *A-priori Sample Size Calculator for Structural Equation Models*. http://www.danielsoper.com/statcalc. Accessed: 2019-07-27. 2019.

[211] Whitney P. Special and Kirsten T. Li-Barber. *Self-disclosure and student satisfaction with Facebook*. In: *Computers in Human Behavior* 28.2 (2012), pp. 624–630. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2011.11.008.

[212] Jessica Staddon, Alessandro Acquisti, and Kristen LeFevre. *Self-Reported Social Network Behavior: Accuracy Predictors and Implications for the Privacy Paradox*. In: *Proceedings of the 2013 International Conference on Social Computing*. 2013, pp. 295–302. DOI: 10.1109/SocialCom.2013.48.

[213] Simon Stockhardt et al. *Teaching Phishing-Security: Which Way is Best?* In: *Proceedings of the 31st International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*. Springer, 2016, pp. 135–149.

[214] Anselm L. Strauss. *Qualitative analysis for social scientists*. New York, NY, US: Cambridge University Press, 1987. DOI: 10.1017/CBO9780511557842.

[215] Anselm L. Strauss and Juliet M. Corbin. *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA, US: Sage Publications, Inc., 1990.

[216] Fred Stutzman and Jacob Kramer-Duffield. *Friends Only: Examining a Privacy-enhancing Behavior in Facebook*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2010, pp. 1553–1562. ISBN: 978-1-60558-929-9. DOI: 10.1145/1753326.1753559.

[217] Jose M. Such et al. *Photo Privacy Conflicts in Social Media: A Large-scale Empirical Study*. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2017, pp. 3821–3832. ISBN: 978-1-4503-4655-9. DOI: 10.1145/3025453.3025668.

[218] Yao-Ting Sung and Jeng-Shin Wu. *The Visual Analogue Scale for Rating, Ranking and Paired-Comparison (VAS-RRP): A new technique for psychological measurement*. In: *Behavior Research Methods* 50.4 (2018), pp. 1694–1715. ISSN: 1554-3528. DOI: 10.3758/s13428-018-1041-8.

[219] Symantec. *State of privacy report 2015*. Tech. rep. Accessed: 2019-07-27. 2015.

[220] Monika Taddicken. *The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure*. In: *Journal of Computer-Mediated Communication* 19.2 (2014), pp. 248–273. DOI: 10.1111/jcc4.12052.

[221] Mohammed Talal et al. *Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors: Multi-driven Systematic Review*. In: *Journal of Medical Systems* 43.3 (2019). ISSN: 1573-689X. DOI: 10.1007/s10916-019-1158-z.

[222] Joshua Tan et al. *The Effect of Developer-specified Explanations for Permission Requests on Smartphone User Behavior*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2014, pp. 91–100. ISBN: 978-1-4503-2473-1. DOI: 10.1145/2556288.2557400.

[223] Marianthi Theoharidou, Nikolaos Tsalis, and Dimitris Gritzalis. *Smart Home Solutions: Privacy Issues*. In: *Handbook of Smart Homes, Health Care and Well-Being*. Ed. by Joost van Hoof, George Demiris, and Eveline J.M. Wouters. Cham: Springer International Publishing, 2017, pp. 67–81. ISBN: 978-3-319-01583-5. DOI: 10.1007/978-3-319-01583-5_5.

[224] Zouheir Trabelsi, Mohammed Al Matrooshi, and Saeed Al Bairaq. *A Smartphone App for Enhancing Students' Hands-on Learning on Network and DoS Attacks Traffic Generation*. In: *Proceedings of the 17th Annual Conference on Information Technology Education*. SIGITE '16. New York, NY, USA: ACM, 2016, pp. 48–53. ISBN: 978-1-4503-4452-4. DOI: 10.1145/2978192.2978229.

[225] Sabine Trepte et al. *A Cross-Cultural Perspective on the Privacy Calculus*. In: *Social Media + Society* 3.1 (2017). DOI: 10.1177/2056305116688035.

[226] Shari Trewin et al. *Perceptions of Risk in Mobile Transaction*. In: *Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW)*. 2016, pp. 214–223. DOI: 10.1109/SPW.2016.37.

[227] Monique Turner, Christine Skubisz, and Rajiv Rimal. *Theory and Practice in Risk Communication: A Review of the Literature and Visions for the Future*. In: *Handbook of Health Communication (2. ed.)* Ed. by Teresa L. Thompson, Roxanne Parrott, and Jon F. Nussbaum. Routledge, 2011, pp. 146–164.

[228] Amos Tversky and Daniel Kahneman. *Judgment under Uncertainty: Heuristics and Biases*. In: *Science* 185.4157 (1974), pp. 1124–1131. ISSN: 0036-8075. DOI: 10.1126/science.185.4157.1124.

[229] Amos Tversky and Daniel Kahneman. *The framing of decisions and the psychology of choice*. In: *Science* 211.4481 (1981), pp. 453–458. ISSN: 0036-8075. DOI: 10.1126/science.7455683.

[230] Sonja Utz and Nicole C. Kramer. *The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms*. In: *Journal of Psychological Research on Cyberspace* 3.2 (2009).

[231] Melanie Volkamer et al. *A Socio-Technical Investigation into Smartphone Security*. In: *Security and Trust Management. STM 2015. Lecture Notes in Computer Science, vol 9331*. Ed. by Sara Foresti. 2015, pp. 265–273. DOI: 10.1007/978-3-319-24858-5_17.

[232] Robin Wakefield. *The influence of user affect in online information disclosure*. In: *The Journal of Strategic Information Systems* 22.2 (2013), pp. 157–174. ISSN: 0963-8687. DOI: https://doi.org/10.1016/j.jsis.2013.01.003.

[233] Na Wang et al. *Investigating Effects of Control and Ads Awareness on Android Users' Privacy Behaviors and Perceptions*. In: *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services MobileHCI)*. ACM, 2015, pp. 373–382. ISBN: 9781450336529. DOI: 10.1145/2785830.2785845.

[234] Tien Wang, Trong Danh Duong, and Charlie C. Chen. *Intention to disclose personal information via mobile applications: A privacy calculus perspective*. In: *International Journal of Information Management* 36.4 (2016), pp. 531–542. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2016.03.003.

[235] Yang Wang et al. *"I Regretted the Minute I Pressed Share": A Qualitative Study of Regrets on Facebook*. In: *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2011, 10:1–10:16. ISBN: 978-1-4503-0911-0. DOI: 10.1145/2078827.2078841.

[236] Jeffrey Warshaw et al. *Can an Algorithm Know the "Real You"?: Understanding People's Reactions to Hyper-personal Analytics Systems*. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, 2015, pp. 797–806. ISBN: 978-1-4503-3145-6. DOI: 10.1145/2702123.2702274.

[237] Rick Wash. *Folk Models of Home Computer Security*. In: *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2010, 11:1–11:16. ISBN: 978-1-4503-0264-7. DOI: 10.1145/1837110.1837125.

[238] Takuya Watanabe et al. *Understanding the inconsistencies between text descriptions and the use of privacy-sensitive resources of mobile apps*. In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. USENIX, 2015, pp. 241–255.

[239] Susan Waters and James Ackerman. *Exploring Privacy Management on Facebook: Motivations and Perceived Consequences of Voluntary Disclosure*. In: *Journal of Computer-Mediated Communication* 17.1 (2011), pp. 101–115. DOI: 10.1111/j.1083-6101.2011.01559.x.

[240] James Q. Whitman. *The Two Western Cultures of Privacy: Dignity Versus Liberty*. In: *Yale Law Journal* 113 (2004).

[241] Gina Wildeboer, Saskia M. Kelders, and Julia E.W.C. van Gemert-Pijnen. *The relationship between persuasive technology principles, adherence and effect of web-Based interventions for mental health: A meta-analysis*. In: *International Journal of Medical Informatics* 96 (2016), pp. 71–85. ISSN: 1386-5056. DOI: https://doi.org/10.1016/j.ijmedinf.2016.04.005.

[242] David W. Wilson and Joseph S Valacich. *Unpacking the privacy paradox: Irrational decision-making within the privacy calculus*. In: *Proceedings of the International Conference on Information Systems (ICIS)*. 2012, pp. 4152–4162. ISBN: 9781627486040.

[243] Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather R. Lipford. *Making privacy personal: Profiling social network users to inform privacy education and nudging*. In: *International Journal of Human-Computer Studies* 98 (2017), pp. 95–108.

[244] Pamela Wisniewski, Heather Lipford, and David Wilson. *Fighting for My Space: Coping Mechanisms for Sns Boundary Regulation*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2012, pp. 609–618. ISBN: 978-1-4503-1015-4. DOI: 10.1145/2207676.2207761.

[245] Pamela Wisniewski et al. *"Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors*. In: *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW)*. ACM, 2015, pp. 302–316. ISBN: 978-1-4503-2922-4. DOI: 10.1145/2675133.2675293.

[246] Ralf De Wolf, Koen Willaert, and Jo Pierson. *Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook*. In: *Computers in Human Behavior* 35 (2014), pp. 444–454. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2014.03.010.

[247] Kim Wuyts, Riccardo Scandariato, and Wouter Joosen. *LIND(D)UN privacy threat tree catalog*. https://lirias.kuleuven.be/retrieve/282270. Accessed: 2019-07-27. 2014.

[248] Wenjing Xie and Cheeyoun Kang. *See you, see me: Teenagers' self-disclosure and regret of posting on social network site*. In: *Computers in Human Behavior* 52 (2015), pp. 398–407. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2015.05.059.

[249] Anna Xu, Taridzo Chomutare, and Sriram Iyengar. *Systematic Review of Behavioral Obesity Interventions and Their Persuasive Qualities*. In: *Persuasive Technology*. Ed. by Anna Spagnolli, Luca Chittaro, and Luciano Gamberini. Cham: Springer International Publishing, 2014, pp. 291–301. ISBN: 978-3-319-07127-5.

[250] Feng Xu, Katina Michael, and Xi Chen. *Factors affecting privacy disclosure on social network sites: an integrated model*. In: *Electronic Commerce Research* 13.2 (2013), pp. 151–168. ISSN: 1572-9362. DOI: 10.1007/s10660-013-9111-6.

[251] Heng Xu, Robert E. Crossler, and France Bélanger. *A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers*. In: *Decision Support Systems* 54.1 (2012), pp. 424–433. ISSN: 01679236. DOI: 10.1016/j.dss.2012.06.003.

[252] Heng Xu et al. *Research Note–Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services*. In: *Information Systems Research* 23.4 (2012), pp. 1342–1363. DOI: 10.1287/isre.1120.0416.

[253] Heng Xu et al. *The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing*. In: *Decision Support Systems* 51.1 (2011), pp. 42–52. ISSN: 0167-9236. DOI: https://doi.org/10.1016/j.dss.2010.11.017.

[254] Alyson Leigh Young and Anabel Quan-Haase. *Privacy protection strategies on Facebook*. In: *Information, Communication & Society* 16.4 (2013), pp. 479–500.

[255] Aristea M. Zafeiropoulou et al. *Unpicking the Privacy Paradox: Can Structuration Theory Help to Explain Location-based Privacy Decisions?* In: *Proceedings of the 5th Annual ACM Web Science Conference (WebSci)*. ACM, 2013, pp. 463–472. ISBN: 978-1-4503-1889-1. DOI: 10.1145/2464464.2464503.

[256] Eric Zeng, Shrirang Mare, and Franziska Roesner. *End User Security and Privacy Concerns with Smart Homes*. In: *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2017, pp. 65–80. ISBN: 978-1-931971-39-3.

[257] Bo Zhang and Heng Xu. *Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes*. In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW)*. ACM, 2016, pp. 1676–1690. ISBN: 978-1-4503-3592-8. DOI: 10.1145/2818048.2820073.

[258] Bo Zhang et al. *Effects of Security Warnings and Instant Gratification Cues on Attitudes Toward Mobile Websites*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2014, pp. 111–114. ISBN: 978-1-4503-2473-1. DOI: 10.1145/2556288.2557347.

[259] Serena Zheng et al. *User Perceptions of Smart Home IoT Privacy*. In: *Proceedings of the ACM on Human-Computer Interaction (CSCW)*. ACM, 2018. DOI: 10.1145/3274469.

[260] Tao Zhou. *Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors*. In: *Information Systems Frontiers* 17.2 (2015), pp. 413–422. ISSN: 1572-9419. DOI: 10.1007/s10796-013-9413-1.

[261] Yajin Zhou et al. *Taming Information-stealing Smartphone Applications (on Android)*. In: *Proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST)*. Springer, 2011, pp. 93–107. ISBN: 978-3-642-21598-8.

[262] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. *Privacy in the Internet of Things: threats and challenges*. In: *Security and Communication Networks* 7.12 (2014), pp. 2728–2742. DOI: 10.1002/sec.795. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.795.

[263] Sina Zimmermann and Nina Gerber. *Why Do People Use Digital Applications? A Qualitative Analysis of Usage Goals and Psychological Need Fulfillment*. In: *i-com* 18.3 (2019), pp. 271–285. DOI: 10.1515/icom-2018-0041.

[264] Michael Zyda. *From visual simulation to virtual reality to games.* In: *Computer* 38.9 (2005), pp. 25–32.