

How to Raise Users' Awareness of Online Privacy
An Empirical and Theoretical Approach for Examining the Impact of Persuasive
Privacy Support Measures on Users' Self-Disclosure
on Online Social Networking Sites

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

Zur Erlangung des akademischen Grades

Doktor der Philosophie (Dr. phil.)

genehmigte Dissertation

von

Johanna Schäwel

aus

Ribnitz-Damgarten

1. Gutachterin: Prof. Dr. Nicole Krämer
 2. Gutachterin: Prof. Dr. Maritta Heisel
- Tag der mündlichen Prüfung: 10.12.2018

DuEPublico

Duisburg-Essen Publications online

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

ub

universitäts
bibliothek

Diese Dissertation wird über DuEPublico, dem Dokumenten- und Publikationsserver der Universität Duisburg-Essen, zur Verfügung gestellt und liegt auch als Print-Version vor.

DOI: 10.17185/duepublico/70691

URN: urn:nbn:de:hbz:464-20191108-140849-1

Alle Rechte vorbehalten.

Acknowledgments

This dissertation would not have been possible without the support, the encouragement and the guidance by the people who joined me through this challenging, exciting, and wonderful experience.

I thank Nicole Krämer, who supervised and supported me, who trusted in my ideas and who widened my horizon in research. Thank you for all your valuable advices and for encouraging me along the way with the arising tasks, challenges, and opportunities.

Further, I would like to thank Maritta Heisel, who also guided me from the beginning of this journey and who enhanced my work through providing me with constant critical, constructive, and motivating feedback.

I wish to thank every single person who contributed to this work.

Thank you for your assistance, your critical reviews, your valuable feedback, for your methodological and technical support, and for every single sparking discussion.

Thank you for your time, your energy, your emotional support in tough times, and for making me enjoy this work even more.

Thank you for encouraging and believing in me – even in times in which I did not.

Thank you for sharing all the ups and downs with me.

Thank you for your patience and your love.

Thank you for everything.

TABLE OF CONTENTS

LIST OF TABLES.....	10
Abstract.....	17
Zusammenfassung.....	19
I INTRODUCTION.....	22
II THEORETICAL FRAMEWORK.....	24
1 The Assets and Drawbacks of Social Media.....	24
2 The Value of People’s Privacy.....	27
2.1 Defining Privacy.....	27
2.2 Online Privacy – An Untamable Challenge?.....	30
3 Privacy Decisions Based on the Assessed Sensitivity of Information and Related Risks.....	33
3.1 Making Decisions.....	34
3.2 The Nature of Risks.....	36
3.3 The Sensitivity of Information.....	37
3.4 A Synthesis of Decision-Making, Risks and Sensitive Information.....	39
4 Disclosing the Self.....	41
4.1 The Offset between Online Self-Disclosure and Online Privacy.....	42
4.2 Temptation of Self-Disclosure – Impulses as a Threat to Privacy.....	45
4.3 Spontaneous Behavior - A Challenge for Privacy Protection.....	45
5 Planned Privacy Behavior.....	48
5.1 Explaining the Privacy Paradox.....	49
5.2 Boon for Privacy or Bane to Self-Presentation? The Privacy Calculus.....	53
5.3 Online Privacy Behavior in the Light of the Theory of Planned Behavior.....	54
5.4 Privacy Protection Motivation.....	56

5.5	Increasing Users' Protection Motivation	58
6	The Impact of Personal Characteristics on Online Privacy Behavior	60
6.1	The Impact of Users' Personality on Online Privacy Behavior	60
6.2	Individual Characteristics as Influencing Factors for Privacy Behavior	62
6.2.1	Need for Privacy	63
6.2.2	Need for Popularity	64
6.2.3	Impression Management	65
6.2.4	Narcissism	67
6.2.5	Need for Cognition	69
6.2.6	Self-Control	70
6.3	Further User-Specific Factors	71
6.3.1	Differences in Privacy Behavior depending on Users' Sex	72
6.3.2	The Impact of Privacy Norms	73
6.3.3	The Impact of Privacy Concerns	74
7	Privacy Protection	76
7.1	The Importance of Protecting Online Privacy	77
7.2	Self-Regulated Privacy: The Appeal of Alternative Protection Strategies	78
8	Technical Privacy Protection	81
8.1	An Interdisciplinary Approach	81
8.2	Self-Adaptive Systems for Privacy Protection	82
8.3	Requirements for Technical Privacy Support	84
8.4	Privacy-Enhancing Design of Systems	88
8.5	Persuasive Privacy Support	94
8.6	The Construct of Persuasion	94
8.6.1	Nudging and Prompting	96
8.6.2	Opportunities to Combine Persuasion and Prompting for Online Privacy Protection	101
9	Summary of Underlying Theories and Approaches	103
III	REQUIREMENTS FOR USER-CENTERED PRIVACY SUPPORT	108

10	Study 1: Paving the Way for Technical Privacy Support - A Qualitative Study of Users' Intentions to Engage in Online Privacy Protection	108
10.1	The Importance of Protecting Online Privacy	109
10.2	Motives for Utilizing Privacy Protective Measures	109
10.3	Users' Perception of their Own Privacy Knowledge	110
10.4	Elicitation of Requirements	111
10.5	Method.....	112
10.6	Results	114
10.7	Discussion.....	129
10.8	Limitations.....	136
10.9	Future Research	137
10.10	Conclusion.....	137
IV	OPTING-OUT FROM SNSs.....	139
11	Study 2: Time-Out for Privacy Concerns - Investigating Motives and Influencing Factors for Deactivating One's Facebook Account as an Alternative Strategy for Regulating Online Privacy	139
11.1	Motives for Opting-Out	140
11.2	Maintaining Privacy Through Regulating Self-Disclosure?	142
11.3	Privacy Concerns as Driver for Privacy Protection	143
11.4	The Role of Online Privacy Literacy	144
11.5	Situational Impression Management Behavior	145
11.6	Method.....	146
11.6.1	Measures	147
11.6.2	Sample.....	151
11.7	Results	151
11.7.1	Descriptive Results	151
11.7.2	Testing of Hypotheses and Research Questions.....	152
11.8	Discussion.....	155
11.9	Limitations and Future Work.....	160

11.10	Conclusion.....	161
V	THE IMPACT OF PERSUASIVE PRIVACY SUPPORT MEASURES ON USERS'	
	ACTUAL PRIVACY BEHAVIOR	163
12	Study 3: Do You Really Want to Disclose This? - Examining User-Oriented Variables that Influence the Impact of Persuasive Privacy Prompts for Reducing Online Privacy Risks	164
12.1	Increasing Privacy Through Reasoned Persuasive Prompting.....	165
12.2	Setting: The Social Network Site.....	166
12.3	Hypotheses	170
12.4	Method.....	173
12.4.1	Measures	174
12.4.2	Sample.....	178
12.5	Results	179
12.6	Discussion.....	202
12.7	Limitations and Future Work.....	211
12.8	Conclusion.....	212
13	Study 4: The Influence of Persuasive Privacy Support on the Dynamics of Self-Disclosure, Self-Withdrawal, and Calculating Privacy	214
13.1	Introduction	214
13.2	Calculating Online Privacy.....	216
13.3	Processing of Privacy-Relevant Information and Privacy-Aware Decision-Making	217
13.4	Persuasion and Personality	218
13.5	Hypotheses	220
13.6	Method.....	222
13.6.1	Measures	225
13.6.2	Sample.....	227
13.7	Hypotheses Testing.....	229
13.8	Discussion.....	241
13.9	Limitations.....	249

13.10	Conclusion.....	250
VI	GENERAL DISCUSSION	252
14	Synopsis of the Underlying Research Model and Empirical Results	252
15	Summary of the Main Findings.....	253
16	The Influence of Intrapersonal and Environmental Factors on Users' Online Privacy Behavior	
	256	
16.1.1	Intrapersonal Factors.....	258
16.1.2	Environmental Factors	279
17	Theoretical Implications.....	282
18	Practical Implications.....	286
19	Ethical implications.....	290
20	Limitations	291
21	Future Directions.....	292
22	Conclusion	294
	References	295

Appendix

Please contact the author if you are interested to obtain the following material:

Study 1: Interviewer guideline

Study 2: Questionnaire

Study 3: Stimulus material (SNS)

Study 4: Stimulus material (SNS)

LIST OF TABLES

Table 1 Overview of all codes related to the research questions (Study 1).....	113
Table 2 Items for measuring situational impression management behavior, including mean values and standard deviation (Study 2).	148
Table 3 Factor loads of factor analysis examining the motives for using the super-logoff (Study 2).	150
Table 4 Absolute numbers and percentages of participants in each experimental group (Study 3).	167
Table 5 Overview of the persuasive privacy prompts (Study 3).	169
Table 6 Items measuring privacy concerns regarding different dimensions of privacy (Study 3).	176
Table 7 Items for measuring intended future usage of a privacy support system (Study 3).	177
Table 8 Items evaluating the persuasive privacy prompts (Study 3).....	178
Table 9 Descriptive statistics of participants for all experimental groups (Study 3). .	179
Table 10 Number of empty fields for female and male participants (Study 3).....	183
Table 11 Means and standard deviations for participants' susceptibility to the persuasive styles authority and consensus (Study 3).....	185
Table 12 Statistics of the coefficients of the moderated regression analysis examining the interaction between the persuasive style of a privacy prompt (-1 = authority, 1 = consensus) and the number of changes, considering the susceptibility to the persuasive style authority (SuAu) as moderator variable and controlling for sex (-1 = male, 1 = female) for n = 150 (Study 3)	186
Table 13 Statistics of the coefficients of the moderated regression analysis examining the interaction between the persuasive style of a privacy prompt (-1 = authority, 1 = consensus) and the number of changes, considering the susceptibility to the persuasive style consensus (SuCo) as moderator variable and controlling for sex (-1 = male, 1 = female) for n = 150 (Study 3)	187
Table 14 Hierarchical multiple regression analysis including vulnerable narcissism as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3).....	188

Table 15 Hierarchical multiple regression analysis including need for privacy as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3).....	189
Table 16 Hierarchical multiple regression analysis including need for popularity as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3).....	189
Table 17 Hierarchical multiple regression analysis including grandiose narcissism as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3).....	190
Table 18 Mean values and standard deviations of participants' personality traits (N = 187; Study 3)	191
Table 19 Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' need for privacy (NfPr) as moderator variable and controlling for sex (-1 = male, 1 = female) for N = 187 (Study 3).....	192
Table 20 Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' need for popularity (NfPo) as moderator variable and controlling for sex (-1 = male, 1 = female) for N = 187(Study 3).....	193
Table 21 Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' vulnerable narcissism (VuNa) as moderator variable and controlling for sex (-1 = male, 1 = female) for N = 187(Study 3).....	194
Table 22 Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' grandiose narcissism (GraNa) as moderator variable and controlling for sex (-1 = male, 1 = female) for N = 187(Study 3).....	195
Table 23 Hierarchical multiple regression analysis including psychological privacy concerns as predictor and sex (-1 = male, 1 = female) as control variable (Study 3) ..	196
Table 24 Mean values and standard deviations of participants' self-reported privacy concerns, attitudes, intentions and behavior (Study 3).....	197
Table 25 Bivariate correlations between behavioral data and self-reports for the control-group (Study 3)	198
Table 26 Bivariate correlations between behavioral data and self-reports for all experimental groups (Study 3)	198

Table 27 Absolute numbers of participants regarding disclosure vs. no disclosure in free-text input fields about the political opinion (Study 3)	200
Table 28 Absolute numbers of participants regarding disclosure vs. no disclosure in free-text input fields about the self (Study 3)	200
Table 29 Users' suggestions for improvement of persuasive privacy prompts.....	202
Table 30 Attributes and levels in the choice-based conjoint task (Study 4).....	224
Table 31 Hierarchical analysis of regression including intervention vs. no intervention as independent variable, sex (-1 = male, 1 = female) as control variable and the number of empty fields as dependent variable (Study 4)	229
Table 32 Hierarchical analysis of regression including “ntervention vs. no intervention as independent variable, sex (-1= male, 1 = female) as control variable, and the sensitivity of disclosure (0 = no disclosure, 1 = disclosure not related to the self, 2 = disclosure related to the self) as dependent variable (Study 4)	230
Table 33 Hierarchical analysis of regression including intervention vs. no intervention as independent variable, sex (-1 = male, 1 = female) as control variable, and the comprehensiveness of disclosure as dependent variable (Study 4).....	231
Table 34 Hierarchical multiple regression analysis including the dummy-coded privacy interventions as independent variable, sex (-1 = male, 1 = female) as control variable and the number of empty fields as dependent variable (Study 4)	232
Table 35 Descriptive statistics regarding user experience for all experimental groups	233
Table 36 Partial correlations between the personal variables of participants and the dependent behavioral variables empty fields, sensitivity of self-disclosure, and number of disclosed categories of self-disclosure, controlled for sex (Study 4).....	237
Table 37 Average utility and importances with standard deviations for every attribute and its corresponding levels of the CBC task for the full sample N = 380 (Study 4) ..	238
Table 38 Hierarchical analysis of regression including need for cognition as predictor, sex (-1 = male, 1 = female) as control variable, and CBC severity of consequences as dependent variable (Study 4).....	241
Table 39 Hierarchical analysis of regression including need for cognition as predictor, sex (-1 = male, 1 = female) as control variable (Study 4)	241

LIST OF FIGURES

Figure 1: Feedback loop between the user and the privacy support system, see Díaz Ferreyra, Schäwel, Heisel, & Meske (2016)	83
Figure 2: Hypothesized overarching research model.....	107
Figure 3: Requirements for a technical privacy support system derived from interviews on the theoretical basis of the theory of planned behavior (Ajzen, 1991).....	129
Figure 4: Persuasive privacy prompts (Study 3).	170
Figure 5: Absolute numbers of participants using the specific SNS (Study 3).....	179
Figure 6: Absolute numbers of empty fields (Study 3).	180
Figure 7: Absolute numbers of changes (Study 3).	181
Figure 8: Mean values for male and female participants receiving a persuasive privacy prompt versus not receiving a persuasive privacy prompt (Study 3).	182
Figure 9: Mean values of the number of empty fields (Study 3).....	184
Figure 10: Interaction effect between the persuasive style and provided information (Study 3).	185
Figure 11: Persuasive privacy interventions (Study 4).....	223
Figure 12: Attributes and levels of the CBC scenario (Study 4).	224
Figure 13: SNS usage of participants (Study 4).	228
Figure 14: Total numbers of participants deciding to keep or to delete the profile after the survey (Study 4).....	228
Figure 15: Number of disclosed self-disclosure categories (Study 4).....	231
Figure 16: Participants' positive and negative emotional affect at measurement t1 and t2 (Study 4).	234
Figure 17: Relative importance values of CBC decisions (Study 4).....	240
Figure 18: Modified research model based on empirical investigations.....	257

Figure 19: Integration of the protection motivation theory, the theory of planned behavior, and the privacy calculus285

Figure 20: Integration of the protection motivation theory, the theory of planned behavior, the privacy calculus, and the protection paradox.....288

The studies of this dissertation have been presented in talks and posters at international conferences and summer schools:

Study 1

Schäwel, J. (2017, May). *Paving the way for technical privacy support: A qualitative study on users' intentions to engage in privacy protection*. Paper presented at the annual conference of the International Communication Association, San Diego, CA, USA.

Schäwel, J. (2017, March). *Paving the way for technical privacy support: A qualitative study on users' intentions to engage in privacy protection*. Poster presented at Interdisciplinary College: Creativity and Intelligence in Brains and Machines, Möhnesee-Günne, Germany.

Study 2

Schäwel, J., Baldy, C., & Krämer, N. C. (2017, September). *An alternative strategy for regulating privacy on online Social Networking Sites: Motives and influencing factors for using the Super Log-Off*. Paper presented at the 10th Conference of the Media Psychology Division of the German Psychological Society, Landau, Germany.

Study 3

Schäwel, J., & Krämer, N. C. (2018, September). *Do you really want to disclose? Examining psychological variables that influence the effects of persuasive privacy prompts for reducing online privacy risks*. Forschungsreferat beim 51. Kongress der Deutschen Gesellschaft für Psychologie, Frankfurt, Deutschland.

Schäwel, J. (2018, May). *How to raise users' awareness of online privacy*. Poster presented at 4th International Summer School „Trust in mediated communication”, Münster, Germany.

Study 4

Schäwel, J. & Krämer, N. C. (2019, September). *The impact of persuasive privacy interventions on online privacy behavior and the evaluation of privacy risks and benefits*. Paper presented at the 11th Conference of the Media Psychology division of the German Psychological Society, Chemnitz, Germany.

Abstract

Social Networking Sites (SNSs) are commonly used to communicate and connect with people across physical boundaries all over the world. Beyond that, SNSs have become public platforms that are increasingly used for extensive self-disclosure. Disclosing the self on the Internet can entail beneficial outcomes such as getting appreciation or social support. Strikingly, self-disclosure on SNSs can cause privacy risks and negative outcomes, affecting different dimensions of people's privacy, as well. From an interdisciplinary perspective, this work addresses the threat to people's privacy in the ubiquitous and heterogeneous online world. Specifically, this dissertation examines possibilities of empowering users with regard to online privacy protection through utilizing technical privacy interventions, which are communicating current privacy risks to the users. Accordingly, users' privacy needs, personal characteristics, and situational motivations to disclose or withdraw the self are considered. Taken together, this work investigated the impact of technical privacy interventions on users' actual privacy behavior under the consideration of intrapersonal factors by means of four empirical studies.

Users' self-disclosure and self-withdrawal behavior on SNSs as well as their individual needs and requirements for technical privacy interventions were explored qualitatively in Study 1. A paradoxical relation between users' desire for privacy and their mistrust in technical privacy interventions was revealed. In sum, Study 1 functioned as fruitful basis for the following studies that further investigated the qualitative findings regarding users' privacy behavior and needs. Study 2 quantitatively assessed users' attitudes toward an opting-out measure (super-logoff; i.e. self-withdrawal), concrete motives for opting-out (which revealed to be *avoidance of pressure*, *protection from personal attacks*, and *avoidance of distraction*), and their behavioral intention to opt-out. Data demonstrated positive relations between the intention to opt-out and each, corresponding attitudes, intentions, amount of self-disclosure, privacy concerns, and impression management motivation. Through an experimental study (Study 3), users' actual privacy behavior was investigated within a non-artificial SNS environment after being exposed to persuasive privacy prompts either in a consensual or in an authoritarian style of communication (with varying degree of provided information within the prompts). The presence of persuasive privacy prompts was related to data parsimony of

participants. Persuasive interventions in a consensual style were more effective if less (compared to more) information was provided within the prompt, whereas the impact of interventions in an authoritarian style did not differ regarding high and low amount of information. Study 4 provided further evidence for the findings of Study 3 through showing that improved persuasive privacy interventions in a consensual style with a moderate amount of information and dynamic adaptation to the current privacy level (i.e. change in color of the privacy intervention depending on the amount of disclosed information) in an SNS environment was positively related to information withdrawal. Study 4 further demonstrated that for privacy-related decision-making (i.e. privacy calculus), the anticipated severity of a negative consequence of disclosing the self is a more decisive factor than the likelihood of its occurrence and anticipated benefits of self-disclosure. In both, Study 3 and Study 4, privacy behavior itself was influenced by specific intrapersonal factors whereas the impact of the privacy intervention was not influenced by individual characteristics.

Overall, findings partly contradict prior research but provide valuable practical implications indicating that technical privacy interventions for online environments should focus on risk-communication through transmitting basic information regarding potential consequences of self-disclosure in a consensual style of communication.

This dissertation contributes to the research field of online privacy by providing actual behavioral data as a response to technical privacy interventions that were designed alongside user requirements (derived from Study 1), and further investigated quantitatively with respect to intrapersonal factors. In addition, insights into the black box of the privacy calculus (Culnan & Armstrong, 1999), stressing the relevance of the severity of negative outcomes related to self-disclosure, are revealed. The findings of four empirical studies are discussed by drawing on the theory of planned behavior (Ajzen, 1991), the protection motivation theory (Rogers, 1975) and the privacy calculus (Culnan & Armstrong, 1999). In sum, this work reflects on the promising opportunities of utilizing technical measures for protecting users' individual online privacy but also on its challenges with regard to the maintenance of users' autonomy and self-determined – but privacy-aware – behavior.

Zusammenfassung

Die Nutzung von sozialen online Netzwerken erlaubt es, physische Grenzen zu überwinden und mit Menschen auf der ganzen Welt zu kommunizieren. Darüber hinaus repräsentieren soziale Netzwerkseiten öffentliche Plattformen, welche zunehmend zur umfassenden Selbstdarstellung und Selbstoffenbarung verwendet werden. Selbstoffenbarung im Internet kann sowohl positive Auswirkungen wie Anerkennung oder soziale Unterstützung, als auch negative Konsequenzen wie den Verlust der individuellen Privatheit mit sich bringen. Die vorliegende Dissertation beschäftigt sich aus interdisziplinärer Perspektive mit der zunehmenden Bedrohung der Privatheit von Nutzenden sozialer Netzwerkseiten in der digitalisierten Welt. Vor diesem Hintergrund analysiert die vorliegende Arbeit verschiedene Methoden zum individuellen Schutz der Privatheit der Nutzerinnen und Nutzer sozialer Netzwerkseiten. Dabei wird die Auswirkung von technischen Interventionsmaßnahmen zur persuasiven Risiko-Kommunikation auf das tatsächliche Nutzungsverhalten unter Berücksichtigung intrapersoneller Faktoren (z.B. das Bedürfnis nach Privatheit), anhand von vier empirischen Studien untersucht.

Das Selbstoffenbarungsverhalten der Nutzerinnen und Nutzer sowie ihre individuellen Bedürfnisse und Anforderungen an technische Interventionsmaßnahmen wurden in Studie 1 qualitativ analysiert. Es zeigte sich ein paradoxer Zusammenhang zwischen dem Wunsch nach gesteigerter Privatheit und dem Misstrauen gegenüber technischer Interventionsmaßnahmen. Studie 2 beleuchtete die Einstellung der Nutzenden gegenüber einer *Opt-out*-Maßnahme („super-logoff“, d.h. temporäre Abmeldung aus dem Netzwerk Facebook), konkrete Motive für diese temporäre Abmeldung (die sich als *Vermeidung von Druck*, *Schutz vor persönlichen Angriffen* und *Vermeidung von Ablenkung* erwiesen) und die konkrete Verhaltensabsicht der Abmeldung aus dem Netzwerk. Die Verhaltensabsicht der temporären Abmeldung stand in einem positiven Zusammenhang mit entsprechenden Verhaltenseinstellungen, dem Umfang der generellen Selbstoffenbarung, den Privatheits-Bedenken und der Motivation zur positiven Selbstdarstellung. Mittels einer experimentellen Studie (Studie 3) wurde das tatsächliche Verhalten von Nutzerinnen und Nutzern in einer realistischen Netzwerk-Umgebung betrachtet, in der sie mit einer Interventionsmaßnahme in Form einer Hinweismail, entweder in einem gemeinschaftlichen oder einem autoritären

Kommunikationsstil (mit variierendem Grad an bereitgestellten Informationen) in Bezug auf die aktuelle Privatheits-Situation konfrontiert wurden. Das Vorhandensein einer Hinweismessage ging mit einer geringeren Menge preisgebender Informationen einher. Interventionen in einem gemeinschaftlichen Stil waren effektiver, wenn weniger (im direkten Vergleich zu mehr) Informationen bereitgestellt wurden, während sich die Auswirkungen von Interventionen in einem autoritären Stil bezüglich der bereitgestellten Informationsmenge nicht unterschieden. Studie 4 untermauert die Ergebnisse aus Studie 3, indem sie zeigte, dass die anhand der Ergebnisse aus Studie 3 modifizierten Hinweismessages in einem gemeinschaftlichen Stil mit einer moderaten Menge an Informationen und dynamischer Anpassung an die aktuelle Privatheits-Situation (d.h. Farbänderung in Abhängigkeit von dem Ausmaß der Selbstoffenbarung) mit geringerer Informationspreisgabe einhergingen. Darüber hinaus zeigte Studie 4, dass das Abwägen von Risiken und Gratifikationen einer Selbstoffenbarung stärker von dem erwarteten Schweregrad einer negativen Folge der Selbstoffenbarung beeinflusst wird als von der Wahrscheinlichkeit, dass negative Konsequenzen eintreten oder dem erwarteten Nutzen, der durch die Selbstoffenbarung entstehen würde. Sowohl in Studie 3 als auch in Studie 4 wurde das Privatheitsverhalten (unabhängig von der Interventionsmaßnahme) durch spezifische intrapersonelle Faktoren beeinflusst, während die Wirkung der Interventionsmaßnahmen nicht zusätzlich durch individuelle Charakteristika beeinflusst wurde.

Aus den gewonnenen Ergebnissen lassen sich wertvolle praktische Implikationen ableiten, welche darauf hindeuten, dass technische Interventionsmaßnahmen eindeutige und kompakte Informationen in Bezug auf Privatheitsrisiken (potenziell in einem gemeinschaftlichen Kommunikationsstil) vermitteln sollten.

Die vorliegende Dissertation trägt zum Forschungsgegenstand der Online-Privatheit bei, indem sie Verhaltensdaten als Reaktion auf technische Interventionsmaßnahmen liefert, welche mittels einer qualitativen Untersuchung abgeleitet und unter Berücksichtigung von intrapersonellen Merkmalen der NutzerInnen sowie ihrer Privatheits-Bedürfnisse untersucht wurden. Darüber hinaus bieten die Ergebnisse der Studie 4 Einblicke in die Blackbox des *privacy calculus* (Culnan & Armstrong, 1999), welche die Relevanz des Schweregrades einer potentiellen negativen

Konsequenz einer Selbstauskunft hervorheben. Die vorliegende Arbeit diskutiert die Ergebnisse von vier empirischen Studien vor dem Hintergrund der *theory of planned behavior* (Ajzen, 1991), der *protection motivation theory* (Rogers, 1975) und des *privacy calculus* (Culnan & Armstrong, 1999). Zusammenfassend reflektiert die vorliegende Arbeit die vielversprechenden Möglichkeiten der Nutzung technischer Maßnahmen zum Schutz der Online-Privatheit, und zugleich die Herausforderungen im Hinblick auf die Wahrung der Autonomie der NutzerInnen sowie des selbstbestimmten – aber Privatheitbewussten – Verhaltens.

I INTRODUCTION

Contemporary social media platforms such as social networking sites (SNSs, e.g., Facebook), microblogs (e.g., Twitter), or instant messenger services (e.g., WhatsApp), allow people to connect, communicate, and interact with others, even beyond physical boundaries (e.g., Ellison & boyd, 2013). However, at the same time, taking advantage of these offers for social connection and self-presentation gives rise to privacy risks such as becoming a victim of bullying, data theft, or stalking (e.g., Doane, Boothe, Pearson, & Kelley, 2016; Kosinski, Stillwell, & Graepel, 2013; Solove, 2008). Therefore, the discrepancies between users' need for social interaction – satisfiable through social media platforms – the associated privacy rights, needs, and concerns, as well as online privacy support measures, became highly relevant issues in the past decades (e.g., Acquisti et al., 2017; Bartsch & Dienlin, 2016; Gross & Acquisti, 2005; Kosinski, Stillwell, & Graepel, 2013; Martin & Shilton, 2016; Masur & Scharrow, 2016; Utz & Krämer, 2009; Wang et al., 2011; Wang et al., 2014; Youyou, Kosinski, Stillwell, 2015). Nonetheless, there is still a gap of knowledge concerning adequate technical measures to secure online privacy and users' intentions to apply privacy protection features while using social media.

In order to diminish this gap, this work investigates users' online privacy protection intentions and behaviors as well as their preferences regarding system-based privacy support measures from an interdisciplinary, user-centered point of view. The aim is to analyze the impact of system-based privacy support measures on users' online privacy behavior (e.g., self-disclosure or withdrawal of information on an SNS) as well as possible moderators (e.g., users' personality traits, privacy concerns, or perceived privacy norms) and mediators (e.g., evaluation of privacy support measures). To date, research concerning the multifaceted realm of online privacy protection often considered either user oriented *or* technologically oriented methods, raising the need for sophisticated consideration of both perspectives in an integrative approach. There is a great opportunity to consult technological features (e.g., real-time support in terms of privacy prompts) as an extension of usual privacy settings provided by SNSs or other (social) media applications (e.g., Cranor, Arjula, & Guduru, 2002; Wang et al., 2011; Wang et al., 2014). However, this opportunity demands user- and system-oriented research regarding usability, applicability, perceived helpfulness, and ethical implications (e.g., Benenson et

al., 2014; Ochs & Lamla, 2017). Since technical features that would accompany users in their daily social online life might be perceived as unwanted interference to their autonomy, they need to be investigated with respect to users' psychological and behavioral patterns and needs. The present thesis integrates these different aspects by using diverse and mixed methodological approaches that focus on the user and his or her characteristics and needs (e.g., the need for privacy or need to express oneself) as well as on system-oriented determinants and requirements (e.g., transparency and applicability). To be more precise, this work combines theoretical considerations from a software engineering perspective (Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016) with applied psychological approaches and theories. Investigations are based on: a qualitative examination of users' requirements concerning system-based privacy support (Study 1); quantitative analyses of users' protection intentions, behaviors, manifestation of personality, and privacy-related knowledge (Study 2); and experimental investigations of actual privacy behavior after being exposed to system-based privacy interventions and corresponding evaluations of possible risks and benefits related to risky self-disclosures on SNSs (Study 3 and Study 4). By virtue of the demand for research concerning the impact and psychological processing of system-based privacy support, this dissertation aims at elaborating exactly these factors and strives for a better understanding of users' behavior after being exposed to supportive measures. Basically, there is a discrepancy between planned and impulsive online privacy behavior that will be referred to with regard to the importance of real-time privacy support. In line with this, a systematic overview of existing privacy support approaches and individual protection strategies is provided, and limitations of existing approaches are discussed in the scope of this work.

The structure of this dissertation is as follows. In order to point out the steadily growing need for research in the realm of online privacy protection, the advantages and disadvantages of social media usage with a focus on assets and drawbacks of SNSs are outlined (Chapter 1). Subsequently, the value of people's privacy and the importance of maintaining privacy with a view to the basic human needs to act as an autonomous and self-determined individual are addressed. Accordingly, fundamental definitions of privacy as well as more recent characterizations of this concept are provided and new challenges of maintaining privacy in the uncontrollable online world are addressed

(Chapter 1). Thereafter, it will be referred to privacy decision-making based on the sensitivity of information by referring to the decisive role of privacy risks (Chapter 1). After having provided a basic understanding for privacy and privacy decision-making, it will be referred to the offset between online privacy and self-disclosure in Chapter 4. These concepts provide the basis for Chapter 5 in which theories for explaining and predicting privacy behavior are summarized. Chapter 6 considers the influence of users' personal characteristics and further intrapersonal factors on their privacy behavior. Chapter 7 emphasizes the relevance of protecting online privacy and introduces self-regulating privacy strategies that are implemented by users of SNSs. Subsequently, current approaches for technical privacy protection are presented and discussed with regard to the chances and open issues. The theoretical framework closes with a hypothesized research model, which summarizes and visualizes the pivotal variables for this work. In Chapter 10, a qualitative study concerning users' requirements for system-based privacy support measures is presented. Chapter 11 presents a quantitative study investigating motives and influencing factors of utilizing an opting-out measure and withdraw from a social network. Drawing on conclusions from qualitative investigations of Study 1 and findings regarding motives and behavioral intentions for online privacy behavior of Study 2, Chapters 12 and 13 present valuable findings regarding users' actual privacy behavior in an SNS environment (Studies 3 and 4). Chapter 14 provides a synopsis of the hypothesized research model and the main findings. Theoretical and practical conclusions of the present dissertation are provided in Chapters 17 and 18. Limitations and future directions are addressed in Chapters 20 and 21. Finally, this work concludes by drawing on empirical results and theoretical investigations in the scope of the present dissertation (Chapter 22).

II THEORETICAL FRAMEWORK

1 The Assets and Drawbacks of Social Media

Social media platforms are commonly used by a heterogeneous group of people from various countries around the world. The number of people in Europe who use the SNS Facebook at least once a month increased from 333 million in the first quarter of 2016 to 377 million in the first quarter of 2018 (Facebook, 2018). Likewise, the number of users

in the United States and Canada increased from 222 million to 241 million. Worldwide, a number of 2,196 billion monthly active users of Facebook was recorded in the first quarter of 2018 (Facebook statistics). As stated in a study regarding cultural patterns of social media usage by Trepte and Masur (2016), around 90% of all respondents from the United States, Great Britain, Germany, The Netherlands, and China logged in to their networks once a day at least (Trepte & Masur, 2016).

For human beings, the relevance of networking and communicating online is not solely elucidated through the overwhelming Facebook usage statistics. In fact, SNS usage can produce immense gratifications, such as building social capital, maintaining friendships and relationships, gathering social support, engaging in impression management, clarifying the self, easily accessing plenty of information, or enjoying entertainment (e.g., Bazarova & Choi, 2014; boyd & Ellison, 2008; Debatin, Lovejoy, Horn, & Hughes, 2009; Smock, Ellison, Lampe, & Wohn, 2011; Hogan, 2010; Ellison, Steinfield, & Lampe, 2007; Krämer, Eimler, & Neubaum, 2014; Krämer & Haferkamp, 2011; Nosko, Wood, & Molema 2010). Research even provides evidence of social media use being neuropsychologically rewarding in terms of specific brain regions related to the limbic system being activated when users share content and receive positive feedback (Meshi, Tamir, & Heekeren, 2015). Within an online social network, users can “publicly articulate connections” (Ellison & boyd, 2013, p. 158) and create individual content that reaches many other people. Furthermore, their unique online identity, allowing for beneficial self-representation, is viewable and searchable for others (Ellison & boyd, 2013). The most common behaviors on SNSs are publishing information (broadcasting), receiving feedback from others, observing other users, providing feedback to other users and comparing oneself with other people (Meshi, Tamir, Heekeren, 2015).

Unavoidably, the transfer of social processes from the offline to the online context also has negative impacts such as users’ perceived pressure to be available for others all the time (e.g., Vorderer, Krömer, & Schneider, 2016), social and informational overload, jealousy, envy, and reduced well-being (mostly with regard to passive usage, which is termed as *lurking*, see Metzger et al., 2012; e.g., Turel & Serenko, 2012; Verduyn, Ybarra, Résibois, Jonides, & Kross, 2017). The most striking negative consequence that is addressed in this work is a loss of privacy.

These negative consequences can occur because users provide (sensitive) information to their social networks, which provides a target area for potential attacks. The provision of sensitive information can happen either actively and intentionally (e.g., through status updates or comments; e.g., Winter et al., 2014) or passively without being aware of it (e.g., via location tracking, clicks, and *likes*; e.g., Kosinski, Stillwell, & Graepel, 2013). On the one hand, shared information on online social networks can be impersonal and detached from private content (e.g., comments regarding fashion, food, or the weather). On the other hand, disclosures can be of a highly personal and sensitive nature (e.g., Nosko, Wood, & Molema 2010), for instance, if they are associated with users' informational data, social relationships, and thoughts or beliefs. These different kinds of information can be assigned to different dimensions of privacy as defined by Burgoon (1982), namely, informational, social, psychological, or physical privacy. These dimensions have been defined with regard to offline privacy behavior but are increasingly applied for examining online privacy behavior as well (e.g., Dienlin & Trepte, 2015; Ruddigkeit, Penzel, & Schneider, 2013) and will be referred to in more detail in Chapter 2.1. Nevertheless, in the context of SNSs, physical privacy might be less relevant than informational, social, and psychological privacy because it is related to delimiting one's own physical space from others and online networks usually represent non-physical environments (see Krämer & Haferkamp, 2011).

Summing up, self-disclosure of sensitive nature is accompanied by privacy risks for the individuals who are sharing it (e.g., Kosinski, Stillwell, & Graepel, 2013; Navarro & Jasinski, 2012; Solove, 2008). Since it applies for all kinds of risks, associated consequences can be of different severity and have various implications. Since it is hard for users to assess the severity of a privacy risk (e.g., due to missing privacy literacy or privacy awareness; e.g., Egelman et al., 2016; see Study 1), and the likelihood of the occurrence of negative consequences associated with sensitive disclosures (e.g., based on optimistic bias; Cho, Lee, Chung, 2010; see Study 1 & Study 4), the present thesis argues that there is a need to raise users' awareness regarding privacy protection on SNSs. This need is further illustrated by privacy violations that still occur (Chapter 2.2), users' dissatisfaction with current privacy measures, or even privacy cynicism (i.e. a "cognitive coping mechanism for users, allowing them to overcome or ignore privacy concerns and engage in online transactions [and self-disclosure]", Hoffmann, Lutz, & Ranzini, 2016,

p. 4) regarding online privacy regulation. The demand for sufficient privacy support raises the question of why maintaining privacy is in fact of high relevance and who can (or has to) take care of it in the apparent uncontrollable online world. Therefore, the following chapter emphasizes the value of privacy (Chapter 2.2) and further discusses the role of privacy in online networks (Chapter 2.2).

2 The Value of People’s Privacy

In order to investigate mechanisms and determinants of online privacy protection, it is necessary to understand the term *privacy* in its origin. Privacy has been defined and examined by many scholars stressing its relevance for individuals and its value for society (e.g., Kokolakis, 2017; Trepte & Reinecke 2011; Vasalou, Joinson, & Houghton, 2015). However, the difficulty of comprehensively defining privacy and distinguishing it from other concepts remains a challenge, particularly in the contemporary digital generation (Acquisti, Taylor, & Wagman, 2016; Thompson & Kaarst-Brown, 2005). In the following, the most influential definitions of privacy will be outlined and integrated in order to generate a basic understanding of the value of people’s privacy.

2.1 Defining Privacy

Privacy in its origin is described as a multidimensional (e.g., Burgoon, 1982), social (e.g., Altman, 1975; Westin, 1967), and dynamic (e.g., Altman, 1975) construct for distinguishing the self from other people. Following Westin (1967, p. 7), privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Westin (1967) further stated that privacy is relevant for an individual’s personal *autonomy*, *emotional release*, *self-evaluation*, and *protected communication*. These functions of privacy illustrate that privacy covers not only individual but also group and organizational levels (see Altman, 1991; Westin, 1967). Altman claims that privacy is the “selective control of access to the self or to one’s group” (1975, p. 18). He further describes privacy as a social process in terms of an interplay of individuals and their physical and social surroundings (Altman, 1975). As already mentioned, Burgoon (1982) further distinguishes between *informational* (identifying information), *social* (distance and proximity toward others), *psychological* (values and beliefs), and *physical* (freedom from surveillance) dimensions

of privacy. For each dimension, there might be specific rules for privacy management and self-regulation. Westin (1967) also postulated different levels of privacy states, namely, *solitude* (freedom from observation), *intimacy* (referring to group seclusion), *anonymity* (freedom from surveillance and identification), and *reserve* (limiting disclosures to others). In privacy research, it is decisive to consider the different levels of privacy instead of having a static understanding of it. Privacy does not simply mean to be anonymous but refers to a complex regulation and balancing of social interactions and individual withdrawal.

Basically, people strive for a balanced level of privacy, which is located on a spectrum between the actual and desired privacy level (Altman, 1975, 1991). The process of balancing privacy depends on several aspects such as social and situational cues (e.g., Li, Sarathy, & Xu, 2010), individual beliefs and experiences (e.g., Cho, Lee, & Chung, 2010), social inputs and outputs (e.g., Altman, 1975; 1991), and the dynamic process of interpersonal control of privacy boundaries (Altman, 1975; 1991). Following Petronio's communication privacy management theory (CPM; 2010), privacy management is driven by humans' concurring needs for privacy on the one hand, and for social interaction on the other hand. Thus, people have to decide what they are disclosing to whom under what circumstances at which point of time (Petronio, 2002) in order to fulfil their most striking and current social needs. In line with these definitions, privacy can be understood as a process of regulating disclosure and withdrawal of personal information by trying to balance individual needs for privacy and sociality and /or popularity (Masur & Scharkow, 2016).

In 2008, Petronio and Durham extended the CPM theory in terms of clarifying the meaning of private information and privacy control in communication processes. Among others, they shed light on the question of what can be regarded as private information by focusing on the users' perspective. People declare information as private if they believe they own it (Petronio & Durham, 2008). In particular, this might be information that was produced by the individual him- or herself, or that clearly delimits the individual from others (Petronio & Durham, 2008) such as ones' insurance number. This quite pragmatic view once again points to the difficulty of generating a distinct definition of privacy and private information. More essentially, against the background of the usage of online social networking platforms, this definition of private information raises a huge problem as it is

often impossible for users to clearly identify the original sender or owner of information in online contexts (e.g., Marwick & boyd, 2014). In online networks, communication circles oftentimes overlap, and information can be transmitted across initially defined boundaries so that the original sender of information has no control over the further processing, transmitting, and spreading of that information (e.g., Marwick & boyd, 2011). This challenges an assumption by Petronio and Durham (2008), who claim that people have the right to control the distribution of private information belonging to them. Nevertheless, SNSs such as Facebook do in fact allow for restricting and defining of the audience, even for single postings (Wilson, Gosling, & Graham, 2012). With such settings, SNSs like Facebook provide the opportunity for users to manage their privacy at least on a basic level, generating the “lowest common denominator” between users’ expectation for privacy protection and the providers’ efforts to adhere to privacy rules and laws. Strikingly, a huge number of users either do not make use of the settings or rely on their biased perception claiming nothing will happen to them personally (e.g., Cho, Lee, & Chung, 2010) leading, for instance, to insufficient audience restriction, thereby affecting users’ social privacy.

Clarke (2006) defines privacy as individuals’ interest to have a personal space in which they are not observed or impaired by other people, organizations, or institutions. Given that privacy was described to consist of several dimensions, Clarke (2006) distinguishes between certain categories of privacy as well. The author discerns *privacy of the person*, *privacy of personal behavior*, *privacy of personal communications*, and *privacy of personal data*. Thereby, *privacy of a person* is described as being concerned with the individual’s body and bodily processes such as requiring consent for blood transfusion or immunization (Clarke, 2006). A person must have the right to decide self-determinedly whether an inference is necessary. Clarke’s (2006) *privacy of a person* is comparable to the physical dimension of privacy by Burgoon (1982), although she did not explicitly point to privacy needs regarding medical processes in her distinction of privacy dimensions. *Privacy of personal behavior* refers to the personal freedom of having specific preferences, habits, and political opinions in public as well as in private places (Clarke, 2006). This definition is related to the psychological dimension of privacy by Burgoon (1982), referring to personal values and beliefs. Given that psychological privacy is a very sensitive dimension, comprising convictions, emotions and fears

(Burgoon, 1982) breaches to an individual's psychological privacy or *privacy of a person* are considered to be very harmful. Disclosures regarding this dimension reflect the inner layers of a person's self, as suggested in the social penetration theory (Altman & Taylor, 1973). *Privacy of personal communications* (Clarke, 2006) is described as the freedom to communicate with other individuals without being observed by third parties. As stated earlier, according to Westin (1967), protected communication is one of the four central functions of people's privacy. *Privacy of personal data* refers to the desire of having control over the availability, usage and transfer of personal data (Clarke, 2006). This dimension is similar to the dimension of informational privacy by Burgoon (1982) and relates to rather superficial layers of self-disclosure (Altman & Taylor, 1973).

Since privacy is a fundamental human right and people feel the need to make self-determined decisions (DeCew 1997), it is very important to maintain these fundamental functions and needs offline as well as online. In online contexts, the challenge of maintaining privacy can be viewed from different perspectives, either from the users themselves, driven by protection motivation, or from external entities that aim at supporting the users. In the scope of this work, both viewpoints are discussed, whereby the focus will be set on external protection methods (here, system-based privacy interventions) taking users' personal traits, behavioral determinants, and specific properties of system-based privacy measures into account.

2.2 Online Privacy – An Untamable Challenge?

People's online privacy behavior has been examined extensively in the past few decades, revealing a wealth of knowledge with regard to variables that influence users' privacy behavior such as personality characteristics (e.g., Masur & Scharnow, 2016; Utz & Krämer, 2009), sociodemographic variables such as age or gender (e.g., Fogel & Nehmad, 2009; Hoy & Milne, 2010), perceived benefits of (sensitive) self-disclosure (e.g., managing relationships and engaging in beneficial self-presentation by striving for social support, e.g., Ellison, Gray, Lampe, & Fiore, (2014); Krämer, Eimler, & Neubaum, 2014; Taddicken, 2011) as well as corresponding intentions and attitudes that lead to actual privacy behavior (e.g., Dienlin & Trepte, 2015). Repeatedly, concurrent privacy concerns and unsecure privacy behavior have been observed in studies (Barnes, 2006; Lee, Park, & Kim, 2013; Zafeiropoulou, Millard, Webber, & O'Hara 2013). This *privacy*

paradox describes the missing link between users' privacy concerns and risky privacy behavior, representing an attitude–behavior gap with regard to online privacy (Barnes, 2006). However, recent approaches point out some methodological limitations of early research on the privacy paradox, namely, the incomplete consideration of influencing factors such as behavioral intentions (e.g., Dienlin & Trepte, 2015) and the complexity of risk evaluation processes. These shortcomings are, for instance, covered by the privacy process model (Dienlin, 2017) and the privacy calculus (Culnan & Armstrong, 1999). The privacy process model claims that an individual engages in privacy regulation if – depending on the privacy context, privacy perception, and current privacy behavior – the present privacy status is not equivalent to the desired status of privacy (Dienlin, 2017). The process of regulating privacy also depends on the perceived controllability of the individual (Dienlin, 2017). These models will be referred to in more detail in Chapter 6.2 (Study 4).

Nevertheless, since conditions and circumstances in online environments are more uncertain and obscure than in offline contexts, the term *online privacy* holds even more complexity than privacy in its origin. Typically, in online environments the boundaries between distinct communication circles become more blurred than in offline settings (e.g., Wisniewski, Lipford, & Wilson, 2012; Vitak, 2012). Users of online SNSs often do not know their audiences and therefore may have difficulties in managing their privacy (e.g., Vitak, 2012). As was stressed by Petronio and Durham (2008) people believe they have the right to control the spreading of their personal information. However, based on the characteristics of online environments (i.e. heterogeneity, openness, and ubiquity), this right of personal data control is threatened, which is, among others, demonstrated by increased numbers of data misuse and identity theft. In 2016, there were 82,649 police-recorded cases of cybercrime in Germany¹. In a survey of 1,017 Internet users in Germany, it was revealed that several participants had experiences of their computers being infected with harmful programs (41%) or of being a victim of spying with regard to access-data (22%; Bitcom Research²); 3% of participants were seriously offended

¹https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (last access: 04th November, 2018)

² https://www.bitkom-research.de/epages/63742557.sf/de_DE/?ObjectPath=/Shops/63742557/Categories/Presse/Pressearchiv_2016/Industrie_im_Visier_von_Cyberkriminellen_und_Nachrichtendiensten (last access: 04th November, 2018)

verbally. However, 48% reported having no experiences of cybercrime at all (Bitcom Research, 2016).

Through sharing personal information online, people create a *collective privacy boundary*, making other users co-authors of specific information (Petronio & Durham, 2008). This can cause a loss of autonomy and control and therefore might confound users' privacy balance (see Westin, 1967). Furthermore, personal information that has been disclosed online reaches not only communication circles comprising other users (i.e. horizontal privacy), but also the network and respective providers (i.e. vertical privacy; Bartsch & Dienlin, 2016; Masur, 2018). To be more precise, horizontal privacy regards privacy protection against misuse of data, attacks by other users (Masur, 2018), cyber-mobbing, or harassment (Doane, Boothe, Pearson, & Kelley, 2016; Navarro & Jasinski, 2012). By contrast, vertical privacy involves privacy issues with regard to security aspects and data protection against misuse by companies who might be interested in selling user data for personal advertisement, potentially involving spam, phishing, or identity theft (e.g., Dabas & Sharma, 2018). This implies that users are exposed to uncontrollable processing of their information with regard to two opposing dimensions (Masur, 2018). Although both, vertical and horizontal privacy need to be addressed by scholars in order to investigate opportunities for comprehensive privacy protection, this work focuses primarily on horizontal privacy. As mentioned, vertical privacy might be understood as a security rather than a pure privacy issue. In fact, there is a difference between privacy and security. IT security considers "the technical side of privacy" (Fischer-Hübner 2001, p. 35), whereas privacy is treated as a social and psychological construct, covering privacy context, perception, self-disclosure, and individual characteristics (Dienlin, 2014).

Owing the diversity of different communication circles and blurred social boundaries (see Petronio, 2010), individuals are exposed to privacy risks when disclosing information online. As stated earlier, Burgoon (1982) defined four categories of privacy (informational, social, psychological, and physical privacy). Referring to these categories, privacy breaches on SNSs can affect users' informational (e.g., through providing the phone number), social (e.g., through neglecting audience settings), psychological (e.g., through disclosing emotions and values), or physical (e.g., in terms of surveillance or unwanted intrusions) privacy, leading to negative outcomes such as data theft, exclusion from social groups, cyber-mobbing, psychological stress,

embarrassment, or even attacks in offline environments (e.g., Fogel & Nehmad 2008; Gross & Acquisti, 2005; Lawler & Molluzzo, 2010; Wang et al., 2011). Being exposed to negative outcomes like negative feedback by other users can result in feelings of frustration or reduced well-being (e.g., Valkenburg, Peter, & Schouten, 2006). In particular, this is the case if disclosures are sensitive, because the more sensitive the information, the worse the feeling of losing control over it.

As is argued in this work, users might be prevented from privacy harms (arising from disclosing sensitive information) by means of system-based persuasive privacy prompts, intervening in real-time (see Chapter 8.4 and 8.5) and supporting users in making privacy-aware decisions. In order for system-based interventions to function and to provide support for privacy-related decision-making, indicators for sensitive information are required. Accordingly, the following sections briefly outline how decision-making processes function and how they are related to online privacy behavior of users. Next, the characteristics of risks and the sensitivity of information will be referred to with regard to risks being involved if sensitive information was disclosed online. Subsequently to the considerations in Chapter 3, the topic of online self-disclosure will be outlined in more detail in Chapter 4, combining the insights regarding the importance of maintaining privacy from Chapter 2 and the processes of assessing sensitivity of information and perceived risks with regard to privacy-related decision-making from Chapter 3.

3 Privacy Decisions Based on the Assessed Sensitivity of Information and Related Risks

Making a decision whether to disclose or conceal personal information depends on the sensitivity of the information that is going to be disclosed. Information sensitivity is a relevant indicator for people who are evaluating whether to disclose or not (see also privacy calculus; Chapter 5.2) and decisive for technical privacy interventions which shall be able to detect a current privacy risk. The assessments of the sensitivity of information might differ between evaluations by the user (i.e. subjectively) and calculations by a system (i.e. objectively). However, whether a disclosure related to the self entails privacy risks, depends on the level of sensitivity of disclosed content.

In order to provide a basic understanding of decision-making and the characteristics of risks, Chapter 3 outlines relevant factors for decision-making processes (Chapter 3.1),

describes the meaning of risks with regard to online decisions and behavior (Chapter 3.2), defines the term *sensitive information* (Chapter 3.3), and finally provides a synthesis of these topics by addressing privacy-related decision-making.

3.1 Making Decisions

A situational cue (e.g., a warning) can trigger either impulsive (amygdala-driven) or reflective and cognitive effortful (located in the prefrontal cortex) processing of information, influencing subsequent decision-making processes (Bechara, 2005; Schiebener & Brand, 2015). The specialty of making decisions is that they beget risks in terms of an uncertainty regarding the outcomes of a decision (Schiebener & Brand, 2015; Yates & Stone, 1992). This is also the case for privacy decisions in online environments. Users of SNSs are making privacy-related decisions every time they disclose or withdraw personal content, regulate their privacy settings, or create or delete an online account. Not all of these decisions are made with the users' full awareness of being in a privacy-relevant situation, but nevertheless they can entail privacy risks or result in privacy protective behaviors.

As explained by Bechara (2005), the impulsive system of decision-making functions based on cues triggering automatic responses through the amygdala system connects characteristics of the cues to its emotional attributes. Some things initially have emotional properties (e.g., food), whereas other things become emotionally attractive based on learning (e.g., money; Bechara, 2005). With regard to online privacy, emotional and affective characteristics can be ascribed to disclosing personal information or photos on SNSs because one has learned that posting personal content can lead to appreciation, social support, or further positive outcomes, which typically represent the benefits of using SNSs (see Ellison et al., 2014; Taddicken, 2011). It is conceivable that social media cues acquire powerful emotional values tempting users to engage in risky self-disclosure of sensitive information. In contrast to the functionality of the impulsive system, the functioning of the reflective system does not require an experience being made (Bechara, 2005). It is also possible that an image of a hypothetical situation triggers a decision (Bechara, 2005). In reference to online privacy, these hypothetical situations might be transmitted by parents, teachers, friends, or the media, affecting the perception of the harms of sensitive information disclosure and its cognitive reflection by an individual.

The reflective system works according to elaborated and strategic decision processes that are able to outperform impulses or habits triggered by the impulsive system (Hofmann, Friese, & Strack, 2009; Smith & DeCoster, 2000). However, the reflective system is energy consuming and requires a large amount of resources in order to detect and inhibit unwanted behavior driven by triggers (Strack & Deutsch, 2004).

People differ with regard to personal characteristics and tendencies (Brand et al., 2008; Kehr, Kowatsch, Wentzel, & Fleisch, 2015), influencing the likelihood of triggering either the impulsive or the reflective route of processing risk-related information as the leading system for processing information (Schiebener & Brand, 2015). Furthermore, people tend to decide more reasonably and cautiously if explicit rules and information are given than if they are not given. Intuitive decision-making is associated with more risky behaviors (Brand et al., 2008). Following Bechara (2005), it depends on socialization and internalized social norms whether the reflective system might gain more control over the impulsive system and steer people's behavior or whether the reflective system is inhibited by other mechanisms, allowing the impulsive system to work (Bechara, 2005). Which of the systems is active in a given decision situation can further depend on the power and level of activation of each system (Hofmann, Friese, & Strack, 2009) as well as on the cognitive capacities and involvement of a person (Petty & Cacioppo, 1986). For predicting the level of self-control, Hofmann, Friese, and Strack (2009) suggest considering a person's reflective and impulsive processes as well as situational and dispositional boundary conditions.

Basically, there are two types of conditions in which risk-related decisions can be made, either under ambiguous (i.e., no information about outcomes is present; e.g., Brand, Heinze, Labudda, & Markowitsch, 2008) or under objective conditions (i.e. the outcomes of a decision are clear or calculable; e.g., Schiebener & Brand, 2015). If the possible outcomes of a decision are calculable (e.g., there is a reasoned risk of disclosed personal information being misused), one would argue that people would choose the preferable option (e.g., not disclosing information or restricting the audience) so that the best outcome (i.e., no privacy intrusion) would be ensured. However, situational variables or executive cognitive capabilities of a person, prior experiences, current situational cues, or individual characteristics can influence decision processes (Schiebener & Brand, 2015). Experiences with situations in which decisions have been made and led to

particular outcomes can result in emotional learning (Schiebener & Brand, 2015). Thus, if a person has experienced beneficial outcomes after making a decision, the likelihood that this decision will be made again might increase. With regard to SNSs, Hofmann, Friese, and Strack (2009) revealed that users who had a positive experience in terms of posting something publicly and getting numerous positive responses would also attempt to reactivate positive feelings (i.e., *clusters*, see Hofmann, Friese, & Strack, 2009). These clusters do not require reflective elaboration of a situation and potential consequences in order to function (see Hofmann, Friese, & Strack, 2009). Thus, if a person, for instance, experienced appreciation and social support (e.g., in terms of likes or positive comments) after disclosing personal information to a social online network, he or she will probably do so again. However, if users were informed about potential privacy risks, and if they had cognitive capacities for processing the provided information, they might have decided to disclose less sensitive information to a website or a social network (i.e., more advantageous behavior). Nevertheless, when risks are unknown or the user is not aware of them (e.g., due to situational circumstances), he or she might decide unfavorably with regard to personal privacy. Therefore, this work argues that privacy-intervening measures such as privacy prompts within SNSs might contribute to raising users' awareness of online privacy by triggering the processing of information and making risky situations less ambiguous. Such prompts can either subtly hint to current privacy situations or directly transmit possible risks of particular online actions. Whether users act in a privacy-aware manner or not as a consequence would depend on the style of the provided information itself (see Kaptein, De Ruyter, Markopolulos, & Aarts, 2012), the processing of information, situational cues, and personal characteristics (Kehr, Kowatsch, Wentzel, & Fleisch, 2015, Schiebener & Brand, 2015). In order to provide more information about the term *risk* and its meaning with regard to online privacy protection in the scope of this work, the next chapter outlines the basic properties of risks.

3.2 The Nature of Risks

A risk consists of particular core elements, namely, a loss, the significance of a loss, the uncertainty regarding the occurrence of a loss, and the kind of loss (Yates & Stone, 1992). With regard to online privacy, a risk has been described as the perceived potential of a loss through disclosing personal information (Malhotra et al., 2004). A risky

situation is a state of certain probability of experiencing a loss based on an action (e.g., disclosing sensitive content on an SNS) or a non-action (e.g., not restricting the audience on an SNS; see Furby & Beyth-Marom, 1992; Beyth-Marom & Fischhoff, 1997, p. 111). For most users, it is difficult to assess individual privacy risks and to manage online privacy (Moll, Pieschl, & Bromme, 2014). Furthermore, users have different privacy expectations that create a diverse picture of privacy needs and requirements (Martin & Shilton, 2016). Perceived risks were shown to be related to privacy protection intentions in terms that if users of SNSs perceived privacy risks they had a stronger intention to protect their online privacy (Saeri, Ogilvie, Macchia, Smith, & Louis, 2014). However, reported intentions to protect privacy still are not accompanied by actual privacy protection behavior (Saeri, Ogilvie, Macchia, Smith, & Louis, 2014). In order to diminish risky situations on SNSs by means of system-based interventions, a definition of sensitive information needs to be formulated for the requirement elicitation of a potential privacy support measure that protects the users from privacy risks. Based on the multidimensionality of privacy (see Chapter 2.1), inter-individual differences in privacy needs, personal characteristics, and prior experiences (e.g., Chen, Widjaja, & Yen, 2015) as well as varying individual rules for privacy (e.g., Petronio & Durham, 2008), some people might evaluate certain information (e.g., last name) as highly sensitive whereas other people might not. This is one of the reasons why universal privacy protection measures might not be sufficient – neither all people’s expectations of technical privacy support can be met nor consensual agreement regarding the definition of the sensitiveness of certain information might be given (see Chapter 3.4). In line with this, defining the level of sensitivity of particular information is also challenging for software developers who want to provide privacy-preserving tools (e.g., Xie & Kang 2015). However, this estimation is necessary for evaluating sophisticated methods for privacy protection. Therefore, the next section outlines characteristics of sensitive information.

3.3 The Sensitivity of Information

Perceived information sensitivity is considered as a relevant factor for risk and benefit estimation (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). As already mentioned, following the communication privacy management theory (Petronio & Durham, 2008), people declare information that they think belongs to them as private and consider

particular privacy rules rooted in motivation, contextual cues, and risk–benefit evaluations for managing the distribution of that information. Problematically, the consideration of privacy rules is based on subjective evaluations of a situation (potentially influenced by the third-person effect or optimistic bias; e.g., Cho, Lee, & Chung, 2010; Gunther & Mundy, 1993) and therefore leaves space for disadvantageous decisions resulting in risky behavior and stressing the relevance of objective and adapted support for privacy decisions. Making the sensitivity of information more salient, for instance, via justified privacy recommendations provided by an objective and user-centered system (e.g., through nudging), the likelihood of a corresponding behavioral change can be increased (Acquisti, 2017; see Study 1). Nudging is a method to guide people regarding decisions they have to make (e.g., through triggering behavior) without obliging them (e.g., Fogg, 2009), which will be referred to in more detail in Chapter 8.6.1.

One reasonable indicator for practically identifying sensitive information is to consider information that has been shared online by individuals and regretted afterwards (e.g., Wang et al., 2011). Wang and colleagues (2011) investigated regrettable disclosures of Facebook users and identified certain categories of regrettable information, such as alcohol and illegal drug consumption, sex, religion and politics, profanity and obscenity, personal and family issues, work and company, or topics with a strong sentiment (e.g., negative or offensive comments, arguments, lies and secrets). Furthermore, Debatin, Lovejoy, Horn, and Hughes (2009) found that Internet users who experienced privacy invasion are more likely to adapt their privacy settings than those who have not been affected personally by privacy harms so far. In addition, negative online privacy experiences is related to the privacy risk assessment of a user (Trepte, Dienlin, & Reinecke, 2015), which in turn can lead to a reconsideration of online privacy protection. Furthermore, as was shown in a study by Masur and Scharnow (2016), people perceive personal fears, concerns, feelings, and details from relationships to be very private, whereas favorite music, hobbies, and work are considered to be less private. Information that was perceived as private by participants in that study can be assigned to the psychological rather than to the informational or social dimension of privacy by Burgoon (1982). However, according to a representative report on users' data protection behavior, users evaluate informational privacy-related information such as financial (75%) and medical (74%) information, as well as identity numbers (73%), to be sensitive and

personal (European Commission 2015). In sum, highly personal information such as personal identifying data, regrets, and negative experiences of self-disclosure are quite valid indicators for information sensitivity. Although users are able to report about what they think is sensitive, they might have problems to use the sensitivity of information as indicator for the assessment whether to disclose or not (nonetheless due to the subjective perception of information and the environment). Therefore, external support for estimating sensitivity and communicating privacy risks based on the sensitivity of information occurs as promising approach for maintaining users' online privacy. Thus, in the following, the dependences between decision-making, assessments of risks, and the meaning of sensitive information, which can be considered for risk communication with the goal of increasing users' motivation to protect their privacy, are outlined (Chapter 3.4). Subsequently, self-disclosing activities that are (partly directly, partly indirectly) influenced by perceived sensitivity of information and potential risks of disclosing are addressed as well (Chapter 4).

3.4 A Synthesis of Decision-Making, Risks and Sensitive Information

This work suggests that appropriate communication of privacy risks in a given online situation can prevent users from engaging in behavior that would result in harmful consequences concerning their privacy. Harmful consequences concerning privacy might entail threats to a person's feeling of autonomy, his or her ability to self-evaluate, and the possibility to emotionally release and communicate in a protected space (see Chapter 2.1; Westin, 1967).

Risk communication is a persistent topic in various fields of research. One sector that is highly concerned with communicating risks to people is the health-care sector (e.g., Schapira, Nattinger, & McHorney, 2001). For instance, the World Health Organization informs people about risks with regard to viral diseases, infections, nutrition, violence, impairments, social determinants of health, and many more topics³. An overwhelming percentage of fatalities are caused by diseases that are initiated by risky behaviors such as drinking alcohol, smoking tobacco, or unhealthy eating, resulting, for instance, in high blood pressure, overweight, or cancer (World Health Organization, 2002). Consequently, the World Health Organization requested comprehensive risk communication and

³ See www.who.int/helath-topics (last access: 14th October, 2018)

information that is adapted to subjective concepts of risks (Renner, Panzer, & Oeberst, 2007, p. 253). Some risks cannot be evaluated rationally because they are closely connected to personal values and attitudes (Renner, Panzer, & Oeberst, 2007). This can be the case for medical decisions (affecting people's physical health) as well as for decisions regarding the sensitive and important realm of personal privacy (affecting, e.g., users' autonomy and well-being; see Chapter 2.1). In line with this, the designing of risk-communicating interventions is a very complex process.

Basically, risks can be communicated either by appeals of fear (aiming at changing attitudes and behaviors based on feelings of anxiety) or by providing objective information (through conveying knowledge; see Renner, Panzer, & Oeberst, 2007). The persuasive power of a fear appeal depends on several aspects. For instance, the intensity of a fear appeal influences the subsequent emotional reaction toward the appeal and affects its persuasive power (for a meta-analysis, see Witte & Allen, 2000). In addition, fear-appealing risk communication can initiate more controlled behavior with regard to the source of the risk and acceptance of risk-communicating messages (Witte & Allen, 2000). The authors also outlined that strong fear appeals are especially effective if the message consists of high-efficacy content in contrast to low-efficacy messages transmitting strong fear. However, the effectiveness of risk-communicating messages does not depend only on the transmitted efficacy and strength of fear but also on the availability of alternative recommendations for action (Sutton, 1982). In line with this, one could argue that it might be more beneficial to provide comprehensive information regarding the risk (including the likelihood of occurrence and associated severity) and elaborated recommendations for action. However, too extensive information in risk-communicating messages might induce information overload (e.g., Eppler & Mengis, 2004) or overextend a person's willingness to and capability of making a decision based on the communicated facts (see also Study 1 and Study 3).

Referring to the current work, an adequate solution to initiate cautious online privacy behavior might be to make use of both appeals, namely, by warning (fear appeal) and informing (information appeal) a user who is engaging in risky behavior. Basically, risks are being estimated based on the likelihood of an incident to occur and the severity of that unwanted incidence (Renner, Panzer, & Oeberst, 2007; see Study 4). It has been argued that an objective risk can be assessed through multiplying the likelihood of

occurrence and the severity of that risk (Renner, Panzer, & Oeberst, 2007). Referring to the privacy calculus (Culnan & Armstrong, 1999; see also Chapter 5.2), individually perceived benefits of an action (e.g., disclose personal information) also play a major role in making privacy-related decisions (e.g., Krasnova & Veltri, 2010), which in turn might influence the impact of risk-communicating privacy support measures within SNSs (see Chapter 5.2). This dissertation focuses on the balancing processes between three important factors in terms of online privacy decision-making, namely:

- (a) perceived benefits of disclosing the self
- (b) the likelihood that a negative consequence will occur based on risky self-disclosure
- (c) the severity attached to the negative consequence (see Study 4).

This trade-off between positive and negative consequences of self-disclosing activities refers to the core of the privacy calculus that has been discussed as being challenging to the privacy paradox (see Chapter 5.2). In order to understand the importance of assessing the sensitivity of information and the need for adequate risk communication with regard to these balancing processes, it is necessary to reflect on users' decisions regarding self-disclosure versus withdrawal. By addressing this, the overriding relevance still refers to heeding users' privacy and regard the relevance for individuals to maintain privacy (see Chapter 2.1). In line with this, the next section discusses the counterbalance of users' disclosing actions and their individual (desire for) privacy.

4 Disclosing the Self

The previous chapters outlined the value of privacy and potential risks of disclosing the self online. The most important dimensions and functions of privacy were presented (Chapter 2.1). Additionally, a theoretical basis for understanding decision-making processes was provided and the basic concept of a risk was introduced (Chapter 3.2). Having these two perspectives of self-disclosure in mind, the following chapter will discuss the offset between disclosing the self and maintaining privacy more concretely.

4.1 The Offset between Online Self-Disclosure and Online Privacy

Self-disclosure is a social and communicative process of revealing personal information to others (e.g., Archer, 1980; Petronio, 2002; Taddicken, 2011). People have different motives for disclosing information about the self, for instance, to maintain friendships (e.g., Christofides et al., 2009; Taddicken, 2013), manage one's own image (e.g., Vitak, 2012, 2015), or gain social capital (e.g., Ellison, Gray, Lampe, & Fiore, 2014; Koroleva, Krasnova, Veltri, & Günther, 2011). Social capital can be understood as actual or virtual resources for strengthening the network of relationships (Ellison et al., 2007). Given that self-disclosure diminishes privacy, these motives are related to the individual's privacy. Especially in online contexts, where social cues are not as present as in offline environments and perceived anonymity is higher than in face-to-face situations, people tend to disclose more about themselves and consequently are confronted with a threat to privacy (e.g., Haferkamp & Krämer, 2011; Taddicken, 2011). The depth (level of intimacy) and breadth (amount of disclosures) of self-disclosure can vary depending on different situational and individual cues and circumstances. Disclosures of sensitive information are associated with more pronounced privacy risks (Mothersbaugh et al., 2012; Taddei & Contena, 2013). According to social penetration theory (Altman & Taylor, 1973), there are different layers of self-disclosure, namely, peripheral, intermediate, and core layers. Social penetration describes processes of disclosures and subsequent strengthening of relationships between people (*bonding*, Altman & Taylor, 1973). Peripheral information can be biographical data such as name or birthdate, which is comparable to the data relating to the informational dimension of privacy by Burgoon (1982). Transferred to the context of SNSs, peripheral layers can also be *likes* on rather superficial topics (e.g., favorite music or books; see Carpenter & Greene, 2016). Information relating to the intermediate layers, for instance, attitudes, values, or beliefs regarding specific topics can be considered as more intimate (Altman & Taylor, 1973). In the context of SNSs, such disclosures can cover the expression of political opinions or social attitudes (Carpenter & Greene, 2016). This layer is related to a "light version" of the psychological dimension of privacy, which describes the perceived level of control over emotional and personal in- and outputs (see Burgoon, 1982). Against this background, Dienlin and Trepte (2015) found that people who state they are concerned about their privacy have a negative attitude toward posting emotional and intimate content

on SNSs. The core layer of self-disclosure relates to the most intimate thoughts, fears, desires, and secrets of a person (Altman & Taylor, 1973). This refers to the deeper psychological dimension of privacy by Burgoon (1982). Furthermore, self-disclosures can differ regarding honesty and tonality (Jourad, 1971). Depending on the level of self-disclosure, personal preferences, and attitudes, the understanding, and the perceived sensitivity of information can vary among users (Masur & Scharkow, 2016).

Given that self-disclosure takes place online (e.g., via SNSs or instant messengers) as well as offline (e.g., face-to-face with friends or family), it is interesting to compare the respective circumstances under which people disclose information about themselves to other persons. This makes it possible to extract knowledge regarding disclosure intentions and possibilities to decrease the amount of sensitive disclosures. Trepte, Masur, Scharkow, and Dienlin (2015) shed light on different communication types and the amount of self-disclosure with regard to privacy risks. The authors defined four different communication types, namely, the type *face-to-face*, *friends-only*, *multi-channel*, and *messenger*. The communication type *face-to-face* prefers to communicate in offline environments whereas the communication via social networks and messengers is avoided. Persons representing this type of communication are older than those of the other communication types, they have high privacy concerns, and low privacy literacy (Trepte, Masur, Scharkow, & Dienlin, 2015). By contrast, persons of the *friends-only* type use messengers and SNSs (mainly to communicate with friends instead of family members) and have experienced negative situations online very often in the past. However, they do not report being concerned about their privacy (Trepte, Masur, Scharkow, & Dienlin, 2015). This is especially interesting when considering the assumption that negative experiences have an impact on future privacy behavior (e.g., Christofides, Muise, & Deamarais, 2012). It seems paradoxical that users had negative experiences but do not change their behavior accordingly. It could be argued that users of this communication type ignore the connection between negative experiences and privacy violations or that the perceived gratification of social media usage is more influential than negative experiences (see privacy calculus; e.g., Dienlin & Metzger, 2016). Concerns by of the *multi-channel* type were moderate, but people belonging to this type experienced most negative situations compared with other communication types (Trepte, Masur, Scharkow, & Dienlin, 2015). By contrast, the *messenger* type

experienced the fewest negative situations and had low privacy concerns. Additionally, they have a pronounced need for informational privacy, which may be the reason for them avoiding public network sites for communication (Trepte, Masur, Scharkow, & Dienlin, 2015). Through the reported findings, it becomes clear that privacy needs and concerns differ between people and contexts, which therefore requires a holistic consideration of all social and contextual entities in privacy research. Accordingly, these results also stress the idea of providing adapted real-time privacy support for different types of users, which will be examined in this work.

Further components shaping users' disclosure behavior are their trust in the audience (i.e., horizontal privacy; Bartsch & Dienlin, 2016) receiving information about them (Hofstra, Corten, & van Tubergen, 2016; Masur & Scharkow, 2016) and in the social network on which the information is disclosed (i.e., vertical privacy; Park & Smith, 2007). Trust in its fundamental definition describes a set of learned expectations that two or more persons have toward each other (Barber, 1983). In a study regarding online privacy settings, Hofstra, Corten, and van Tubergen (2016) found that people who limited the access to their profiles had lower trust in their Facebook audience. Furthermore, Saeri, Ogilvie, Macchia, Smith, and Louis (2014) found that Facebook users having positive attitudes with regard to online privacy protection reported having low trust in other users of the network. Thus, trust might be an important variable with regard to perceived and defined privacy boundaries in an online social network as well as with regard to the intention to engage in protection strategies. In some situations, individually defined boundaries (e.g., through audience restriction) can make the users feel safe and confident so that they in turn disclose even more information to their *trusted audience* than to a more unknown audience. However, it is still possible that information can pass these trusted circles, for instance, if a co-owner of information spreads sensitive content that was published by a close friend (see Chapter 2.1).

In contrast to the viewpoint that people reveal more and more information about themselves on the Internet by representing their personality similarly to their real one in offline contexts, there has also been research on increased anonymity in the Internet. For instance, it has been argued that in sensitive discussions (e.g., regarding politics) within online forums or on networking sites, people are more likely to share their own opinions if they perceive a particular level of anonymity so that they cannot be attacked or excluded

by others' opposing opinions (e.g., Chen, Chen, & Yang, 2008). Furthermore, it has been reported that users tend to withhold their opinion on SNSs if they perceive to represent a minority regarding a topic in the network, and there have been studies on how far fear of isolation can influence a user's perception of public opinions (e.g., Neubaum & Krämer, 2017a; Neubaum & Krämer, 2017b). However, the circumstances for either not expressing one's opinion because of the perception of belonging to a minority or disclosing information related to one's self in order to manage one's opinion might differ. Nevertheless, perceived social norms (i.e., strong concepts shaping and determining people's perception of the environment and subsequent behavior; e.g., Ajzen, 1991) and opinion climates (i.e., perceived predominant opinion on a topic) seem to be very strong predictors of users' online behavior. This also raises normative and philosophical questions regarding the intrinsic motivation to express feelings and thoughts. Nevertheless, self-disclosure as it has been introduced can be planned but also happen spontaneously. The severity of spontaneous and unreflected self-disclosure will be reflected on in the following chapter.

4.2 Temptation of Self-Disclosure – Impulses as a Threat to Privacy

Online self-disclosure can be driven by emotional and impulsive behavior or by careful elaborations of situational factors. In the next sections, the challenge for establishing privacy-protective actions under the consideration of people's urge to reveal personal information will be discussed.

4.3 Spontaneous Behavior - A Challenge for Privacy Protection

Impulsive behavior is somewhat detached from planned behavior and its underlying motives and drivers (e.g., attitudes or internalized norms, see Chapter 5.1 and Chapter 6.2). Situations in which information is shared spontaneously are often based on situational cues and less often driven by elaborated attitudes and intentions toward self-disclosure. In contrast to the theory of planned behavior (Ajzen, 1991) and protection motivation theory (Rogers, 1975), there are also approaches that focus on more situational behavior (e.g., Masur, 2018).

Individuals in emotional or stressful situations tend to use mental shortcuts for making a decision (see *impulsive system*, Chapter 3.1), rather than elaborating on

advantages and disadvantages as it is more likely in the case for planned behavior (see Chapters 3.1 and 5.2). With reference to SNSs, specific cues might trigger impulsive self-disclosing behaviors that might be regrettable afterwards (see also Wang et al., 2011). Consequently, even if users had privacy literacy for instance, or already experienced negative outcomes due to thoughtless self-disclosures, this might not hinder them from behaving risky as a response to tempting cues owing the restricted capacity to elaborate. Attitudes and intentions regarding a topic or an object, which usually are valid predictors of behavior (if they are easily accessible; see Ajzen, 1991; Fazio, 2007), might be overridden by impulsive responses to particular cues or demands (e.g., the anticipation of appreciation due to a self-related posting). Also, if attitudes and intentions are either not strongly related to the topic or not accessible in spontaneous situations, their predictive power lacks accuracy.

Impulsive people tend to have difficulties inhibiting their behavior (Logan, Schachar, & Tannock, 1997). In line with this, people showing impulsive behaviors might have more trouble to behave according to privacy rules and privacy literacy (if present), because they might not perceive the need to consider privacy rules in spontaneous, emotional or stressful situations. Therefore, impulsive behavior constitutes a threat to users' online privacy, which can be addressed by implementing real-time privacy support that interrupts impulsive situations and triggers more elaborated evaluation of current privacy risks. Although, online behavior on SNSs can be planned and intentional (e.g., if a person wants to create and maintain a specific impression), there are situations in which users behave spontaneously as well (e.g., disclosing in an intense mood). Impulsivity is a state in which a person is not capable of thinking about long-term goals or planned actions but is instead directed by immediate triggers and impulses (Hofmann, Friese, & Strack, 2009), mostly resulting in automatic processes without following a behavioral intention (Bargh, 1997). Whether people can or cannot resist temptations depends, among others, on their behavioral self-control (see Hofmann, Friese, & Strack, 2009; see Chapter 6.2.6). Thus, the occurrence of spontaneous behavior depends on the concurring constructs of self-control relating to conscious intended processes (see Förster & Denzler, 2006; Hofmann, Friese, & Strack, 2009; Baumeister, Heatheron, & Tice, 1994) and impulses (Hofmann, Friese, & Strack, 2009). The fact that impulses can release behavior is also referred to in persuasive research, which proposes the usage of triggers at a specific time

point in order to induce (intended) behavioral changes (along with motivation and ability; see Fogg, 2003, 2009).

In accordance with Baumeister and Heatherton (1994), Hofmann, Friese, and Strack (2009) define an impulse as a specific arousal combining general motivations with a certain stimulus in the direct environment, which is associated with an anticipated satisfaction of needs. Transferred to social media, an impulse might arise with the motivation to be socially connected to other people together with a particular stimulus such as a specific posting on Facebook that releases strong emotions such as joy or anger (e.g., a highly controversial posting), associated with the anticipation of counter-arguing and therefore experiencing emotional release (similar to an incentive). Strikingly, concomitant gratification would be short-termed and detached from concerns and long-term behavioral goals. Transferred to risky self-disclosing behavior on SNSs, privacy concerns and long-term goals such as behaving in a privacy-aware way and rationally evaluating the risks and benefits of information disclosure (privacy calculus) are likely to be faded out if users acted spontaneously (driven by impulses and triggers and guided through the impulsive system, see Chapter 3.1; Schiebener & Brand, 2015). In fact, SNSs intentionally trigger disclosing and sharing behaviors of users (e.g., Treem & Leonardi, 2013; Vitak & Kim, 2014) which makes self-control a relevant factor for privacy-aware online behavior (see also *self-control*, Chapter 6.2.6). People lacking of self-control or abilities to identify a tempting situation and its risks require external support. Self-controlled actions require much energy and willpower (Förster & Denzler, 2006; Baumeister & Heatherton, 1994), thus, even people who tend to control their actions in general, might be exhausted if they would need to control themselves in every single situation. With regard to controlling for privacy, system-based support measures can attempt to control situations while users still act autonomously by deciding whether to accept a privacy supporting recommendation proposed by a system or not.

This chapter summarized that spontaneous privacy behavior is a challenge to privacy, and not easily predictable. Nevertheless, self-disclosure on SNSs can still happen in a planned manner. Many researchers addressed users' (planned) privacy behavior by drawing on approaches and theories that are able to predict and explain behavior. The following chapter gives an overview of approaches explaining and predicting planned privacy behavior (Chapters 5.1, 5.2, and 5.3). Further, Chapter 5 introduces an approach,

which describes behavior as a response to an external cue, which cannot be described as fully planned, but also not as fully spontaneous (Chapter 5.4). Reflecting on these approaches is relevant for the present thesis because learning about the factors that influence privacy behavior can help to derive valuable insights with regard to how behavior can be changed.

5 Planned Privacy Behavior

In order to understand and explain users' apparent contradictory online privacy behavior, it is essential to consider the behavioral determinants that can predict human behavior (e.g., behavioral intentions and attitudes). Recently, behavioral predictors with respect to the theory of planned behavior (Ajzen, 1991) have been examined in online privacy research (e.g., Dienlin & Trepte, 2015, Ho, Lwin, Yee, & Lee, 2017; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014). The background to this is that although most users are concerned about privacy risks (European Commission 2015; Osatuyi 2015; Taddicken 2014; Vitak 2015), many of them do not put their concerns into protective practice, for instance, because of a lack of behavioral intentions (Dienlin & Trepte 2015). In 2016, almost 44% of American, 30% of German, 53% of British, 39% of Dutch, and 57% of Chinese users did not even know whether their online profile is searchable on search engines or not (Trepte & Masur, 2016). By contrast, the willingness to have an open profile for sharing information and photos with everyone in the network is very low (Trepte & Masur, 2016). What was once defined as the *privacy paradox* (Barnes, 2006; Trepte & Teutsch, 2016) addresses this main problem; although people (claim to) know that divulging private information online might entail manifold negative consequences that they are afraid of, they do not engage in privacy protection activities. Conversely, they disclose largely unfiltered sensitive information to their online audience (Acquisti & Gross 2006; Barnes 2006; boyd & Hargittai 2010; Hughes-Roberts, 2013; Lee et al., 2013; Madden, 2012; Tufekci, 2008). Recently, more and more scholars have tried to solve the privacy paradox by providing explanations for seemingly contradicting behavioral patterns of users. The most prominent and convincing approaches will be outlined in the following.

5.1 Explaining the Privacy Paradox

In 2013, 50% of interviewed people in the United States reported having concerns regarding their privacy, compared with 33% in 2009 (Rainie et al., 2013⁴). Although privacy concerns seemed to be widespread back in 2013, users reported publishing personal photos (66%), their birthdate (50%), email address (46%), home address (30%), or even their private phone number (21%) and political affiliation (20%) online. Furthermore, 21% of consulted participants reported that they had already experienced some kind of data misuse (e.g., their social networking account was compromised or used by another person without authorization) and 12% had been victims of stalking or harassment (Rainie et al., 2013⁴). More recently, statistics reveal even more pronounced privacy concerns. In 2014, for instance, Trepte and colleagues reported that 82% of people in Germany did not want their personal data to be accessible for the public (rooted in privacy concerns). Nevertheless, an increase of disclosed data was recorded at the same time (Trepte et al., 2014). In 2016, 57% of German people reported to be worried about providers of websites storing their data and 46% were anxious about other people reading private online messages without permission (Braun & Trepte, 2016). Furthermore, 76% of the individuals asked did not like the idea of providing personal data in exchange for using specific offers “for free”, and 57% said that it should not be allowed to invade people’s privacy in order to gain profit for society (Braun & Trepte, 2016). Consequently, reported concerns and attitudes regarding online privacy seemingly contradict the actual privacy behavior of Internet users (e.g., Barnes, 2006; Hughes-Roberts, 2013; Lee et al., 2013; Reynoldes et al., 2011; Taddicken, 2014; Trepte & Reinecke, 2011; Tufekci, 2014).

However, the privacy paradox has also been challenged by scholars who did not find support for its existence in their studies (e.g., Blank et al., 2014; Christofides et al., 2009; Young and Quan-Haase, 2013). Based on an inconsistency in research regarding the privacy paradox, scholars tried to explain or solve the apparent paradox by applying different theories and methods of investigation (e.g., Dienlin & Trepte; 2015; Trepte, Dienlin & Reinecke, 2014; Trepte & Teutsch, 2016). For instance, Trepte, Dienlin, and Reinecke (2014) argued that the evident mismatch between privacy attitudes and privacy behavior might not be as strong as expected, because attitudes and behaviors differ

⁴ See <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/> (last access: 4th November, 2018)

regarding various dimensions of privacy behavior and privacy attitudes (see Burgoon, 1982).

In 2016, Trepte and Teutsch addressed the privacy paradox with three different hypotheses, namely the *gratification hypothesis*, the *knowledge hypothesis* and the *social desirability hypothesis*.

The *gratification hypothesis* claims that people strive after social support and optimized self-presentation, which can be gathered by disclosing information about the self so that other people can react to it and support the person (Trepte & Teutsch, 2016). In addition, people strive to increase their social capital through self-disclosing on SNSs, which is perceived to be beneficial by most people as well (Ellison et al., 2014). Against this background, people seem to give stronger weightings to anticipated gratifications than to the protection of their individual privacy (Trepte & Teutsch, 2016). Thereby, users might not always be objective and tend to consider heuristics (i.e. mental shortcuts for processing the environment without experiencing an information overload) to assess the risks and benefits of a situation (Trepte & Teutsch, 2016). In sum, the gratification hypothesis states that users behave paradoxically because their desire for social support along with experiencing gratification is perceived as being more relevant than potential privacy risks, or that privacy risks are suppressed in order to receive social support. This gratification hypothesis shows parallels with the privacy calculus approach in the sense that users weigh gratifications against potential risks and decide to disclose or withdraw information depending on anticipated benefits and risks (Culan & Armstrong, 1999; Krasnova & Veltri, 2010). If risks are less prominent to the user, he or she will more likely disclose information than if risks were more present (Culan & Armstrong, 1999; Krasnova & Veltri, 2010). However, the privacy calculus assumes that people are rational and objective in their evaluation of risks and benefits (which has been criticized as well, e.g., Acquisti, 2004), whereas the gratification hypothesis assumes the users to be subjectively driven by heuristics (Trepte & Teutsch, 2016).

The second hypothesis for explaining the privacy paradox is the *knowledge hypothesis* (Trepte & Teutsch, 2016). This hypothesis states that people do not have sufficient literacy regarding privacy policies, measures, and protection strategies so that it is not possible for them to engage in protection measures (Trepte & Teutsch, 2016). One way to overcome this issue is to educate users of social media applications regarding

features and strategies to protect privacy and consequently increase their privacy competence and literacy (Bartsch & Dienlin 2016; Egelman et al. 2016). Competence in general is considered as knowledge, ability, and proficiency combined with motivational preconditions to perform behaviors or actions in a self-regulated way and adequately in a given context with given preconditions (Six & Gimmler, 2007). Online privacy literacy, as defined by Trepte and colleagues (2015), is a combination of two different kinds of knowledge: declarative (i.e. knowing measures and settings for protection) and procedural knowledge (i.e. knowing how to implement these measures). Hence, privacy literacy comprises knowledge regarding data protection, technical aspects, protection strategies, legal conditions, and how to consider these aspects for privacy protection (Trepte et al., 2015). Park (2013) defined privacy literacy as a principle to empower individuals to undertake informed control of their online personas. Egelman and colleagues (2016) developed a *Teaching Privacy Curriculum* providing information for teachers on how to inform users about privacy issues and what to inform them about. Thereby, they referred to ten principles of online privacy; on the Internet:

- (1) Everyone leaves digital footprints.
- (2) There is no anonymity.
- (3) Every information is utilizable.
- (4) Every information is readable by everyone.
- (5) Usage of personal information by other parties is not controllable.
- (6) Search algorithms are a threat to privacy.
- (7) Online activities are a crucial part of life.
- (8) You never know with whom you communicate.
- (9) No or less Internet usage is no guarantee of privacy.
- (10) Online privacy is one's own responsibility.

Privacy literacy is an important factor when assessing whether to share information or not, whom to trust, and which protective measures to use. Users who do not have valid privacy literacy are less able to protect their online identity, which might be one reason why people with high privacy literacy feel safer than do people with low literacy (Bartsch & Dienlin, 2016). To be more precise, Bartsch and Dienlin (2016) found that users who state they possess high privacy literacy also tend to protect their online identity more strongly through restricting the access to their profiles on an SNS. Changing

the privacy settings very often has been identified as one indicator of having higher levels of privacy literacy (Bartsch & Dienlin, 2016). However, even if users are literate and configure their privacy settings, disclosed information can still leak through other parts of the network.

The *social desirability hypothesis* assumes that people (claim to) care about their privacy (although they might actually be less concerned) because they perceive a social consensus regarding the importance of privacy protection (Trepte & Teutsch, 2016). Media reports and the spread of people's opinions can strengthen this perception, especially because most reports stress privacy threats and invasions (in 2016, 90% of privacy reports in German media referred to informational privacy, whereas only 30% referred to physical privacy and 10% each to social and psychological privacy; see Braun & Trepte, 2016). Therefore, it has become a social norm to be alarmed about privacy and to express a similar opinion. Against this background, self-reports regarding privacy must be considered very carefully taking into account possible influences of perceived social norms. Since perceived social norms and personal attitudes have a strong influence on people's (reported) planned behavior (Ajzen, 1991), this influences the way users respond when being asked about privacy behavior and attitudes. Social norms can be injunctive (perception of what the others think one should do), descriptive (perception of what others actually do), or personal (internalized rules and values with regard to behavior; Cialdini, Reno, & Kallgren, 1990).

Summing up, the suggested hypotheses provide possible explanations for users' insecure privacy behavior. In fact, this would not support the assumption that the privacy paradox does not exist, but rather clarifies the reasons for the existence of the paradox. In the light of this work, these findings illustrate once more that supportive privacy measures working in real-time can be regarded as a valuable opportunity to protect users' online privacy by calling for their attention even if they are striving for gratification, have little privacy-related knowledge, or want to be appreciated by others. Nevertheless, there are further frameworks and theories challenging the privacy paradox, for instance, the privacy calculus, which will be referred to in the next section.

5.2 Boon for Privacy or Bane to Self-Presentation? The Privacy Calculus

According to the privacy calculus (Culnan & Armstrong, 1999; based on Laufer & Wolfe, 1977), people evaluate risks and benefits associated with the disclosure of private information about the self to others (Dienlin & Metzger, 2016; Krasnova & Veltri, 2010; Trepte, Reinecke, Ellison, Quiring, Yao, & Ziegele, 2017). Based on this evaluation, users of online SNSs decide either to disclose or not disclose information to their network (e.g., Dienlin & Metzger, 2016). A study on cultural differences between German and US American users regarding the determinants for this evaluation showed that German users are more afraid of privacy threats and evaluate privacy risks more seriously than do American users (Krasnova & Veltri, 2010). Interestingly, American users appeared to be concerned, too, but for them the gratifications of self-disclosure outweighed potential risks (Krasnova & Veltri, 2010). Benefits of information disclosure on SNSs comprise enjoyment, self-presentation, and maintaining relationships, whereas perceived risks comprise privacy concerns with regard to anticipated damages and the likelihood of the occurrence of a privacy threat (Krasnova & Veltri, 2010).

The decision to disclose or not to disclose can be understood as rational assessment (Culnan & Armstrong, 1999). Oftentimes, the gratification of disclosing private information is more present for users than the perceived damages and disadvantages of information disclosure (as is also claimed by the gratification hypothesis; see Trepte & Teutsch, 2016). Benefits and gratifications of self-disclosure are usually directly perceivable (e.g., social feedback, recognition) whereas risks and privacy violations are often delayed (e.g., job loss, cyber-mobbing, exclusion from social groups). Following the privacy calculus, private information is considered as a tradable asset or product (Culnan & Armstrong, 1999). Although the privacy calculus assumption is reasonable, it is difficult for human beings to evaluate costs and benefits objectively owing to their individual subjective perceptions of their environment. Usually, people are not able to completely rationally assess situations (Acquisti, 2004). Even if people tend to act rationally in general, they can be confronted with emotional, stressful, or unexpected situations in which resources for rational and objective evaluation of risks and benefits are not available. In addition, information and situations that have to be processed can be incomplete or false and cognitive capacities vary between people and situations (Acquisti, 2004; Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Consequently, it can be reasonably

assumed, that the individual evaluation of risks and benefits of sensitive information disclosure takes place in aware situations but that the evaluation either does not happen at all or it is solely based on peripheral cues or heuristics in unaware situations. Moreover, Facebook and other social media platforms allow for convenient experiencing of gratifications so that potential concerns can be outperformed by perceived benefits of self-disclosure (Debatin, Lovejoy, Horn, & Hughes, 2009). However, there are also contradicting findings, revealing that people prefer online privacy instead of convenience (e.g., O’Neil, 2001). Nevertheless, a measure for interrupting unaware states, allowing for a more conscious evaluation of the situation, could help users of SNSs to make deliberated privacy decisions and to decrease the likelihood of occurrence of threats.

Besides the fact that users differ with regard to thinking styles and need for cognition (i.e., influencing factors for risk–benefit evaluation), and therefore approach distinct processes of risk assessment (i.e. a challenge to the privacy calculus; Kehr, Kowatsch, Wentzel, & Fleisch, 2015), online self-disclosure does not always allow for careful evaluation beforehand. To be more precise, disclosures in fact can happen spontaneously, based on impulses or triggered by emotions, which does not allow for careful consideration of anticipated threats and gratifications. The impulsive characteristic of self-disclosure was referred to in the Chapters 4.2 and 4.3. in contrast to that, a theory that often is used to explain users’ privacy behavior – the theory of planned behavior – will be outlined by highlighting advantages of using this theory and challenges of considering online privacy behavior as being planned.

5.3 Online Privacy Behavior in the Light of the Theory of Planned Behavior

According to the theory of planned behavior (TPB; Ajzen, 1991), people’s attitudes, subjective norms, perceived behavioral control, and intentions are valid indicators for predicting and understanding planned behavior. Understanding a user’s online behavior can help to foresee and reduce potential privacy risks and consequently provide privacy support. Furthermore, the strength of a person’s intention to perform an action gives a reference to the likelihood that this behavior will be performed (Ajzen, 1991; Baker & White 2010). That is, if attitudes toward an action or an object are very specific, they can be understood as an indicator of actual behavior (Davidson & Jaccard, 1979), whereas unspecific and vague attitudes are less reliable predictors of behavior (Davidson &

Jaccard, 1979). Therefore, it is extremely important to ask users of SNSs very specifically about their privacy attitudes and corresponding intentions if one is aiming at deriving or predicting actual privacy behavior.

Since anticipating or performing behaviors can also bring uncertainty, an individual's perceived control over an action is another pivotal factor that influences the likelihood of the occurrence of a respective action (Ajzen, 1991). If an individual perceives that he or she is not able to handle a situation, the likelihood of performing an action may decrease. Thus, perceived control is an influencing situational determinant that must be strengthened when aiming at a behavioral change such as modifying users' online privacy behavior. However, the prediction of behavior becomes less accurate when people's reported behavioral control is not reliable. According to Ajzen (1991), this can happen if the person has too little information regarding a situation or required behavior, preconditions have changed, or the situation is totally new. Additionally, even though a situation might not be completely unfamiliar (e.g., sharing information in SNSs), the perceived control can be grounded on a biased perception (e.g., Baek, Kim, & Bae, 2014). More precisely, a person might believe to know about situational requirements (e.g., interaction rules on SNSs, impacts of online self-disclosure) and based on this assumption develop and maintain false perceptions (e.g., "I'm not endangered"). The TPB would predict that there can be no engagement in privacy protective behavior when users do perceive a lack of control or when they forget about it in impulsive situations (see Finneran & Zhang 2005; Kahneman 2011). Consequently, users' behavioral intentions would not be sufficiently pronounced, even if they would like to protect their privacy (according to their attitudes). If a person has a false perception of individual privacy control, intentions to remain secure in terms of sharing less (sensitive) content or restricting the profile might fade into the background.

Furthermore, perceived subjective norms regarding a topic, a behavior, or an object also shape a person's behavior (Ajzen, 1991). Thereby, it is of great relevance whether a person perceives themselves to be judged by others, especially if he or she performs controversial behavior. In sum, people's attitudes, perceived subjective norms, and perceived behavioral control affect their behavioral intention to perform an action, which can then be considered for making a prediction about the actual behavior (see Ajzen, 1991; Rise, Sheeran, & Hukkelberg, 2012).

In conclusion, the theory of planned behavior (Ajzen, 1991) can be considered when investigating general privacy behavior and long-term privacy decisions, as was done by Dienlin and Trepte (2015). However, many privacy-related actions happen based on short-term decisions or on spontaneous and emotional situations. In such cases, it is still reasonable to consider users' intentions, perceived control, social norms (which probably even differ between communication circles), and attitudes to estimate the direction of a privacy decision but there are different cognitive processes involved as well. Strikingly, these processes can significantly differ from self-reported privacy intentions and attitudes. This is why it is important to focus on real-time privacy behavior of users in natural settings as well as on spontaneous situations.

5.4 Privacy Protection Motivation

Originally, the protection motivation theory (PMT) was used to explain people's motivation to engage in (preventative) healthy behavior (Rogers, 1975, 1983). This theory explains a person's protection motivation based on three different elements of information processing and respective cognitive processes:

- (a) The source of information.
- (b) The cognitive mediating process.
- (c) The coping mode (Rogers, 1975; Floyd, Prentice-Dunn, & Rogers, 2000).

The source of information is crucial for an evolving protection motivation. On the one hand, there are environmental sources including persuasive communication and observational learning, which accompany a proposed action. In the scope of this work, it will be focused on persuasive risk communication by means of system-based interventions (i.e. hinting messages and visual triggers indicating the current level of risk). In addition to that, intrapersonal sources such as personal characteristics, prior experiences (negative or positive), intentions, perceived norms and attitudes toward a protective behavior are playing a vital role (Rogers, 1975; Floyd, Prentice-Dunn, & Rogers, 2000). The sources of information can lead to a threat evaluation of respective risks (evaluation of maladaptive responses) or to coping evaluation mechanisms (evaluation of adaptive responses) of that risk. Within the present thesis, the personal characteristics of users and the relations between these traits and users' privacy protective

behavior after having communicated current privacy risks are examined (see Studies 3 & 4). The risk evaluation then results in the actual protection motivation, which can be maladaptive or adaptive coping. For adaptive coping, the person's self-efficacy and response efficacy are of high relevance. The process of evaluating communicated threats starts with the mal-adaptive coping process, which comprises of assessing anticipated rewards, as well as severity and vulnerability of consequences of unprotected behavior (Rogers, 1975). Depending on the outcome of this coping process (and the outcome of the coping appraisal process), the motivation to engage in protective behaviors will be affected positively or negatively. While the threat appraisal process is decisive for the perceived severity of a threat and the perceived need to counteract this threat, the coping-appraisal is important for the individual perceived ability and capacity of dealing with the threat (*perceived control*; see Ajzen, 1991). In sum, the protection motivation theory (Rogers, 1975) is a good approach for analyzing persuasive risk communication, focusing on the cognitive evaluation processes that induce protection motivation and behavioral changes.

Since the protection motivation theory (Rogers, 1975) is considered in this work to learn about privacy protection motivation and to derive how privacy risks should be communicated to users of SNSs in order to increase protection motivation, the ethical boundaries and users' reactions to fear-arousing risk communication (e.g., reactance; see also Ketelaar & van Balen, 2018) need to be addressed as well. In fact, some scholars already investigated privacy and security behavior against the background of the protection motivation theory (e.g., Chen, Beaudoin, & Hong, 2016; Lee, LaRose, & Rifon, 2008; O'Connell & Kirwan, 2014; Woon, Tan, & Low, 2005).

According to Rogers (1975, 1983), fear-arousing risk communication has an impact on protection motivation. More drastically, he claims that the level of fear that is evoked by a risk-communicating external source shows a linear relation to the likelihood that the adaptive response follows as protective behavior (Rogers, 1975). Also, current studies offer insights into the role of concerns and perceived risks for privacy protection behaviors. For example, Dienlin and Metzger (2016) showed that privacy concerns are related to protective behaviors of users of SNSs. Protective behaviors can, for instance, be self-withdrawal or self-censorship on Facebook. Thus, communicating privacy risks

(addressing privacy concerns) should be considered as a supportive approach for increasing privacy protection motivation and subsequent privacy behavior.

Following PMT, subjective appraisals are more relevant for engagement in (privacy) protection behavior than are objective threats (Rogers, 1983; Dienlin & Metzger, 2016), indicating that the perceived severity of a risk is pivotal for protective behavior. Since perceived privacy risks and their severity can influence the extent of users' privacy concerns (Xu et al., 2013), which in turn influence users' privacy behavior (Dienlin & Trepte, 2015), risk communication is pivotal for inducing privacy-related behavioral changes. Privacy risks in general have been defined as "the expectation of losses associated with the release of personal information" (Xu, Luo, Carroll, & Rosson, 2011, p. 46, in Dienlin & Metzger, 2016). This basic definition is helpful for discussing online privacy behavior although privacy risks and their severity are subjective concepts and need to be defined for every individual separately. Perceived privacy risks are related to users' privacy concerns (see Chapter 5.3.3). Hong and Thong (2013) define privacy concerns as the extent of being worried about misuse of personal data by Internet providers. However, in the present work, privacy concerns do not cover solely concerns regarding website providers misusing personal information that might affect users' informational (Burgoon, 1982), or vertical privacy (Bartsch & Dienlin, 2016), and privacy of personal data and personal communication (Clarke, 2006), related to peripheral layers of self-disclosure (Altman & Taylor, 1973), but also those concerns resulting from sensitive self-disclosure regarding the inner layers (Altman & Taylor, 1973) such as mobbing, exclusion from groups, or receiving negative feedback, affecting psychological and partly social privacy (Burgoon, 1982) as well as the privacy of personal behavior as it was termed by Clarke (2006).

5.5 Increasing Users' Protection Motivation

Following Ryan and Deci (2000), human motivation covers an individual's activation and behavioral intention, depending on contextual cues and personal characteristics, experiences, and the source of motivation. People can be motivated internally or externally (or *amotivated*, Ryan & Deci, 2000), which later on has an influence on behavioral outcomes and well-being, especially with regard to long-term behavioral changes. Intrinsic motivation is defined as "the inherent tendency to seek out novelty and

challenges, to extend and exercise one's capacities, to explore, and to learn" (Ryan & Deci, 2000, p. 70). Users of social media can also be externally motivated to either disclose (e.g., by SNS providers) or withhold information (e.g., from data protectionists) by employing gamification (Deterding, 2011; Fogg, 2009). Typically, behavioral changes are more stable when they are based on intrinsic motivation because people who are intrinsically motivated are more likely to be excited and confident about respective behavior (Ryan & Deci, 2000) than are people who are motivated solely based on external cues. This indicates that an anticipated behavioral change regarding the privacy behavior of users might require additional supporting elements for increasing users' perceived control and self-confidence.

Cognitive evaluation theory deals with human intrinsic motivation referring to different social cues, environmental factors, and human needs for competence and autonomy (Ryan & Deci, 2000). This theory is a part of self-determination theory (SDT) by Ryan and Deci, proposing that feedback that supports users' feelings of competence and autonomy can increase their intrinsic motivation to engage in a particular behavior (Deci & Ryan, 2000). Furthermore, Deci and Ryan (2000, p. 70) state that "optimal challenges, effectance-promoting feedback, and freedom from demeaning evaluations were all found to facilitate intrinsic motivation."

If privacy-supporting measures were to be designed alongside these requirements, the likelihood that this privacy feedback would induce a behavioral change would probably increase. Therefore, risks should be communicated in a clear, supportive, persuasive, and target-oriented way. Most importantly, the users' need for autonomy and their self-confidence have to be maintained so that they attribute positive feedback not only to an external supportive tool but also to themselves (see also *locus of causality*; Deci & Ryan, 2000). More precisely, privacy risk communication in terms of feedback for inducing behavioral changes should not solely consist of threats, pressure, or unrelated rewards, but instead consider the users themselves and strengthen their autonomy. Against this background, it seems promising to infer the most likely privacy risks for users of SNSs and provide them with risk-related information in order to help them maintain their online privacy. The impact of communicating privacy-risk-related information to users is empirically tested in this dissertation.

However, the extent to which a risk-communicating support measure can help users to increase their privacy behavior also depends on the person him/herself. It can be assumed that users with specific characteristics (e.g., those with a high need for privacy and a low need for popularity) perceive privacy protection to be important and might be more sensitive toward privacy support measures than who evaluate self-presentation as being more valuable than privacy protection (e.g., those with a lower need for privacy and higher need for popularity). Therefore, Chapter 6 will outline relevant personal manifestations and traits of people that were repeatedly shown to be related to online disclosure behavior as well as to privacy protection intention.

6 The Impact of Personal Characteristics on Online Privacy Behavior

In the following, the influence of people's personal traits and further intrapersonal factors on their privacy behavior is addressed. The focus lies on those characteristics, which already have been revealed to be related to general privacy behavior or to decision-making processes.

6.1 The Impact of Users' Personality on Online Privacy Behavior

This work argues that persuasive strategies can enhance the effectiveness of system-based privacy support interventions such as warning messages, prompts or other visual cues (see Chapter 8.6.1). Since the early investigations of persuasion (e.g., Hovland, Janis, & Kelley, 1953; Petty & Cacioppo, 1986), this method has been discussed in many disciplines with regard to various advantages, disadvantages, and concerning the factors influencing the impact of persuasion (e.g., people's personality traits). As early as 1992, Haugtvedt and Petty stated that the processes of persuasion depend not only on the characteristics of a persuasive message itself but also on people's personality traits. Moreover, people's individual characteristics also influence their disclosure behavior as well as privacy protection intentions on SNSs (e.g., Ahn, Kwolek, & Bowman, 2015; Christofides, Muise, & Desmarais, 2009; Hofstra, Corten, & van Tubergen, 2016; Utz & Krämer, 2009; Utz, Tanis, & Vermeulen, 2012). In line with this, the current work argues

that users' personal traits and characteristics can influence the impact of persuasive privacy support interventions.

Users who disclose much personal information tend to have many online friends and use sparse protective settings (Heirman et al., 2016). In a longitudinal study, Trepte, Dienlin, and Reinecke (2014) investigated users' privacy risk assessment, as well as informational, social, and psychological privacy behaviors based on prior negative experiences. It was revealed that people who had already negative experiences assessed their personal privacy risk to be higher than those who did not (Trepte, Dienlin, & Reinecke, 2014). People who assessed their individual privacy risk as being high engaged in more intense protection behavior regarding informational data than did users who perceived themselves to have low privacy risks, but strikingly not regarding their social and psychological privacy (Trepte, Dienlin, & Reinecke, 2014). Basically, personal experiences are an important factor for developing or modifying attitudes toward objects, persons, or behaviors, which in turn have an impact on actual behaviors (Tormala, Petty, & Brinol, 2002). Especially, if experiences are associated to negative emotions they can be highly influential (see Rogers, 1975). Therefore, it would be reasonable if negative experiences of privacy violations would trigger comprehensive privacy protection. However, on the basis of the results of their study, Trepte, Dienlin, and Reinecke (2014) concluded that users might perceive the protection of their informational privacy (e.g., through providing fewer identifying data) as being sufficient for avoiding negative experiences in the future. This could, among others, be based on the privacy-related media coverage that mostly concentrates on threats with regard to informational privacy (see Braun & Trepte, 2016), and the resulting perceptions of (injunctive) social norms regarding data protection (see also TPB; Ajzen, 1991). The impact of perceived social norms on users' online behavior becomes even more relevant when considering that perceived prevalent norms differ with regard to current communication circles and are influenced by an immense number of different people who are participating in various discussions concerning heterogeneous topics. According to Trepte, Dienlin, and Reinecke (2014), users might perceive a satisfying and sufficient increase of privacy through limiting the access to identifying data such as full name or birthdate. Through solely limiting the access to data relating to informational privacy, but still providing information related to the dimensions of social and psychological privacy, users are still

able to gather gratifications (Trepte, Dienlin, & Reinecke, 2014) on the one hand, but enjoy a feeling of safety on the other hand. As already outlined in Chapter 5.3, users' behavioral attitudes, intentions, and perceived social norms are useful indicators for explaining long-term privacy behavior (when examined according to the TPB; e.g., Dienlin & Trepte, 2015). Although, this work primarily focuses on situational effects of privacy support measures, it seems advantageous to examine users' privacy norms, attitudes, intentions, and manifestations of personality in order to learn about their general privacy behavior (e.g., Study 1 and Study 2), potential influences of intentions and prevalent norms on the impact on situational privacy support, as well as moderating roles of personality concerning privacy support measures and subsequent behavior (see Study 2 and 3). Therefore, influencing manifestations of personality will be referred to in the following section (relevant for both, long- and short-term behavior). Moreover, this work argues that it can be beneficial to consider personal characteristics of users for elicitation of requirements toward technical privacy protection measures (see Study 1). Referring to the characteristics of potential users of *systems-to-be* is also a common procedure for developing software for particular user groups (e.g., An, Kwak, & Jansen 2017; Meis & Heisel, 2017). The following sections summarize the most important influencing personal factors of privacy behavior for this work.

6.2 Individual Characteristics as Influencing Factors for Privacy Behavior

Given that users of SNSs upload content, write comments, or click the *share* and *like* buttons, they leave their personal footprints on the Internet, expressing parts of their (managed) personality (Fullwood, Nicholls & Makichi, 2015; Vitak, 2015). Furthermore, personality characteristics can influence users' behavior and, therefore, their online (privacy) behavior might be influenced by these characteristics as well (Chen, Widjaja, & Yen, 2015). Kehr, Kowatsch, Wentzel, and Fleisch (2015) concluded in their study regarding the evaluation of risks and benefits of online self-disclosure grounded in individual thinking styles (i.e. high vs. low need for cognition), that besides personality factors being indicators of privacy-related perceptions, cognitive evaluations of privacy-related information differ based on individual traits and processing styles. Moreover, in a study with 354 Asian Facebook users by Chen, Widjaja, and Yen (2015), users' openness

to new experiences was found to be a negative moderator in the relation between their need for popularity and self-disclosure.

In line with this, an increasing number of scholars suggest considering individual characteristics of users for developing recommender systems or privacy support measures taking inter-individual differences of users into account (e.g., Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Aside from sociodemographic variables like users' gender, this dissertation considers users' need for privacy and popularity, their expression of narcissism and individual impression management motivations, as well as their need for cognition as influencing variables shaping their privacy behavior. All these variables will be referred to in the following sections.

6.2.1 Need for Privacy

Basically, every person has a need for privacy (see Chapter 2.1; DewCew, 1997; Halmos, 1953; Westin, 1967). However, this need for privacy can differ with regard to contextual cues and among individuals. Following Westin (1967) and Altman (1975), Margulis (2011, p. 15) describes the need for privacy as the “continuing dynamic of changing internal and external conditions, to which we respond by regulating privacy in order to achieve a desired level of privacy”. The strength of this need might differ between individuals depending on personal characteristics and situational privacy states (see Dienlin, 2014). The need for privacy can be divided into informational, interactional, and physical need for privacy (Trepte & Masur, 2017). When investigating the need for privacy, Buss (2001) considers people's self-disclosure as well as their need for concealment and personal space. In a quantitative study with 550 participants, Blanchio, Przepiorka, Boruch, and Balakier (2016) investigated users' need for privacy in relation to Facebook usage. They found that the need for privacy was a negative predictor of users' Facebook usage (whereas loneliness and self-promoting motives were found to be positive predictors). In that study, the need for privacy was measured by means of a privacy questionnaire by Jêdruszczak (2005) including items such as “sometimes I need to get away from others and be alone” (Blanchio, Przepiorka, Boruch & Balakier, 2016, p. 29). Since the need for privacy is an important influencing variable for privacy concerns (Yao, Rice, & Wallis, 2007) that can indirectly influence users' privacy behaviors (Dienlin & Trepte, 2015, Dienlin & Metzger, 2016), this variable plays an

important role when investigating users' privacy behavior in general *and* after receiving a persuasive privacy prompt in particular. It might be reasonable to assume that users with a high need for privacy follow a privacy recommendation more strictly than do people with a low need for privacy. So far, this relation has not been investigated experimentally with regard to the impact of real-time privacy support measures, which is why this dissertation aims at examining the influencing role of users' need for privacy concerning such measures (see Study 2 and 3). According to the privacy process model, individuals engage in privacy regulation if they perceive a privacy state that is not in accordance with the desired level of privacy (Dienlin, 2014; see Study 4). Similarly, an individual's need or desire for protection might depend on his or her perception of current privacy protection. Those individuals who feel sufficiently protected in privacy-relevant situations will probably have a weaker wish for more protection (e.g., through a supportive tool) compared with persons who perceive a lack of privacy protection that results in perceived insecurity. In an online study, Morton (2013) revealed users' desire for privacy to be related to their informational privacy concerns (Morton, 2013). Dienlin (2017) found that shy persons and those who tend to avoid risks tend to desire more privacy from other people, whereas they do not tend to wish for anonymity from the government. This indicates that the general risk tendencies of individuals also influence their desire for privacy, which in turn might have an influence on their intention to disclose personal information on the Internet or their willingness to use protective privacy support tools. It is conceivable that users with a high need for privacy are more prone to privacy interventions than users are with a low a need for privacy. Therefore, participants' desire for privacy will be examined in the present work, as well.

6.2.2 Need for Popularity

Users' need for popularity contradicts their need for privacy but it is related to online privacy behavior as well. This need is defined as the motivation to behave in a way so as to appear popular and liked (Santor, Messervey, & Kusumakar, 2000) implying that users need to provide information in order to get recognized by others. In line with this, users' online self-disclosure is, among others, driven by their individual need for popularity (Christofides, Muise, & Desmarais, 2009; Hofstra, Corten, & van Tubergen, 2016; Utz, Tanis, & Vermeulen, 2012). Since people with a high need for popularity want

to be visible in order to get positive feedback, recognition, and respect (Utz, Tanis, & Vermeulen, 2012), they might be less prone to withdrawing information after receiving a persuasive privacy prompt. However, there are also contradicting findings indicating that the need for popularity is not a significant predictor of presenting oneself in status updates on Facebook (Winter et al., 2014). Moreover, Chen, Widjaja, and Yen (2015) found evidence of openness to new experiences being a negative moderator in the relation between need for popularity and self-disclosure on Facebook. In that study, self-disclosure was measured with items by Krasnova, Spiekermann, Koroleva, and Hildebrand (2010) referring to self-disclosure habits (e.g., “When I have something to say I like to share it on the online social network”). Based on heterogeneous findings regarding the predictive role of the need for popularity in online self-disclosure behavior and the potential impact of users’ need for popularity on the effectiveness of privacy support measures, the current work examines the moderating role of this manifestation of personality between privacy support measures and actual privacy behavior (see Study 2 and Study 3).

6.2.3 Impression Management

Chester and Bretherton (2007, p. 223) define impression management as “the process of controlling the impressions that other people form”. It is a person’s endeavor to create and maintain a specific impression of him- or herself in order to be perceived by others in the way the person wants to be seen (see Goffman, 1959; Leary & Kowalski, 1990). According to Goffman (1959), people behave in their everyday lives like actors in a theater, because they want to build and maintain a specific facade or impression (Goffman, 1959). People who engage in impression-managing activities want to present themselves as someone they would like to be or to be perceived by others (Goffman, 1959; see also Utz & Krämer, 2009). Self-presentation is an important factor for impression management since it is a controllable act of highlighting and hiding individual characteristics to form the desired impression of oneself (Leary & Kowalsky, 1990). This highlighting and suppressing of particular characteristics depends on environmental and situational factors (Goffman, 1959). For instance, the impression a person wants to create for colleagues at work might differ from the one that is created for peers. People who ascribe a high value to the opinion of others regarding the self tend to engage more

intensely in impression-managing activities than do individuals who are not concerned about other people's opinions (Leary & Allen, 2011). Consequently, the motivation of a person to engage in impression management affects his or her daily life (Chester & Bretherton, 2007), which is also true for their social life online (e.g., on SNSs). Since users have time to think about the desired impression being presented via their individual profile, and since they can use several technical options to strengthen the created impression (e.g., through uploading or editing pictures), impression management can be carried out perfectly on SNSs. Furthermore, the impression can be carefully adapted to particular communication circles and perceived audiences (although perceived audiences often differ from the real ones, i.e. *invisible audiences*; e.g., Vitak, 2012) and self-presentation itself can occur in an asynchronous (i.e. artifacts) or synchronous (i.e. performances) way (see Hogan, 2010). There has been a wealth of research concerning users' impression management motivation and its impact on social media usage, profile preparation and disclosing or "untagging" behavior (e.g., Birnholtz, Burke, & Steele, 2017; Krämer & Haferkamp, 2011; Lankton, McKnight, & Tripp, 2017; Vitak, 2015). In addition, scholars increasingly consider impression management motivations in the light of online privacy threats. For instance, users with strong impression management motivation and strong narcissism manifestation tend to engage less intensely in the adaptation of privacy measures than do users with low manifestations of these characteristics (Krämer & Haferkamp 2011; Panek, Nardis, & Konrath 2013; Utz & Krämer 2009). Narcissism will be referred to in more detail in the following subsection. Furthermore, people who strongly engage in impression management through their online profiles tend to have less restricted online profiles than those engaging less in impression management (Utz & Krämer, 2009). Given that without disclosing information about oneself, it is hardly possible to create and maintain a positive impression, users' self-disclosure and impression management motivations relate to and often involve each other (Krämer & Haferkamp, 2011; Utz, 2015). However, impression management and self-disclosure are not the same but rather distinct concepts that are nevertheless based on similar motivations and drivers (Krämer & Haferkamp, 2011). In sum, impression-managing activities are highly relevant in investigating online behavior, especially if it is aimed at examining the impact of protective measures and potential influences of the manifestation of impression management (see Study 2).

6.2.4 Narcissism

Since early investigations on narcissism, this trait has been referred to as *extreme self-love* (Freud, 1946). Narcissism has been associated with low empathy and sensitivity for other people as well as with high expressions of authority (regarding the self as authority), self-sufficiency, exaggerated opinion of oneself, exhibitionism, disposition to exploiting other people, vanity, and demanding appreciation (see NPI, Raskin & Terry, 1988). According to Morf and Rhodewalt (2001), narcissistic people tend to be egocentric and to have a less stable emotional system in comparison with non-narcissistic people. Furthermore, individuals with a strong expression of narcissism tend to engage more in self-deception, have higher expectations regarding the self, and experience more congruence between the real and the desired self than do people with weak manifestation of narcissism (Bierhoff & Herner, 2006). Narcissistic people also tend to experience somewhat unstable feelings of self-esteem compared to non-narcissistic persons (Bierhoff & Herner, 2006). More recently and with regard to the usage patterns on SNSs, narcissism has been revealed to be related to the desire of having a great social network and to present the self in a positive light (Bergman, Fearington, Davenport, & Bergman, 2011), implicating a higher level of overall social media usage (see also Buffardi & Campell, 2008). Buffardi and Campell (2008) also found narcissistic users of SNSs to provide more content that is self-promoting. Additionally, narcissistic persons are less socially anxious with regard to the fear of being shamed (see also Wink, 1991). Narcissistic persons also upload more content and pictures of themselves to SNSs (Ong et al., 2011 Attrill, 2015), driven, for instance, by the need for self-promotion (Mehdizadeh, 2010). In line with this, high levels of activity in online social networks can be predicted by users' narcissism as narcissistic users tend to produce much self-promoting content such as presenting oneself in status updates (Buffardi & Campbell, 2008; Winter et al., 2014).

The results reported so far considered narcissism as a holistic concept in itself but, in fact, narcissism can be partitioned into vulnerable and grandiose narcissism (Ahn, Kwolek, & Bowman, 2015; Miller et al., 2011; Miller, Gentile, Wilson, & Campbell, 2013; Paramboukis, Skues, & Wise, 2016; Pincus, Cain, & Wright, 2014; Wink, 1991). With regard to online privacy, users' expression of vulnerable narcissism has a significant positive effect on their behavioral intention to control privacy on the Internet (Ahn, Kwolek, & Bowman, 2015). This influence of vulnerable narcissism on privacy

protection behavior might be explainable by the fact that vulnerable narcissistic persons act driven by fear and suspicion, being extremely sensitive and fragile (Wink, 1991). Thus, vulnerable narcissistic people might also be more afraid of privacy harms that could possibly have negative consequences for their image. By contrast, grandiose narcissistic persons tend to be dominant, extroverted, and self-assured (Wink, 1991). In their study regarding the intention to engage in privacy protection, Ahn, Kwolek, and Bowman (2015) did not find grandiose narcissism to predict the behavioral intention of users. The authors conclude that providers of SNSs should be aware of users' personal traits having an effect on their SNS usage. More precisely, it is suggested to use this knowledge for adapting the networking site itself or privacy policies in particular to the individual traits of users, for instance, by providing more comprehensive explanations concerning privacy policies to vulnerable narcissistic persons, or making self-protective functions available for users (Ahn, Kwolek, & Bowman, 2015). Further, vulnerable narcissism has been revealed to relate to specific posting behavior on the Internet (e.g., Barry, Daucette, Lofin, Rivera-Hudson, & Herrington, 2017). In line with Barry and colleagues (2017), this work argues that users' expression of narcissism plays an important role for online behavior because social media offers plenty of opportunities for beneficial self-presentation (i.e. one aim of narcissistic persons), and therefore, it might also influence the willingness to engage in privacy protection (e.g., in terms of restricting the profile or limiting self-disclosure). Moreover, Barry and colleagues (2017) found Instagram users' vulnerable narcissism to be related to posting selfies, aiming at presenting the self advantageously in a (perceived) controllable social media environment. Self-evidently, from the perspective of the users, no social media platform can be considered as a completely controllable environment. Given that users' expression of narcissism is related to the time a user takes to edit selfies before sharing (Fox & Rooney, 2015), it can also be assumed that other online actions (e.g., the decision to self-disclose or withdraw content) of narcissistic persons are carefully planned as well. On the one hand, (vulnerable) narcissistic persons tend to share positive images and information about themselves (Barry et al., 2017). On the other hand, this might indicate a tendency to cautious online behavior in terms of not disclosing sensitive content and thereby risking a negative impression, but rather carefully and thoughtfully deciding how to present the self.

In sum, it is important to distinguish between the two expressions of narcissism when investigating privacy protection behavior of (narcissistic) persons. In line with reported findings, this dissertation also argues that vulnerable narcissism, in contrast to grandiose narcissism, is positively related to privacy behavior and that the effect of privacy support measures on users' disclosure behavior might depend on users' manifestation of narcissism as well (see Study 2 and Study 3).

6.2.5 Need for Cognition

Need for cognition is defined as “the tendency for an individual to engage in and enjoy thinking” (Cacioppo & Petty, 1982, p. 116), which is a relevant factor affecting people's decision-making (Cacioppo & Petty, 1982; Haugtvedt & Petty, 1992). A person's need for cognition describes his or her desire to engage in problem-solving and elaborated thinking (Cacioppo & Petty, 1982). Along with the desire to cognitively exert themselves, persons with a high need for cognition find immense joy in solving problems and finding a solution (Carenini, 2001). They also elaborate available options and choices more carefully and take more alternative solutions into account instead of being satisfied with the simplest one (Levin, Huneke, & Jasper, 2000). In doing so, people with a high need for cognition are very straightforward, rational, and motivated (Curseu, 2006; Epstein, 1996). As Haugtvedt and Petty (1992) stated, people's need for cognition has an influence on their tendency to actively process information of persuasive communication. With regard to social media usage, it has been revealed that the expression of users' need for cognition positively correlates with their tendency to seek for information online (Das, Echambadi, McCardle, & Lockett, 2003). Further, the need for cognition of social media users can impact their information-seeking behavior and their formation of attitudes online (Carenini, 2001). Since people with a high need for cognition perceive their environment differently compared with those with a low need for cognition, the perception of websites and social media offers by people who like to think in an elaborated way might differ from the perception of other people (see Attrill, 2015). In line with this, people high in rational thinking might perceive privacy support measures (e.g., warning messages) differently than people low in rational thinking might. With regard to online privacy behavior, it has recently been revealed that users with a high need for cognition elaborated the risks and benefits of online self-disclosure carefully and

reflected, whereas users with a low need for cognition tend to discount rational evaluation of possible privacy threats and instead rely on subjective feelings regarding the intention to self-disclose on SNSs (Kehr, Kowatsch, Wentzel, & Fleisch, 2015). In addition, individuals lower in need for cognition tend to rely on the experimental system of decision-making (based on heuristics and emotions), while a high need for cognition is an indicator of considering the rational system of decision-making (based on deliberation; Epstein, 1996; Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Moreover, users' need for cognition might be related to a more careful anticipation and weighing of potential privacy risks and benefits of self-disclosure and consequently influencing the privacy calculus. Kehr, Kowatsch, Wentzel, and Fleisch (2015), for instance, found that people's need for cognition was positively related to the perception of privacy risks of self-disclosure. In line with Kehr, Kowatsch, Wentzel, and Fleisch (2015), this work assumes that users with a higher need for cognition might differ from users with a lower need for cognition with regard to online privacy decisions associated with privacy risks. This assumption challenges the privacy calculus (Culnan & Armstrong, 1999), which originally assumed that people rationally weigh risks and benefits of upcoming decisions without taking individual needs and capacities for rational decision-making into account. It needs to be noted, that the extent to which rational and cognitive elaboration is needed for making a certain decision depends on the content and the impact of the decision itself. In their study with 177 users from the United States, Kehr, Kowatsch, Wentzel, and Fleisch (2015) revealed that participants' need for cognition was positively related to perceived risks but not significantly related to perceived benefits (both, risks and benefits were operationalized according to the privacy calculus). Nevertheless, the authors found perceived risks and benefits to be mediators in the relationship between need for cognition and the intention to disclose on an SNS. In sum, it is reasonable to assume that the extent to which users enjoy thinking might also affect their risk assessment of online disclosure behavior, which is the reason for need for cognition being considered in the present work.

6.2.6 Self-Control

Following the the theory of planned behavior, perceived control over an action is an element shaping human behavior in the sense that if an individual perceives control, he or she will more likely perform the action than if the person would not perceive having

control (Ajzen, 1991). Self-control helps people to regulate behaviors and emotions in everyday life (Beaver, Barnes, & Boutwell, 2014) and to resist and avoid impulses or temptations (Ent, Baumeister, & Tice, 2015). Transferred to online privacy, users with high self-control might be more inclined toward resisting the temptation of gathering social support or gratification through disclosing sensitive information along with more thoughtful privacy regulation. Furthermore, high self-control is related to individual well-being and to the low likelihood of consuming substances in an abusive manner (Tangney, Baumeister, & Boone, 2004). In line with this, it can be assumed that people with a strong expression of self-control are also less prone to abusively or thoughtlessly using social media, conceivably indicating a more controlled and aware online privacy behavior. Chen, Beaudoin, and Hong (2017) found that characteristics related to weak self-control were positively related to being a victim of Internet scams. Further, perceived control over information can decrease perceived risks concerning individual privacy threats (Olivero & Lunt, 2004). Moreover, a qualitative study in the realm of e-commerce revealed that a low extent of privacy concern is related to a strong perceived control (Olivero & Lunt, 2004). Therefore, users with pronounced self-control might not need privacy interventions for enhancing their online privacy, conceivably indicating that users with high self-control are less prone to privacy interventions. Nevertheless, self-control and perceived control over personal data on the Internet are different constructs. Both seem to be very relevant for privacy behavior and privacy protection intentions on SNSs. However, they need to be considered distinctively, which is why this work distinguishes between self-control as a trait and perceived privacy control as an additional variable (see Study 4).

6.3 Further User-Specific Factors

Besides users' stable personality traits, there are further variables such as sociodemographic variables, perceived social norms, and privacy concerns influencing online behavior. In the following sections, the relevant variables for this work will be outlined, emphasizing the relation to privacy and privacy protection behavior.

6.3.1 Differences in Privacy Behavior depending on Users' Sex

Male and female users differ with regard to certain behaviors on social media. For instance, the distribution of male and female Facebook users in January 2018 worldwide shows that between 18 and 34 years, there are more male (18–24 years: 16%, 25–34 years: 16%) than female users (18–24 years: 12%, 25–34 years: 12%; Facebook, statista, 2018^{5,6}). By contrast, there were 52% female and 48% male Facebook users in the United States⁵. In Germany, there were 3.3 million female and 3.8 million male Facebook users aged 18–24 years in January 2017. Furthermore, there were 4.5 million female and 5 million male users aged between 25 and 34 years, whereas at the ages of 35 to 44 years there were 3 million female and 3.2 million male users^{5,6}.

However, the disparity between female and male Instagram users is smaller than the disparity between female and male Facebook users. Worldwide, there were 15% female and 16% male Instagram users aged between 18 and 24 years. At the age of 25–34 years, there was exactly the same amount of male and female users (each 15%)⁵.

With regard to online privacy, research revealed that male and female users of online applications differ in their privacy and self-disclosure behavior as well as regarding their privacy concerns (e.g., Hoy & Milne, 2010; Special & Li-Barber, 2012, Sun, Wang, Shen, & Zhang, 2015; Youn & Hall, 2008). That is, women have stronger privacy concerns than men do (Bujala, 2011; Hoy & Milne, 2010), women tend to disclose less contact information and use more privacy settings than men do (Special & Li-Barber, 2012), and also tend to engage more in privacy behavior compared with men (Saeri, Ogilvie, Macchia, Smith, & Louis, 2014). Furthermore, women are more influenced by perceived risks regarding their intention to disclose online than men are (Sun, Wang, Shen, & Zhang, 2015). In 2011, Bujala investigated gender differences in the habits and intensity of Internet usage of users in Poland. Among others, she found that female users spent less time online (on average nine hours per week), were more skeptical regarding online services or relationships, and along with these aspects, had less online experiences compared with male users. By contrast, male users used the Internet more often and more intensely (on average 12 hours per week), mainly for entertainment reasons (e.g., exposure to music, films, humorous content). A survey with 254 college students in

⁵ See <https://wearesocial.com/de/blog/2018/01/global-digital-report-2018> (last access: 4th November, 2018)

⁶ See <https://de.newsroom.fb.com/company-info/> (last access: 4th November, 2018)

Taiwan revealed differences between males and females regarding the usage of Facebook's privacy settings in terms of women being more concerned regarding self-disclosing activities than men were and in line with this chose stricter privacy settings than men did (Kuo & Tang, 2015). More precisely, male and female users differed with regard to all categories of privacy settings, namely, basic, personal, and contact settings, showing women to be more conservative with their privacy. Furthermore, Saeri, Ogilvie, Macchia, Smith, and Louis (2014) found that female users engaged more in privacy behavior than male users did. Therefore, it might be reasonable to suggest that male and female participants are influenced differently by privacy support measures and show different privacy behaviors. In contrast to this assumption, Witte and Allen (2000) concluded in a meta-analysis regarding fear appeals in health communication under consideration of users' personality and characteristics that neither users' personality (with some exceptions) nor their gender seems to have a significant influence on the perception/impact of risk communication. Since the privacy support measures that are considered here are tools for communicating risks, it was controlled for sex in the analyses of this dissertation.

6.3.2 The Impact of Privacy Norms

Research on social processes and humans' perceptions of the social environment revealed that prevalent social norms can seduce people to behave in a way that they think society or their peers believe to be appropriate (e.g., Asch, 1951; Park & Smith, 2007). In general, people tend to follow and stick to perceived social norms in order to feel socially accepted, gain social approval, and fulfill their need for assessing the self positively (e.g., Cialdini & Goldstein, 2004). Fear of isolation or of being excluded from social groups makes people adhere to group rules and prevalent norms and values within a group (Miller & Prentice, 1966). With regard to SNSs, it has been revealed that perceived social norms referring to appropriate privacy behavior positively influence the usage of restrictive privacy settings (Utz & Krämer, 2009). Given that perceived norms are an important factor shaping people's (privacy) behavior, and that young adults and adolescents (i.e. typical social media users) are oftentimes affected by peer pressure, Utz and Krämer (2009) suggested that privacy protective recommendations might be especially influential if they are transmitted by a peer member instead of an authority,

and that awareness of privacy behavior might increase when peers behave securely as well. However, in contrast to social norms in offline contexts, the online context is more ambiguous, and prevalent norms might be more heterogeneous than in physical environments (Steijn, 2016). Despite this ambiguity of online contexts making it more difficult to adhere to norms, Steijn (2016) argues that perceived privacy norms might be the most relevant factor persuading users to engage in privacy protection. Furthermore, Steijn (2016) argues that neglecting social norms in privacy research might be one reason for not finding relations between privacy concerns and privacy behavior (i.e. the privacy paradox, see Chapter 5.1).

Addressing the reported findings, this work considers perceived privacy norms as a potential factor shaping users' privacy behavior in terms of responding to system-based persuasive privacy support. Since there are different dimensions of privacy norms, namely, peer (involving perceptions regarding friends and family), societal (here, containing perceived norms of people living in Germany), and media norms (covering the perception of media coverage), this work distinguishes between these dimensions of social norms (see Park & Smith, 2007).

6.3.3 The Impact of Privacy Concerns

Privacy concerns are a relevant but ambiguously influencing factor in privacy research. So far, privacy concerns have been identified as being a predictor of online privacy behavior by several scholars, whereas other scholars were not able to find support for privacy concerns having a direct impact on online activities, as it is reflected on in the following. Inconsistencies in research findings demonstrate the difficulty of clearly identifying under which conditions privacy concerns might indeed affect actual behavior and which circumstances detach concerns from the prediction of behavior. Nevertheless, the extent of users' privacy concern seems to be a relevant variable with regard to the impact of privacy support measures and subsequent privacy behavior.

In general, concerns are negative attitudes to or associations with an object or situation. In contrast to general (bipolar) attitudes that can be either positive or negative, concerns always refer to anticipated negative outcomes of a situation and therefore can be designated as unipolar (see Dienlin & Trepte, 2015). Thus, a concern represents the extent to which a person is worried about a possible negative outcome of a situation, for

instance, negative consequences of the disclosure of personal information on the Internet (Li, Luo, Zhang, & Xu, 2017). Xu and colleagues (2008) state that privacy concerns refer to the potential loss of privacy as a negative consequence of disclosing personal information. With regard to concerns of self-disclosure on websites, Andrade, Kaltcheva, and Weitz (2002) concluded that the integrity of privacy policies and the reputation of a website provider reduce privacy concerns, whereas offered rewards increase concerns of users, indicating a certain extent of skepticism of the users. Dienlin and Trepte (2015) suggest considering privacy concerns in addition to privacy attitudes and intentions in order to explain privacy behavior more reliably. Although the authors did not find evidence of a direct relation between privacy concerns and privacy behavior, they found an indirect influence of concerns on informational, social, and psychological privacy attitudes, which then had a direct effect on informational, social, and psychological privacy behaviors (see Dienlin & Trepte, 2015). Deduced therefrom, privacy concerns, if accompanied by respective privacy attitudes and intentions, can influence the extent of self-disclosure and the behavior of SNS users. Consequently, on the one hand, concerns might be regarded as advantageous and positive because they seem to shape users' privacy behavior in a way that their privacy is less threatened if concerns are accompanied by privacy literacy or privacy awareness for instance (because otherwise concerns might instead induce reactance or replacements of fears). On the other hand, privacy concerns might also be seen as being adverse because continuous concerns and fears can reduce people's well-being (see also Westin, 1967) and might threaten their carefree online life. In this dissertation, concerns will be regarded as one driver for privacy behavior and a negative predictor of online self-disclosure. Whether concerns are negatively or positively connoted will be discussed later. If privacy behavior is distinguished into self-disclosure and self-withdrawal, it can be observed that privacy concerns and anticipated benefits predict self-disclosure behavior whereas withdrawing behavior is driven by privacy concerns and privacy self-efficacy (Dienlin & Metzger, 2016). Facebook users with strong privacy concerns tend to use more self-withdrawal mechanisms, such as not friending someone or limiting disclosures on Facebook, compared with unconcerned users (Dienlin & Metzger, 2016). However, privacy concerns are not the only predictor of online behavior but they can induce information withdrawal if anticipated benefits are not as salient as anticipated negative outcomes (see privacy calculus; Culnan &

Armstrong, 1999). Thus, neither anticipated benefits nor privacy concerns explain users' online behavior exclusively but the interplay of both contribute to explain the online behavior of social media users (see Dienlin & Metzger, 2016). However, on the basis of a meta-analysis, Baruh, Secinti, and Cemalcilar (2017) concluded that users with pronounced privacy concerns are likely to use measures for privacy protection and at the same time are less likely to reveal information about themselves. Therefore, when analyzing privacy decisions, it is important to consider both, perceived benefits as well as anticipated negative consequences of self-disclosure.

7 Privacy Protection

“There exists a failure in translating users' privacy needs into socio-technical environments” (Reynolds et al., 2011, pp. 213–214). This conclusion by Reynolds, Venkatanathan, Gonçalves, and Kostakos (2011) emphasizes one major aspect of the present work. Despite the existence of several approaches for privacy and security protection, there is still dissatisfaction with the support measures provided, conceivably because of the missing fit between users' individual privacy needs and the provided measures.

Approaches for enhancing users' online privacy and reducing privacy risks are of common interest in the modern digitalized world. Researchers, teachers, parents, and politicians are trying to find adequate ways to support Internet users in maintaining online privacy, especially concerning the usage of SNSs. So far, research covered both, system-based support approaches such as nudging and prompting (i.e. elements that guide humans' behavior, e.g., Wang et al., 2013) as well as educative support measures for increasing privacy literacy (i.e. knowledge concerning privacy protection and respective measures; e.g., Egelman, Bernd, Friedland, & Garcia, 2016). The problem is that despite several users implementing anti-virus software, for instance, their privacy is not comprehensively protected (which might contradict the users' perceptions). A survey on protection measures with regard to cybercrime with 1,639 participants in Germany (Bundesamt für Sicherheit in der Informationstechnik, 2016⁷) revealed that 92.1% of users use current anti-virus software, 86.5% use safe Internet connections (what *safe*

⁷ See https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (last access: 4th November, 2018)

really means and whether people have a common understanding of its meaning are open to question), or implement updates immediately (82.2%). Still, privacy is being violated and negative consequences with regard to privacy breaches are experienced. This highlights the importance of providing more sophisticated online privacy support, which will be referred to in the following section.

7.1 The Importance of Protecting Online Privacy

For adequately regulating online privacy, users need to understand which information is sensitive, who has access to it, and what can be derived from the provided data (see Chapter 3). In other words, how their disclosures could be used against their will or without their approval, infringing their rights of privacy. Today, it is possible to draw conclusions about users' personal preferences and habits based on their Facebook *likes* or group memberships (see Kosinski, Stillwell, & Graepel 2013). Information disclosed on users' profiles can be used to predict personal traits and attributes like sexual orientation, religious and political views, personality traits, intelligence, happiness, and tendency toward addictions (Kosinski, Stillwell, & Graepel 2013; Zheleva & Getoor 2009). Such assumptions may be made not only by institutions, organizations, and SNS providers, but also by acquaintances, employers, or strangers – albeit less systematically. According to Livingstone (2008), insecure privacy behavior is attributable to both, bad interfaces of social network providers lacking information regarding privacy risks and the missing literacy of the users themselves.

Although some privacy protection approaches such as privacy-enhancing technologies (PETs; see Heurix et al. 2015) have already been proposed, a persuasive real-time solution as it is introduced in this work represents a novel idea with various benefits. PETs, as opposed to the approach proposed here, aim at protecting users' identities through maintaining *anonymity*, *unlinkability*, *pseudonymity*, and *unobservability* (Fischer-Hübner 2001; Pfitzmann & Hansen 2008), mainly covering the dimension of informational privacy. By contrast, this work additionally aims at covering the multidimensionality of privacy by also considering social and psychological privacy (see Chapter 2.1). Furthermore, the current theoretical concept covers planned and spontaneous actions, minimizes effort for the user, and is adapted to the user's needs and respective dimensions of privacy and privacy violations.

Still, users tend to underestimate their own privacy risks, and to overestimate those of others (Baek, Kim, & Bae 2014). Consequently, users of SNSs have a biased view of their online privacy (Baek, Kim, & Bae, 2014) which can result in a lack of privacy protection intentions and risky and regrettable online behaviors. Against this background, there is the need for evaluating advanced privacy protection measures and analyzing users' reactions and opinions toward respective measures from a psychological point of view.

Privacy protection services and systems should consider some user experience design principles in order for them to get adopted and accepted by users for generating privacy-aware behaviors on the Internet. An investigation in 2014 revealed that users of SNSs are most satisfied with systems that provide individual aggregation possibilities of privacy settings such as grouping social contacts and making individual options regarding with whom to share something and with whom not (Knijnenburg & Kobsa, 2014). Actually, the most commonly used social networking site Facebook allows for these required procedures and still, people do not feel comprehensively comfortable and safe on Facebook (see Study 1). This led to the emergence of self-developed privacy protection strategies by users, which will be considered in the following section.

7.2 Self-Regulated Privacy: The Appeal of Alternative Protection Strategies

The SNS Facebook provides privacy and security information for its users. However, Facebook's *privacy help* gives access to basic security information, for example, on hacking or restricting access to the profile and postings, instead of providing comprehensive individual privacy support. Facebook's *privacy basics* contain information referring to secure passwords, data encryption, and virus detection methods. The social network even provides a copy of collected user data that can be downloaded by the user (Facebook.com). Undoubtedly, providing such information is important. Still, privacy violations happen and insecure behaviors occur (e.g., Internet Crime Complaint Center, 2016). Notably, these settings primarily concern informational privacy (see Burgoon, 1982), implying that social and psychological privacy can be still attacked and damaged. Consequently, although SNSs in fact provide certain settings for managing privacy (e.g., defining audience for specific postings, creating friend lists, limiting access to the profile), several users tend to engage in self-developed protective strategies such

as self-censorship, selective or strategic information sharing, creating multiple identities, providing false information, or *lurking* (e.g., Metzger et al., 2012). Matzner, Masur, Ochs, and van Pape (2016) refer to individual-driven data protection measures as do-it-yourself (DIY) protection and distinguish between preventive (e.g., data parsimony) and corrective (e.g., deleting postings) measures. Strategies like *whitewalling*, *social steganography*, and the *super-logoff* (boyd, 2007, 2010) are even more advanced and will be referred to in the following. Thus, the impact of the settings and information offered by SNS providers on users' privacy behavior remains uncertain. Even though there is a considerable amount of privacy research, the question of which user types decide to use alternative self-developed measures for privacy protection under which circumstances remains open.

The procedure of whitewalling (also *whitewashing*, *blog scrubbing*) describes a process of deleting or modifying postings or blog entries on SNSs after they have been read by other users (boyd, 2007; Child, Petronio, Agyeman-Budu, & Westermann, 2011; Raynes-Goldie, 2010). Whitewalling therefore allows the most accessible digital footprints to be concealed. Through using this strategy users are still able to communicate and release their emotions and feelings but by deleting the content after some time they feel less attackable (boyd, 2007). However, shared information can be spread, commented on, or distorted by other people even it is only online for a short time. One alternative to sharing information and deleting it afterwards would be to communicate via messenger or face-to-face, although there might be a special gratification in sharing it publicly so that the remaining risk is accepted by users.

One further alternative privacy strategy is called *social steganography* (boyd, 2010; boyd & Marwick, 2011). Steganography itself is not a new concept but a well-known measure for hiding the real meaning of a message owing to security reasons (cf. boyd & Marwick, 2011). The specialty of such hidden messages is that people who are not the intended receiver do not even realize that the text they are reading might contain more than what is obviously visible. Social steganography allows its users to communicate via a public channel without permitting other readers to take part in the interaction. For those who do not know how to decode a message, its meaning is invisible (boyd & Marwick, 2011). Again, it would be easier for users to consult other channels of

communication, but they are instead willing to make the effort of using this strategy than to change the channel of communication.

The most radical measure applied by Facebook users might be to temporarily deactivate one's account (i.e. *super-logoff* or *opting out*). It is the very same procedure that has to be executed if a user wants to delete his or her Facebook profile. Only if the user does not reactivate the account during a specified period of time will it be deleted completely. Deactivating one's account entails that a user who is currently not online cannot be addressed, linked, or stalked by other people (see boyd, 2007, 2010). The user is hidden and seems to be invisible for the network. During this time, the numerous gratifications of SNSs (e.g., positive feedback) disappear from one second to another. The radical character of this strategy makes it highly interesting to examine the motives and influencing factors in considering a *social retreat* for privacy protection. danah boyd was the first one who extensively examined the super-logoff (boyd, 2007, 2010). She found that American teenagers perceive the super-logoff to be an adequate measure to avoid negative consequences of online self-disclosure (e.g., being observed or punished by parents or teachers) with little effort. If the user wants to login again, he or she can reactivate the account and use the network as before (see Study 1).

Further reasons for considering self-driven protection strategies or not, and the situational circumstances in which alternative strategies are employed, might be quite diverse and depend, amongst other things, on inter-individual privacy perception (e.g., Teutsch, Masur & Trepte, 2018), privacy skills (e.g., Büchi, Just, & Latzer, 2016), and individual privacy regulation experiences (e.g., Bartsch & Dienlin, 2016). It might be the case that users implement alternative protection strategies only several times or solely for specific situations, whereas they behave in a less privacy-aware way in other situations or other networks. This makes it highly interesting to examine particular motives for using alternative strategies and to shed light on the sensitivity of these special situations. It should be taken into consideration that especially the users' perception of privacy is increased by using such strategies but that sporadically hiding particular postings or information does not guarantee privacy. Thus, there might be a discrepancy between perceived and actual levels of privacy.

Summing up, there is a lack of knowledge regarding the relation between users' privacy attitudes, concerns, and individual intentions and motives to deactivate their

accounts. This dissertation strives to answer the question whether the super-logoff contributes to increases in perceived levels of online safety and consequently might even override users' privacy concerns. The motives for using the super-logoff will be investigated with respect to current research regarding privacy protection strategies (see Study 2).

Self-protection strategies of users are one possibility for increasing online privacy. However, self-regulated protection measures do not provide comprehensive protection since there might be unknown risks against which users do not protect themselves, a lack of attention or interest (e.g., if gratifications outweigh situational protection motivation), or misjudgments of threats. Therefore, technical support from an objective and user-centered entity is needed.

8 Technical Privacy Protection

This chapter addresses the basic conclusion by Reynolds and colleagues (2011), saying that there is a mismatch between users' privacy needs and provided features to protect online privacy by outlining chances and boundaries of system-based measures for increasing users' privacy. This interdisciplinary approach represents a pivotal part of this dissertation, which is combining psychological and technical factors for developing adequate privacy support measures for users of SNSs. Accordingly, current privacy-enhancing approaches are presented and discussed as well.

8.1 An Interdisciplinary Approach

This work hypothesizes that current privacy protection approaches do not fully meet the users' expectations and requirements. So far, different approaches for privacy protection have been suggested, focusing on different perspectives, namely, either external (e.g., through systems, external parties) or internal (e.g., self-regulated attempts, increasing literacy) empowerment. However, privacy support should be adapted to the user and to the current situation as well as to the threatened dimension of privacy. There is a big challenge, on the one hand, of developing privacy support as suitable to the user as possible, and, on the other hand, leaving sufficient space for users' autonomy without inducing feelings of anger or strong paternalism.

Users differ in their privacy needs, personality, and privacy management strategies (see Chapter 6). Recently, Wilkinson and colleagues (2017) also suggested a user-tailored privacy by design approach in order to avoid a “one-fits-all-solution” (p. 1). According to the authors, users do not make use of privacy settings provided by the SNS Facebook although this contradicts their self-reported needs for privacy (Wilkinson et al., 2017). Therefore, it is argued that systems that are adapted to the user and the current privacy situation might be more expedient solutions for increasing privacy behavior than the so-called generic one-fits-all solutions (Wilkinson et al., 2017). As proposed by Díaz Ferreyra and Schäwel (2016) and Díaz Ferreyra, Schäwel, Heisel, and Meske (2016), to provide adapted support in real-time, self-adaptive systems might be needed. Therefore, the next subsection will briefly outline the main functions of self-adaptive systems before it will be referred to requirements for technical privacy support in more detail in the subsequent section.

8.2 Self-Adaptive Systems for Privacy Protection

Self-adaptive systems are systems that are able to work autonomously and do not necessarily need a steering user. They can be considered to provide user-oriented outputs adapted to the users behavior. They consist of a *managed system*, providing features to the user and a *managing system* which monitors the managed system and its environment (Salehie & Tahvildari, 2009; Weyns, Iftikhar, Malek, & Andersson, 2012). The functionality lies in a closed feedback loop between the two systems exchanging information regarding the user and the situation. Therefore, a monitoring, a detecting, a deciding, and an acting phase are passed by the system, allowing for collecting and converting data from the environment (monitor), analyzing symptoms (here, behavior) that could indicate a required system response (detection), inducing an action that is required in the situation (decision), and finally applying the action in order to support the user (action; Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016; Salehie & Tahvildari, 2009; see Figure 1). Before implementing self-adaptive software, it is necessary to clearly define the problem that is supposed to be solved by the software and to develop a blueprint for the software architecture (see Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016, Jackson, 2001). This is a very important step, since specifying requirements of a system presupposes the

identification of a problem that needs to be solved (Jackson, 2001). In this case, the “global problem” is an unaware state of a user of an SNS during sensitive self-disclosure associated with a risk of experiencing negative consequences. According to Jackson (2001), in order to distinguish the problem from an adequate solution, it is helpful to clearly identify where the problem is located. The problem described above is located in the “world outside the computer” (Jackson, 2001, p. 3), whereas the solution lies in the computer, or more precisely, in the software that is intended to support the user (see Jackson, 2001).

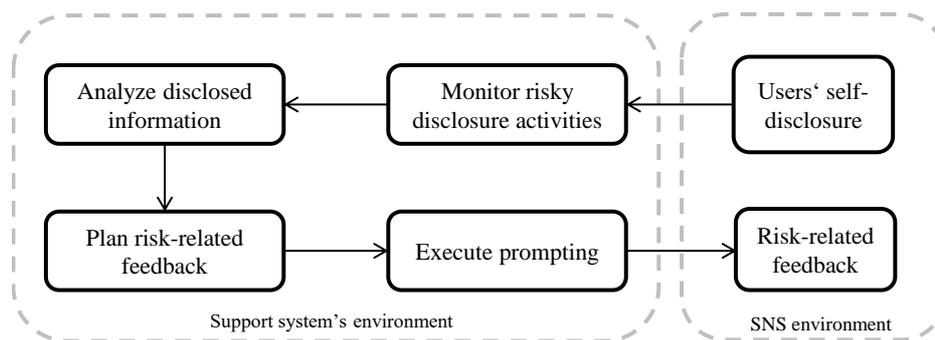


Figure 1: Feedback loop between the user and the privacy support system, see Díaz Ferreyra, Schäwel, Heisel, & Meske (2016)

Identifying sensitive information which pose a privacy risk and shall induce the described feedback loop need to be translated into privacy rules so that a rule-based self-adaptive system may be consulted by a user who wants to protect his or her privacy on an SNS (see Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016). Adaptation in this case refers to the fit with situational circumstances as well as users’ capabilities of processing given privacy recommendations. Therefore, as it is a requirement concerning intelligent tutoring systems for providing suited feedback to learners (see Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016), a proper presentation of a privacy recommendation with regard to timing, design, and the information is required. The need for the adaptation of a system to its users raised the demand for flexible systems that can deal with unforeseen and heterogeneous situations, represented in interdisciplinary research that focuses on situational and individual needs from different perspectives. Along with the rise of self-adaptive systems, there is an increase in various possibilities for interdisciplinary user-support measures. Central aspects are the way risks

are communicated to users, for example, with regard to the style of communication, the persuasiveness, and the amount of information provided.

8.3 Requirements for Technical Privacy Support

So far, the challenge of protecting and maintaining privacy in the online world is being addressed by various research areas and from different perspectives (e.g., Acquisti et al., 2017; Belk, Fidas, Germanakos, & Samaras, 2014; Benenson et al., 2014; Hausawi & Allen, 2014; Wang et al., 2011). As already indicated, it can be distinguished between privacy-regulating endeavors by the government (e.g., through laws), privacy education (e.g., teaching privacy literacy in school), privacy-enhancing technologies (e.g., privacy-by-design concepts or nudges), and self-initiated and self-developed protection behaviors by users themselves (e.g., super-logoff). Privacy-by-design approaches basically follow some main principles of adaptation. These principles comprise:

- (a) Being proactive instead of reactive.
- (b) Treating privacy as a default setting instead of gathering all available information by default.
- (c) Embedding privacy into the design by treating it as a relevant component of the system.
- (d) Including privacy.
- (e) Including security.
- (f) Being transparent.
- (g) Being user-centric and supportive (see Cavoukian, 2011).

From a technical point of view, privacy technologies fulfil the task of reducing the amount of collected identifiable data of an individual (Registratiekamer, 1995). Fischer-Hübner (2001) goes one step further by stressing the importance of protecting “confidentiality, integrity and availability” (p. 107) of data belonging to an individual when defining privacy-enhancing technologies. According to Fischer-Hübner (2001), privacy-enhancing technologies should cover the protection of user identities by providing “anonymity, pseudonymity, unlinkability, and unobservability” (p. 107), control of information access, as well as data encryption. These aspects of privacy

protection mainly cover the dimension of informational privacy as defined by Burgoon (1982), describing personal and identifying data belonging to an individual.

Meis and Heisel (2017) provide an overview of how the core elements of privacy-enhancing technologies (PET) can be considered and integrated in requirement models for building software. Common interest in PETs has increased drastically since 2012, which is noticeable through the growing number of research articles in that realm (Degeling, Lentzsch, Nolte, Herrmann, & Loser, 2016). Since software engineers play an important role in building PETs, it is important to provide a pattern format for PETs that can be referred to in the requirement engineering process. The proposed patterns for designing and integrating PETs relate to the initial and general conditions regarding the software system (i.e. name, motivation, context, problem), the privacy forces arising (i.e. confidentiality, integrity, availability, anonymity, data unlinkability, undetectability, pseudonymity, intervention, as well as information concerning collection, storage, flow, and exceptions), general forces (e.g., user experience), the solution approach, and finally the design issues (general and privacy benefits and liabilities, examples, and related patterns; Meis & Heisel, 2017). These patterns that were inferred in order to help engineers in requirement elicitation and subsequent actual integration of relevant privacy-enhancing factors for future software systems represent relevant demands for users of SNSs and privacy protection tools as well. That is, in order to transmit a feeling of privacy and security, social media providers should be oriented toward these aspects when offering networks for social interaction. However, it might often be the case that the demands are either not fully met or not comprehensively communicated to them by current social network providers. Thus, users might feel a threat to their basic need for privacy. In order to clarify the privacy situation for users of SNSs and decrease feelings of privacy cynicism or the disregard of potential privacy harms (see Hoffmann, Lutz, & Ranzini, 2016), privacy protective tools should meet the presented expectations of transparency. Therefore, it might be helpful if privacy protective tools would be oriented toward these privacy-preserving and privacy-enhancing patterns that might also increase the trustworthiness of the system and the users' willingness to use the privacy protective tool.

Heurix and colleagues (2015) compared existing PETs and developed a taxonomy regarding these technological features. The authors argue that it is important to integrate

measures for maintaining user privacy and data privacy in this taxonomy. User privacy can be related to the social and psychological dimensions defined by Burgoon (1982) whereas data privacy refers to informational privacy. Following the taxonomy of PETs by Heurix and colleagues (2015), information PETs have different dimensions, namely:

- (a) *Scenario*.
- (b) *Aspect*.
- (c) *Aim*.
- (d) *Foundation*.
- (e) *Data*.
- (f) *Trusted third party*.
- (g) *Reversibility*.

All of these dimensions can be distinguished further. The element *scenario* has the task of defining the privacy threat (e.g., by untrusted clients or servers). More closely related to SNSs, an untrusted audience for sensitive information disclosure might be the typical threat defined by the scenario dimension of a PET. The dimension *aspect* of a PET elucidates whether the identity of a user, the content, or a behavior needs to be addressed by a PET. The dimension *aim* covers several privacy aims (i.e. indistinguishability, unlinkability, deniability, and confidentiality) and decides which one is the most relevant in a given scenario of privacy threat. The dimension *foundation* functions as a definer for the security model (e.g., computational or theoretical) to consider and the strength of protection that is needed (e.g., level of cryptography). The type of data that are being threatened and therefore addressed by a PET are defined by the dimension *data*, considering stored, transmitted, and processed data. A *trusted third party* is a highly relevant and critical factor for users' trust in the privacy supportive system. The task of such a trusted entity is to be involved in sensitive operations that a supportive privacy measure might not provide by itself, for example, managing user registration or authentication (Heurix et al., 2015). Depending on the kind of privacy support, the trusted entity might differ regarding the frequency of intervening (e.g., permanently, situational, or never), the phase in which intervention is needed (e.g., regularly, for the setup, or none), and the specific task (e.g., operating, validating, or "no task"; Heurix et al., 2015). Whether an action by a PET is reversible or not is defined by the dimension *reversibility*,

distinguishing between cooperation (e.g., required or not) and degree (e.g., full, partial, none, deniable) of potential reversibility.

When building information technologies and systems in the realm of software engineering, privacy can be assured by following design principles (D' Acquisto, Domingo-Ferrer, Kikiras, Torra, de Montjoye, & Bourka, 2015):

- (a) Restricting the amount of personal data of an individual who is using a system or a technology (*minimize*).
- (b) Hiding personal and identifying data in plain views (*hide*).
- (c) Separating different pieces of information relating to one individual so that it is not possible to get a full picture of that person (*separate*).
- (d) Aggregating personal data so that as little as possible information of the person is used (*aggregate*).
- (e) Making data processing transparent (*inform*).
- (f) Giving users the possibility to intervene in the processing of their personal data (*control*).
- (g) Meeting legal requirements (*enforce*).
- (h) Demonstrating that there is compliance with privacy policy (D' Acquisto, et al., 2015).

By considering all these principles, it may be ensured that the users' informational privacy is protected to a certain extent. Current privacy-by-design approaches aim at integrating privacy from the starting point of development instead of treating privacy as an add-on to an existing system (e.g., Hausawi & Allen, 2014; Degeling, Lentzsch, Nolte, Herrmann, & Loser, 2016). This becomes increasingly important but also more challenging in the modern, digitalized, and heterogeneous world. However, some scholars argue that privacy-by-design practices did not become a widespread method (Ayalon, Toch, Hadar, & Birnhack, 2017).

As already outlined, users of technologies, systems, and social networks differ in their needs, experiences, sociodemographic characteristics, and usage patterns (see Chapter 6). Therefore, it is of special relevance that researchers from different disciplines work together in order to create interdisciplinary measures for protecting online privacy,

by considering human as well as system factors (see Alavi, Islam, Mouratidis, 2014; Degeling, Lentzsch, Nolte, Herrmann, & Loser, 2016).

One thing that software engineering and social psychological approaches have in common is the consideration of the social context of the individual. As proposed by the privacy-by-design approach of Degeling, Lentzsch, Nolte, Herrmann, and Loser (2016), it is important to integrate the users' environment in the design process of privacy-sensitive systems. The advantage of the so-called socio-technological design approach is that the environment of the future user as well as multiple stakeholders from various fields can be considered for developing the system (Degeling, Lentzsch, Nolte, Herrmann, & Loser, 2016).

However, the functionalities reported to date cover the security aspect of personal data rather than the social and psychological dimensions of privacy (see Burgoon, 1982). Certainly, technologies and systems should follow these guidelines for transparent and fair processing of user data. Still, by communicating sensitive emotional data and striving for social support online, users risk not only their informational but also their psychological privacy. This work aims at integrating technological features and principles for guaranteeing privacy with social and psychological privacy needs of users of online network services. In line with this, self-adaptive support measures should be able to communicate risks to the users in real-time, referring to situational privacy states. In this regard, how risks are communicated is especially relevant (as was explained in Chapter 3.4).

8.4 Privacy-Enhancing Design of Systems

Users oftentimes have difficulties to understand specific terms of privacy policies owing to complex wordings (e.g., Kelley, Bresee, Cranor, & Reeder, 2009) or a lack of privacy literacy (e.g., Egelman, Bernd, Friedland, & Garcia, 2016). This has been a relevant topic for several years. Optimistic biases (see also Cho, Lee, & Chung, 2010) constitute a further threat to users' privacy because false perceptions of online privacy might trigger or even enhance insufficient engagement in protection measures.

LaRose and Rifon (2007) analyzed the processing of privacy-related information of 227 participants by comparing the impact of privacy warnings and privacy seals (privacy seals are quality labels indicating that data processes happen in compliance with

data protection laws) on self-disclosing intentions on websites and perceived negative consequences of revealing information. The authors found that the presence of a privacy warning label negatively influenced users' reported intentions to reveal personal information (LaRose & Rifon, 2007). In contrast, the presence of a privacy seal had a positive influence on users' intention to disclose personal information, whereas it had no impact on the perception of negative consequences (LaRose & Rifon, 2007). LaRose and Rifon (2007) critically reflected on this result by emphasizing the danger of misleading privacy seals fostering users to provide personal information, driven by the promise of data protection. Since the privacy protection measures investigated in the current work can be considered as warnings as well, the study reported by LaRose and Rifon (2007) can be regarded as a valuable starting point for investigating the impact of warning messages. The fact that the warning label was able to reduce users' intention to engage in self-disclosing activities supports the idea of communicating potential risks of sensitive self-disclosure to users in order to support them in reducing privacy risks due to revealing sensitive information.

In 2009, Kelley, Bresee, Cranor, and Reeder investigated how privacy policies can be presented at best in order to be comprehensive and clear for users. The gap between privacy policies as they are communicated and the users' understanding of it was addressed by using an approach of re-designing the presentation of privacy policies based on the typical design of nutrition (e.g., vitamins, amount of fat, calories) or energy (e.g., energy information on a fridge) labels (Kelley, Bresee, Cranor, & Reeder, 2009). With this, they addressed the problem that users in theory should be able to make informed privacy decisions by reading the policies, but that they are not doing it in practice (Kelley, Bresee, Cranor, & Reeder, 2009). By means of mainly qualitative investigations the authors found that a memorable and structured representation of privacy information helps users to better understand and remember presented information. In addition to that, it was also observed that with a well-structured collection of privacy information, the users' information seeking experience was more enjoyable (Kelley, Bresee, Cranor, & Reeder, 2009). The authors considered specific patterns for making privacy information more salient to users. For instance, they used colors to indicate the extent of privacy invasion by means of darker colors indicating higher risk. The main issues being analyzed in the mentioned work were users' ability to find relevant privacy information, the users'

understanding of provided information, and the time that users need to find such information. Following the authors, all research aims were achieved because users did find privacy-relevant information faster and easier. This implies that re-thinking the appearance of privacy-related information can be a first step toward increasing users' online privacy awareness and shaping users' online behavior (see Study 3 and Study 4). In line with Kelley, Bresee, Cranor, and Reeder (2009), utilizing visual cues such as color and grid structures help users to compare options and to choose the most advantageous one for them. Due to the simplification of privacy and security information, users would not need to engage in high cognitive effort (in contrast to the need for cognitive effort when processing comprehensive information on one's own). The approach of compressing privacy relevant information and providing cues for accurate privacy decisions is addressed in the current work as well.

Talukder, Ouzzani, Elmagarmid, Elmeleegy, & Yakout (2010) suggested a security measure (the *privometer*) indicating the leakage of information provided to a network by friends of one's own friendlists. In line with the aforementioned approaches, they also suggested using simple visualizations of privacy threats such as a tachometer ranging from low to high information leakage. However, the authors did not test the impact of the *privometer* empirically but rather provided a concept of how to implement such a privacy measure. In contrast to the current work, the work by Talukder and colleagues (2010) focuses on security and informational privacy issues (although the *privometer* indicates the leakage of information caused by a user's online friends, the social privacy, which mainly relates to restricting one's own profile for other people, might be addressed by this tool as well). However, as it was argued in Chapter 2.1, privacy comprises of more than solely informational data. That being said, it might be the case that a user's informational privacy is protected through a measure like the *privometer*. However, there still might be a lack of protection regarding psychological privacy. More precisely, a user might have concealed his or her identifying information such as name, birthdate or E-Mail address, but provided sensitive information regarding political or religious views, sensitive beliefs and values regarding controversy topics, which represent target areas for privacy harms and disadvantageous experiences as well.

In addition to the lack of literacy, which would be necessary for understanding the relevance of privacy protection and the content of privacy policies, users seem to feel

incapable of preventing privacy violations and invasions from companies so that they might conclude that reading privacy policies does not make a difference (Kelley, Bresee, Cranor, & Reeder, 2009). This stresses the demand for alternative methods to help users protect their privacy despite a low literacy or low self-efficacy.

A further problematic issue is that users tend to believe that their private data may be the price to pay for conveniently gathering information on the Internet, being entertained by online services, buying products and services, or being able to communicate and interact with users on SNSs (see Study 1). This is an alarming picture because it threatens not only users' data security and online privacy but also their feeling of autonomy and control over protected communication (i.e. functions of privacy) as well as their freedom to decide which information about them is communicated to whom under which conditions (see Chapter 2.1; Westin, 1967). If users do not have the opportunity to fulfil their privacy needs or are able to withdraw from the public, this can have dramatic consequences for their well-being and psychological balance (see Westin, 1967). Withdrawing from the public in a physical sense covers different states, namely, *solitude*, which means that a person is not being observed by one or more individuals, *intimacy*, describing intimate conversations in small groups and fostering close relationships under exclusion of the public, *anonymity*, referring to the right of not being identifiable, and *reserve*, which describes the limiting of disclosure toward other people (Westin, 1967). Following Westin's theory of privacy (1967), people need privacy in order to regulate and handle daily interactions and social situations. This is one of the reasons why there needs to be effort in enhancing and protecting privacy and why it must be treated with respect and under full consideration of its significant value for people.

Studies regarding privacy-enhancing techniques revealed that specific recommendations of privacy-aware applications can have a certain persuasive power on users' privacy decisions (e.g., Knijnenburg & Jin, 2013). Since persuasive strategies are considered as a potential solution approach for adequately communicating risk-levels with regard to current privacy states and recommending adapting behavior to the respective level of threat, the findings of Knijnenburg and Jin (2013) will be outlined briefly in the following. The authors (Knijnenburg & Jin, 2013) investigated users' check-in decisions in location-sharing services and in what sense it is possible to support users in making more privacy-aware decisions. Location-sharing applications fulfil social

needs since they enrich the social exchange with friends when talking about current events or recommended locations. As Knijnenburg and Jin (2013) summarize, such location-sharing services may evoke privacy concerns, possibly even more than usual social media applications. According to the authors, this calls for providing the user of such services with more control (i.e. an important factor in the theory of planned behavior, see Chapter 5.3) of disclosed information. However, the problem that has been faced in these circumstances is that more possibilities to control a situation might also result in overstraining the users (Knijnenburg & Jin, 2013). This is indeed a well-known problem, and, as is also the case when giving recommendations that are not liked or desired by the user (see Knijnenburg & Jin, 2013), it can lead to reactance reactions or even to negative feelings (e.g., Fitzsimons & Lehmann, 2004) resulting in preferring disadvantageous behaviors and neglecting the recommended action (Brehm, 1966). According to Brehm's reactance theory (1966), the feeling of reactance is basically grounded in a person's perception of being impaired of freedom and limited decision-making independence. These feelings can result in actions that directly or indirectly restore freedom, evoke aggression against the source of reactance (in this case, privacy support measures), or in changing the attributed appeal of threatened situation (here, self-disclosing without restriction; Brehm, 1966). The strength of reactance toward a privacy support measure depends on the users' individually perceived importance of limited freedom or autonomy with regard to online disclosing decisions as well as on the degree of the loss of freedom (see Dickenberger, 2006). The perception of threatened freedom can be shaped by carefully formulating privacy support messages (e.g., instead of communicating "you have to..." rather use "think about...", see Study 2 and Study 3).

Furthermore, organizations and providers can supply privacy seals or warning labels for secure or insecure content or processes (e.g., Kolb, Bartsch, Volkamer, & Vogt, 2014; LaRose & Rifon, 2007; Rifon, LaRose, & Choi, 2005; LaRose & Rifon, 2006). For users, such seals can be very beneficial at first glance because the cost of searching for information regarding privacy policies decreases and they are able to compare different providers based on privacy protection processes (LaRose & Rifon, 2007). However, as with all promising methods, there is also a downside to privacy seals. Users tend to rely on privacy seals and associate comprehensive protection of privacy with them (e.g., Rifon et al., 2005) although privacy seals might not guarantee extensive privacy protection but

instead indicate the accuracy of one's own privacy policies. A big pitfall of privacy seals is that they claim transparency, but oftentimes it is neglected to reveal the mechanisms of certification so that actual transparency is not given in all cases. Nevertheless, privacy seals can have a persuasive impact on consumers and users of online websites, can increase the intention to disclose information (LaRose & Rifon, 2007) and the expectations of transparent processes of data usage (Rifon et al., 2005), function as heuristic cues (Rifon et al., 2005), and influence the selection of providers for sensitive purchases (Egelman, Tsai, Cranor, & Acquisti, 2009). Following the assumptions of the elaboration likelihood model (ELM; Petty & Cacioppo, 1986), the mental processing of privacy seals can take place via two basic routes of information processing – the central or the peripheral route. If the central route of information processing is activated, characterized through high involvement, available cognitive resources, and the motivation to understand provided information (see also reflective information processing, Schiebener & Brand, 2015; Chapter 3.1), privacy seals might not be perceived as *carte blanche* for unconcerned privacy behavior. It needs to be mentioned that involvement can either be *issue involvement* (e.g., Kiesler, Collins, & Miller, 1969), *ego involvement* (e.g., Rhine & Severance, 1970), related to the personal relevance of an issue for an individual, or *response involvement* (Zimbardo, 1960) referring to the situational importance of an issue and influencing the engagement in a situation or task. In a study on the impact of message framing and issue involvement on specific behavioral attitudes it was revealed that negatively framed messages were more persuasive if participants had high issue involvement, whereas positively formulated messages had a higher persuasive impact on participants with low issue involvement (Maheswaran & Meyers-Levy, 1990). Related to the current work, this might indicate that users with high issue involvement in privacy protection might be more susceptible to risk communication that refers to negative consequences of sensitive data sharing than are users with low involvement. Low-involved users might be more persuadable by positively and consensually framed privacy recommendations. Based on the central route of information processing (according to the ELM), the user would probably engage in a more intense search for information and scrutinizing if being confronted with privacy seals (see LaRose & Rifon, 2007; Petty & Cacioppo, 1986). If the peripheral route is activated, privacy seals can induce trust, safety, and security based on peripheral cues, heuristics, and low extent of

questioning (LaRose & Rifon, 2007). This type of processing information can be compared to the impulsive system for decision-making (see Schiebener & Brand, 2015, Chapter 3.1)

This work aims at contributing to previous findings regarding privacy-enhancing technologies and persuasive methods of shaping people's behavior with respect to online privacy protection. The goal is to combine knowledge concerning advantageous presentation of privacy-related information (see Kelley, Bresee, Cranor, & Reeder, 2009) and the impact of privacy seals and privacy warnings (see Kolb, Bartsch, Volkamer, & Vogt, 2014; LaRose & Rifon, 2007), by considering the opportunities and pitfalls of persuasive communication and its influence on behavioral changes.

8.5 Persuasive Privacy Support

The current work combines the potential of persuasion and nudging in order to find the most advantageous type of privacy support for users of SNSs who want to increase their online privacy on SNSs. Persuasion and nudging are related but still distinct from each other concerning one relevant aspect. Persuasion assumes an intrinsically motivated user who is willing to and aware of a targeted behavioral change (Fogg, 2009). In contrast, nudging is also applied without the user being aware of it or having the intrinsic motivation to change behavior (i.e. a criticism to the concept). This work combines both approaches by drawing on the principle that the user is motivated to change the behavior. Given that, from a psychological perspective, it is extremely important to ensure users' autonomy and well-being when giving privacy suggestions. The advantages as well as the critical aspects of persuasive privacy prompting will be outlined. The following sections describe the characteristics and areas of applications of persuasive strategies (Chapter 8.6) and nudging (Chapter 8.6.1).

8.6 The Construct of Persuasion

This work argues that persuasive privacy support measures can call for users' attention in a privacy-relevant situation (see also Acquisti et al., 2017; Wang et al., 2013). Persuasion is the process of supporting people in reaching a behavioral goal through encouraging the person who is aiming at a behavioral change, for instance, through simplifying required actions (e.g., providing information or examples) or making use of

motivational elements (e.g., positive feedback). Fogg (2003, p. 1) defines persuasion as “(...) an attempt to change attitudes or behaviors or both (without using coercion or deception)”. Persuasive systems aim at users’ behavioral change via motivational and self-monitoring features and triggering behavior (Fogg, 2002, 2009). Persuasive privacy support might especially be helpful for users who have a general desire to protect their privacy but show a lack of skills, triggers, or intentions. Since every person has a basic need for privacy (DeCew, 1997), it seems appropriate to use persuasive strategies for this realm. The effectiveness of persuasive systems has already been demonstrated by previous studies in diverse realms such as health care (Yoganathan & Kajanan, 2013), environmental protection (Kappel & Grechenig, 2009), or enhancing prosocial behavior (Schäwel & Krämer, 2018). Bang, Torstensson, and Katzeff (2006), for example, developed a persuasive game to help people modify their behavior with regard to wasteful energy consumption. In a meta-analysis, Hamari and colleagues (2014) revealed commonly considered persuasive elements being visual (e.g., visualizing the progress) and acoustic feedback (e.g., ambient tones for success) as well as social comparison and support mechanisms (e.g., ranking lists or mutual exchange of constructive feedback). The effectiveness of persuasive strategies might differ among individuals (Kaptein et al., 2012). In light of the theory of planned behavior (Ajzen, 1991) and self-efficacy theory (Bandura, 1997), it should be ensured that the persuasive technology or strategy increases the perceived behavioral control of the particular behavior in order to avoid reactance and increase the likelihood of a behavioral change. If the individual perceives that he/she is not able to control a situation because the required abilities are not present, or the action of interest is too costly in terms of cognitive or time effort, the individual might feel uncomfortable and the likelihood that behavioral triggers work might decrease. Online privacy protection might be perceived as being complex, which can result in insufficient privacy behavior, persuasive strategies might contribute to raising awareness of online privacy and actual privacy-protecting behaviors. In the present study, it is aimed at combining mechanisms of warning messages (see Chapter 8.5) with persuasive strategies. In a study regarding the processing and the impact of privacy warning labels and privacy seals, LaRose and Rifon (2007) found that privacy warnings can increase the perceptions of privacy risks referring to information usage and decrease users’ disclosures to a website (for users with low self-efficacy). LaRose and Rifon (2007) conclude their study

with the suggestion that privacy warnings should include context-dependent recommendations so that the user has a clear picture of the concrete risk and what can be changed in order to minimize the risk. Hence, it was assumed that users who are confronted with privacy interventions indicating privacy risks will disclose less information than users who are not exposed to privacy interventions. Besides the great potential of persuasion, this method bears critical aspects as well. It can be argued that utilizing persuasion in order to make people do things that they would not have done without being exposed to persuasive measures resembles an unethical procedure. However, persuasion as it is referred to in this work refers to behavior increasing an individual's privacy and security without having third-party profits in mind. In addition, people are not simply unknowingly subliminally convinced to buy a product, for example (as it has been oftentimes criticized concerning persuasive advertisement), but they are made aware of potential threats by leaving the decision up to them whether they should act in the way it was recommended.

8.6.1 Nudging and Prompting

During the past few decades, the concepts of nudging and prompting have been utilized and discussed in various disciplines (e.g., energy saving, health, working space, privacy, or nutrition) as well as from different points of view (e.g., Balebako et al., 2011; Balebako & Cranor, 2014; Selinger & White, 2011; Stieglitz, Potthoff, & Kißmer, 2017; Wang, Leon, Scott, Cen, Acquisti, & Cranor, 2013; Wang, Leon, Acquisti, Cranor, Forget, & Sadeh, 2014; Wilkinson, 2013; Ziegeldorf, Henze, Hummen, & Wehrle, 2015). There is a huge potential for using nudges to guide and support users regarding multiple needs and decision situations. However, nudging is an ambivalent topic since it can be understood as a kind of manipulation as well. In the following, the potential of nudging and related ethical considerations will be outlined and transferred to the realm of online privacy protection.

Nudging in terms of user-friendly guiding implies that the intention of a nudge is clear to a user and that he or she is not deceived or misled by it. Hausman and Welch (2010, p. 126) define nudges as “(...) ways of influencing choice without limiting the choice set or making alternatives appreciably costlier in terms of time, trouble, social sanctions, and so forth. They are called for because of flaws in individual decision-

making, and work by making use of those flaws”. Oriented toward modern technology, Meske and Potthoff (2017, p. 2589) define nudges as a “subtle form of using design, information and interaction elements to guide user behavior in digital environments, without restricting the individual’s freedom of choice”. According to Acquisti and colleagues (2017), one has to consider different aspects of nudges for increasing privacy and security, for example, a nudge’s *information* (for a realistic perspective of risks) or its *presentation* (providing necessary contextual cues in the user-interface). Sunstein (2014) provided a collection of the ten most relevant nudges from his point of view, which will be briefly summarized in the following.

The *default nudge* describes a setting in a system that may help the user to make an advantageous decision, for example, regarding sustainability, by printing documents double-sided by default (Sunstein, 2014). This default nudge shows similarities to the idea of privacy-by-design approaches for systems that provide the most advantageous initial situation for the user (see Chapter 8.3). The individual being confronted with a (default) nudge should be informed about the intention of the respective setting and the setting should not exploit the user (Sunstein, 2014). Transferred to SNSs, initial privacy settings allowing postings to be accessible for the public without restriction can be understood as a disadvantageous default nudge (see also Knijnenburg & Kobsa, 2014). The second nudge described by Sunstein (2014) is *simplification* in terms of reducing cognitive effort that is demanded by users for making a decision. Sunstein (2014) argues that reducing complexity can support the usage of systems more intuitively which might result in a more positive user-experience. This is one of the guidelines for the persuasive prompts discussed in this work and is related to Fogg’s persuasive strategy *reduction* suggesting to make complex things easier in terms of reducing information that is not necessarily needed or to translate complex terms into more simple ones (Fogg, 2003). The third relevant nudge described by Sunstein (2014) focuses on the use of *social norms*. This is especially interesting from a social psychological point of view since one determinant for a person’s behavior is the perceived social norm regarding the topic of interest (see Chapter 6.2.2). Sunstein (2014) stresses that people tend to do what other people do or at least what other people think one should do because they want to be liked and accepted by others (Marxwell, 2002). People often adapt to others in order to receive the desired appreciation, which is referred to as *normative social influence* in social

psychology (Nail, MacDonald, & Levy, 2000). Normative social influence does not necessarily change a person's opinion or attitude, but it shapes his or her behavior in a way that corresponds to the perceived social norms (Levine, 1999; Nail, MacDonald & Levy, 2000). Thereby, it does not even matter whether the people, whom one is comparing oneself to, are known peers or unknown strangers (see also Asch, 1956; Cialdini & Goldstein, 2004). As stated earlier (see Chapter 6.2.2), a social norm can shape and determine people's perception of the environment and prevalent opinions and subsequently influence behavior (see also Ajzen, 1991) which might explain the impact of nudges using social norms as argumentation. In line with this, as already stated, Utz and Krämer (2009) also suggested that recommendations stemming from peers are more influential than those stemming from authorities (Chapter 6.2.2), stressing the importance of the perception of other people's and peers' opinion with regard to individual behavioral intentions. A further nudge described by Sunstein (2014) is *increases in ease and convenience*. This means that barriers regarding a decision should be reduced and the execution of behaviors should be presented as easy as possible in order to persuade people to implement them. Elements of persuasion use the same principle, as the occurrence of behavior is described to be more likely if it is perceived to be easily implementable (further relevant elements are behavioral motivation and triggers, cf. Fogg, 2003). *Disclosure* is the fifth type of nudging mentioned by Sunstein (2014), which resembles the guideline of being transparent. It is described as making information regarding a suggestion visible, such as providing nutrition tables or a detailed list of environmental costs associated with the use of an energy-consuming product (Sunstein, 2014; see also Chapter 8.5, Kelley, Bresee, Cranor, & Reeder, 2009). This is also related to the aspect *information* by Acquisti, claiming that users need to be informed about processes that decide what the user is confronted with (2017). The sixth nudge is the most important one regarding the current work, namely, *warnings, graphic, or otherwise (as for cigarettes;* p. 586), also related to the element *presentation* by Acquisti and colleagues (2017). It is argued that warning nudges can catch users' attention, especially if they are designed in a specific noticeable way (e.g., large font, bright colors, bold letters if serious risks are involved). As early as in 2006, Rousseau and Wogalter provided design principles for warning labels, claiming that a label should have a noticeable color, left-sided text, and a frame in order to be recognized. Furthermore, according to Rousseau and Wogalter

(2006), a label should contain the word *warning* in the heading, as well as a description of the threat and potential consequences. However, against the background of reactance research (e.g., Brehm, 1966), the appearance of the word *warning* might not be that beneficial. Users might ignore the warning in terms of a “now more than ever”-mindset (see Devos-Comby & Salovey, 2002) or have negative feelings of powerlessness and a lack of capabilities to solve the situation. Furthermore, Sunstein (2014) argues that “attention is a scarce resource” (p. 586) and that the risk of people discounting the warning is given. Therefore, Sunstein (2014) suggests investigating the effects of positive and concrete warnings (e.g., with recommendations for alternative actions), which is done in the current work (see Study 3 and Study 4).

It can be deduced that persuasive privacy prompts should be presented as encouraging suggestions instead of demotivating paternalistic demands in order to sufficiently encourage users accepting a system’s suggestion (Sunstein, 2014) and preserving users’ autonomy. Research in the health-care realm has shown similar effects regarding cigarette warning labels. Warnings without recommendations for actions seed reactance and negative feelings (see also protection motivation theory; Rogers, 1975) instead of helping people quit smoking. Privacy nudges have already been proposed as a promising measure for improving users’ online privacy on Facebook (e.g., Acquisti et al., 2017; Wang et al., 2013). But still, underlying psychological mechanisms that influence the impact of privacy nudges are mainly unknown. In the following, research on nudges, directly referring to privacy protection, are presented and discussed, focusing on lessons that have been learned and open challenges to be solved.

Zhang and Xu (2016) investigated privacy nudges for mobile applications to assist in the privacy decision-making processes of users. Exploring two different types of privacy nudges, namely, a *frequency nudge* (e.g., “the app reads contacts every 6 hours”) and a *social nudge* (e.g., “possibility to read contacts: 64% of users turn on”), revealed that privacy nudges have an influence on privacy attitudes. It was concluded that privacy nudges, which are integrated in an app and visible during the process of installation, can help the users in terms of understanding privacy conditions and can make privacy decisions easier (Zhang & Xu, 2016). This approach focused on privacy policies and online security rather than on self-generated content by the users. By contrast, Wang and colleagues (2013) examined the effects of privacy nudging regarding user-generated

inputs on an SNS. The authors developed three nudges for the social network Facebook, namely, a *profile picture nudge* (randomly presenting Facebook friends who would see the posting), a *timer nudge* (delay before a posting is published), and a *sentiment nudge* (informing the user that the posting can be perceived negatively). It was revealed that participants posted less content after receiving privacy nudges (Wang et al., 2013). The most promising nudge was the profile picture nudge supporting the assumption that the confrontation with a specific audience can influence users' disclosures and privacy behavior (Vitak, 2012; Wang et al., 2013). However, the nudges by Wang and colleagues (2013) were neither adapted to users' characteristics nor to the dimensions of privacy. The current thesis argues that nudges can be improved if they take the sensitive information itself, the related dimension of privacy, and user-centered variables into consideration.

Ziegeldorf, Henze, Hummen, and Wehrle (2016) also proposed a comparison-based privacy measure as being a more promising measure than privacy nudges like those by Wang and colleagues (2013). They argue that the disadvantage of privacy nudges, as proposed by Wang and colleagues (2013), is the required understanding about which behavior is risky as well as a lack of individuality and appropriateness in nudging. The authors suggest a comparison-based privacy protection measure that compares a user's amount of self-disclosure and other online behavioral patterns to those of his or her friends or other groups for comparison. The advantage of this approach is that no ground truth or explicit rules for defining sensitive information are needed (Ziegeldorf, Henze, Hummen, & Wehrle, 2016). However, comparing one's own privacy behavior with the behavior of other people does not guarantee best privacy practice. Other users' behavior can be rooted in false evaluations of privacy, missing privacy literacy, or individual privacy needs that might differ from those needs of other persons, which presents the danger of reinforcing inadequate privacy behavior. Of course, if the peer group, to whom one is comparing oneself to, shows cautious and reflected privacy behavior, this approach is a promising idea. However, this would require other users to be aware of privacy risks and be literate in terms of protective behavior.

In the case of this work, a privacy nudge is defined as a suggestion for a behavioral change in a specific situation (e.g., online self-disclosure) of endangerment (e.g. high likelihood of negative consequences) with the aim of protecting users' privacy through

providing supportive prompts. It is focused on a prompt's presentation (appearing context-related and in a certain style) and provided information (give reasons for suggested behavior) in order to help users to make wise privacy decisions and be informed about privacy risks in real-time. Furthermore, principles of persuasion are closely related to nudging in this work; persuasive prompting will be considered as a type of nudging (see Study 3 and Study 4).

In contrast to the supportive and guiding nature of persuasive prompting, manipulative measures would neither inform the user about intent and aims nor try to meet users' needs. In social media contexts, scholars use the term *digital nudging* in order to address the digitalized nature of this measure more clearly. Especially because of the complexity and variety of available information and possible threats, it is a great opportunity to provide user-centered *digital nudges* in order to trigger advantageous and, if possible, rational decision-making. In the current case, advantageous decision-making means to make privacy-aware decisions through reducing the likelihood of being exposed to privacy harms after sensitive information disclosure.

8.6.2 Opportunities to Combine Persuasion and Prompting for Online Privacy

Protection

In this dissertation it is assumed that persuasive privacy prompts might be an adequate concept for raising users' awareness of online privacy threats stemming from imprudent online behavior. Therefore, it needs to be figured out how persuasive prompts or other intervening visual cues (see Study 4) can be designed and presented in a way that does not induce reactance or cause negative feelings. It has been argued that making decisions under uncertain risk conditions (e.g., self-disclose to an unknown audience or not) can lead to mindlessness in association with considering heuristics (see Chapter 3.1). In social psychology, heuristics are defined as mental shortcuts that are used to understand, categorize, and judge the environment (Kahneman, 2011). Basically, heuristics are necessary for people to survive in their social environments and to adapt themselves to basic circumstances. Still, heuristics can be dangerous as well, for instance, if people derive false mental shortcuts that then affect a person's behavior. For example, based on mindlessness and the usage of heuristics, users of online social services might

provide personal information to websites or networks without questioning whether it is actually needed for respective processes. In fact, a lot of information is collected by institutions like Google and Facebook which might not necessarily be needed to provide their services (Heurix, Zimmermann, Neubauer, & Fenz, 2015). A warning in terms of a privacy intervention can release users from their mindlessness in specific situations and induce more awareness for privacy threats (which might not be possible by solely relying on educative approaches since privacy literacy might not be retrievable at any time, depending on situational cues, for instance). Following the elaboration likelihood model by Petty and Cacioppo (1986; see also Chapter 8.5), a persuasive warning label would call users' attention and activate the central route of information processing resulting in more elaborated decisions. Originally, the elaboration of information as it is described in the elaboration likelihood model referred to the elaboration of messages with strong versus weak arguments or messages that are transmitted via an attractive/trustworthy versus unattractive/not trustworthy communicator resulting either in persistent attitude changes or temporary weak attitude changes (see Petty & Cacioppo, 1986). As already stated, depending on users' involvement and individual motivation to engage in the behavior of interest (here, privacy protection), persuasive support messages as they are considered in the current work can be processed in either a more or a less elaborated way.

This work focuses on effects of system-based persuasive privacy prompts on actual privacy behavior and psychological variables that influence these effects, depending on the persuasive style (see Kaptein et al., 2012; Fogg, 2009) and the information provided within a prompt (see Study 1; Acquisti et al., 2017). More precisely, it is aimed at analyzing the influence of system-based persuasive privacy prompts that are formulated alongside specific persuasive styles (i.e. authority or consensus) on users' actual privacy behavior on an SNS (i.e. self-disclosure or information withdrawal). Furthermore, it will be examined whether persuasive privacy prompts will be more effective (i.e. users provide less sensitive information) if prompts contain reasons for respective suggestions. The following chapter summarizes pivotal approaches that have been outlined in this work and will be considered for deriving hypotheses, discussing findings and providing theoretical and practical implications of this work.

9 Summary of Underlying Theories and Approaches

The following section summarizes the key assumptions of the approaches and theories that are considered in the present work, and critically reflects on advantages and barriers for analyzing users' online privacy behavior on SNSs.

As explained in Chapter 5.1, the privacy paradox (Barnes, 2006) was a valid assumption, claiming that users' privacy behavior cannot be explained by their privacy attitudes and concerns. However, this paradox was addressed by scholars from various theoretical and methodological viewpoints revealing new perspectives on users' seemingly paradoxical privacy behavior.

One approach that is considered to explain why people tend to disclose sensitive information about themselves although it might entail negative consequences is the privacy calculus claiming that people weigh risks and benefits of self-disclosure in order to decide whether to disclose personal information or not (Culnan & Armstrong, 1999). Krasnova, Spiekermann, Koroleva, and Hilebrand (2010) initially used this approach for examining privacy behavior on SNSs. They revealed that perceived risks were related to a less comprehensive, and perceived benefits were related to a more comprehensive profile on a specific SNS. However, this approach bears criticism as well, since the privacy calculus assumes the actor to be rational although human beings are not able to act and decide rationally under all conceivable conditions (e.g., Acquisti, et al., 2017). Nevertheless, its assumption that people are driven by the anticipation of benefits, was also addressed by Trepte and Teutsch (2016) who stated the *gratification hypothesis* as one attempt for solving the privacy paradox (see Chapter 5.1). The gratification hypothesis, as well as the privacy calculus, states that people disclose themselves if benefits of self-disclosure are anticipated, and, if they are more salient than potential risks. However, Trepte and Teutsch (2016) indicate that users are not fully rational actors but might be driven by heuristics and subjective perceptions of benefits. This assumption is also indicated in the protection motivation theory, which states that a person's decision to perform an action (here, self-disclosure or self-withdrawal) is based on individual subjective evaluations of threat and coping capabilities (Rogers, 1975).

The theory of planned behavior was used to explain users' seemingly paradox privacy behavior as well (see Chapter 5.3). In particular, Dienlin and Trepte (2015) demonstrated that, if privacy is operationalized adequately (i.e. considering different

dimensions of privacy), and considered comprehensively (i.e. examining behavioral intentions *and* attitudes), a person's privacy behavior occurs less paradox and more reasonable. Basically, the theory of planned behavior (Ajzen, 1991) explains reasoned actions which are based on an interplay of attitudes, perceived social norms and perceived control over an action which influences persons' behavioral intentions and subsequently their actual behavior. Since this theory is predominantly considered for explaining elaborated and reasoned behavior, concrete short-term and affective behavioral elements are missing within the model. However, although "the TPB emphasises the controlled aspects of human information processing and decision-making" (Ajzen, 2011, p. 1116), Ajzen (2011) points out that emotional and affective states are actually included in his theory in terms of triggering particular behavioral attitudes and intentions which might be salient and easily accessible in emotional situations. Thus, although the theory of planned behavior mainly aims at explaining "goal-directed" (Ajzen, 2011, p. 1116) behavior, this does not implicate that the actor is understood as being rational and detached from emotions. Ajzen (2011) stresses that perceived norms, attitudes, and intentions are also not free from subjective beliefs and that they represent the users' perception, which cannot be completely rational since human beings perceive the environment filtered through their own characteristics. In sum, the theory of planned behavior can be considered as analyzing "goal-directed" and reasoned behavior, which implicitly covers persons' irrationality and emotionality.

In contrast to the theory of planned behavior (Ajzen,1991) and the privacy calculus (Culnan & Armstrong, 1999), the protection motivation theory (Rogers, 1975) assumes that a current risk has been communicated to a person, which then influences his or her protection motivation and protective behavior (see Chapter 5.4). The core elements within the protection motivation theory are the source of the risk-related information, the cognitive evaluation of the threat, and the chosen mode to cope with the threat (Floyd, Prentice-Dunn, & Rogers, 2000; Rogers, 1975). Dienlin and Metzger (2016) investigated the privacy calculus in the realm of SNSs, referring to assumptions of the protection motivation theory (Rogers, 1975). In their study, Dienlin and Metzger (2016) demonstrated that privacy concerns predict self-withdrawal (but also self-disclosure) behaviors (whereas anticipated benefits solely influence self-disclosure). Following the authors, this is in line with the protection motivation theory, which, according to Dienlin

and Metzger (2016), claims that solely the perception of concerns (instead of anticipated rewards) leads to protection motivation. However, the threat appraisal within the protection motivation theory, which either increases or diminishes the likelihood that the non-protective behavior will be implemented, does not only comprise of concerns (i.e. negative evaluations) but also of maladaptive response rewards. The threat appraisal assesses the maladaptive behavioral response (see Floyd, Prentice-Dunn, & Rogers, 2000). If the individual perceives great rewards of conducting the non-protective behavior, he or she will more likely select the maladaptive response, indicating that protection motivation would be low, and the unprotected behavior would be conducted (e.g., anticipation of many *likes* leads to self-disclosure). In contrast, the perceived threat will decrease the likelihood that an individual selects the maladaptive coping, indicating that the non-protective behavior would not be conducted. Thus, concerns are not the only driving factor within this theory but they indeed have strong influence on protection motivation and protective behavior.

The current thesis considers the most decisive elements of the mentioned approaches within the empirical studies, attempting to explain users' online privacy behavior. This work explores requirements for system-based privacy support measures (Study 1), the motives to opt-out from an SNS, the influence of intrapersonal factors on the intention to opt-out (i.e. impression management motivation, privacy concerns) as well as the relation between general self-disclosing activities and the attitudes and intentions regarding opting-out (Study 2). Further, Study 3 and Study 4 assume the impact of system-based privacy support measures (i.e. persuasive privacy prompts and visual cues) on users' privacy behavior to be moderated by individual characteristics and needs, namely, the need for privacy, the need for popularity, grandiose narcissism, vulnerable narcissism, self-control, and privacy concerns. Furthermore, this work hypothesizes, that the susceptibility to particular persuasive styles and perceived privacy norms also moderate the impact of privacy interventions on the privacy behavior. Moreover, privacy concerns, attitudes, and intentions are assumed to influence users' privacy behavior. Further, it is asked, whether the presence of system-based privacy support influences users' perceived privacy control, affect, or the user experience. Additionally, this work assumes that the presence of system-based privacy support might have an influence on the weighing of risks and benefits related to self-disclosure (Study 4). Finally, the need

for cognition is hypothesized to influence the weighing of risks and benefits related to online self-disclosure (Study 4).

In the following, four empirical studies analyzing the proposed relations are outlined, and discussed. Each chapter provides limitations and future directions. Figure 2 provides an overview of investigated variables and hypothesized relations which will be referred to in the following sections.

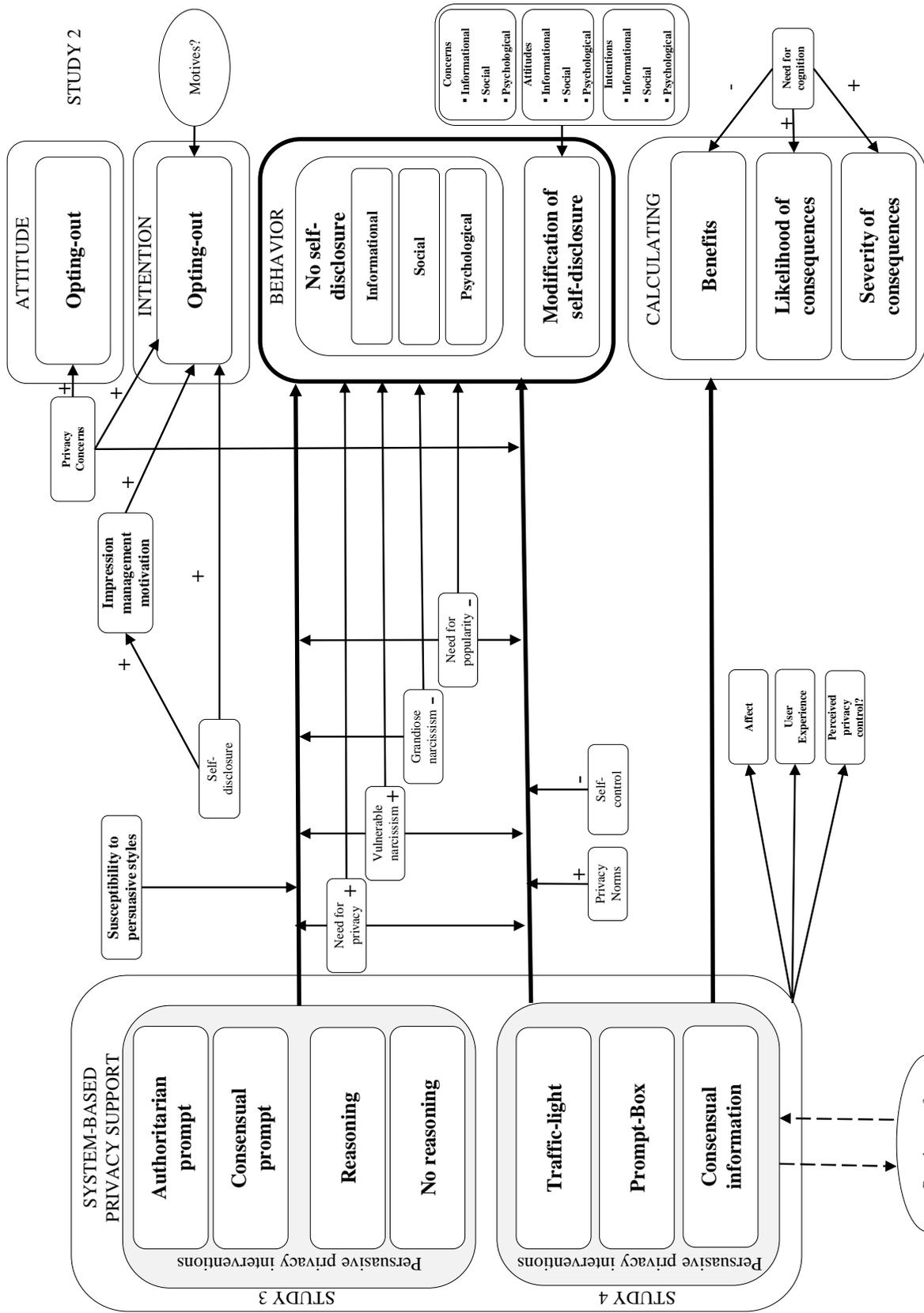


Figure 2: Hypothesized overarching research model.

III REQUIREMENTS FOR USER-CENTERED PRIVACY SUPPORT

10 Study 1: Paving the Way for Technical Privacy Support - A Qualitative Study of Users' Intentions to Engage in Online Privacy Protection

As outlined in Chapter 2.2, users of SNSs tend to disclose sensitive personal information on the Internet without utilizing privacy protective measures albeit privacy threats might occur. While there is an impressive body of research about the benefits of online self-disclosure (see Chapter 4.1), there is still a lack of knowledge of how to empower users in protecting their privacy. Building on key assumptions of the theory of planned behavior (Ajzen, 1991, see Chapter 5.3), Study 1 qualitatively addresses users' desires for technical privacy support, the questions of how to increase people's intentions to reflect on risky online actions, and how to induce conscious online behavior by means of technical privacy support. One system-based solution for raising situational privacy awareness is utilizing privacy nudges. As explained in Chapter 8.6.1, privacy nudges can increase users' attention in dangerous situations of sensitive self-disclosure (Acquisti et al. 2017; Wang et al. 2013) by triggering them at crucial points of time and guiding behavioral outcomes in terms of privacy-aware practices (Acquisti, 2009). Given that most nudges are neither adapted to the users themselves nor to the dimension of privacy that is going to be violated, these prompts might be experienced as random warnings instead of efficient privacy support by users. So far, requirement-elicitation with a view to application – considering a concrete concept of a potential measure as well as users' individual characteristics from an interdisciplinary view, combining psychology and software engineering – is missing. This work argues that current approaches need to be expanded by considering the individuals themselves (see Chapter 6.2) and the multidimensional concept of privacy (see Chapter 2.1). Therefore, Study 1 reflects on methods for encouraging users to improve privacy-protecting practices and requirement elicitation for privacy-supportive and user-centered nudging.

10.1 The Importance of Protecting Online Privacy

As described in Chapter 2.1, privacy is a fundamental human right and need for making self-determined decisions (DeCew, 1997), stressing the necessity to maintain privacy in offline environments as well as on the Internet. In order to support users in their privacy decisions it is crucial to point out potential risks of insecure privacy behavior and in line with that, demonstrate in how far particular self-disclosures can be dangerous (see Chapter 3). Users' disclosures and behavioral patterns on SNSs can be utilized by third parties in order to predict personal characteristics (e.g., Kosinski, Stillwell, & Graepel, 2013) or spread by other users and cause rumors and psychological stress (e.g., Wang et al., 2013; see Chapter 1 and Chapter 2.2). However, estimating the likelihood and severity of privacy risks and negative consequences to occur is still a difficult task for users (Baek, Kim, & Bae, 2014; Moll, Pieschl, & Bromme, 2014, see Chapter 3), making privacy support measures that are able to point out these factors more relevant than ever.

Since the overarching goal of this dissertation is to explore how to raise users' privacy awareness and – even more important – how to evoke protection intentions and induce protective behaviors, it is necessary to learn about users' current levels of (perceived) consciousness regarding online privacy issues. Therefore, the research questions of Study 1 refer to the requirements toward a future protection measure. This feature-based background delimits the current study from previous work that focuses on describing and explaining users' behavior instead of developing adapted support features. To begin with, Study 1 aims at shedding light on users' current privacy awareness and intentions by addressing the following research question:

Research Question 1 (RQ1): (To what extent) are users of SNSs aware of online privacy?

10.2 Motives for Utilizing Privacy Protective Measures

Privacy concerns are an important driver for engaging in privacy protection (e.g., Bartsch & Dienlin, 2016; Dienlin & Trepte, 2015; Osatuyi, 2015; Vitak, 2015, see Chapter 6.3.3) and consequently an element that can contribute to the theory of planned behavior (Ajzen, 1991) in order to predicting behavior even more comprehensively

(Dienlin & Trepte, 2015). For developing privacy protection measures, it is indispensable to learn about users' concerns and, consequently, to derive issues that could be risky but are still unknown to the users. Unknown risks could evoke false perceptions, which in turn distort perceived control (see Chapter 8.6). By asking people about motives and reasons for protecting themselves, the perceived consequences of not engaging in privacy protection and the gaps or misunderstandings concerning adequate measures of privacy protection can be derived. Additionally, it can be figured out how participants perceive their own risks and levels of control. This is important since it has recently been argued that users' perception of privacy is not always equal to their actual privacy state (e.g., Dienlin, 2014). Covering these issues, the second research question was:

Research Question 2 (RQ2): (Whereof) do users want to be protected and what are their motives and reasons for required protection?

10.3 Users' Perception of their Own Privacy Knowledge

As mentioned in Chapter 7.2, the social network Facebook provides basic security information regarding hacking, creating secure passwords and data encryption processes. However, comprehensive individual privacy support for users seems to be lacking and the impact of provided security information remains unanswered. Among others, this might be one reason for Facebook users creating alternative privacy strategies going beyond the usual Facebook security settings. The most prominent methods, namely super-logout, whitewalling, and social steganography (boyd 2010; boyd & Marwick 2011) were referred to in Chapter 7.2. Apparently, these strategies help users to feel protected. Despite it is actually not possible to avoid online privacy risks completely through logging off, deleting content, or encoding messages it is nevertheless considered as potential privacy increasing method by some users (boyd, 2010; boyd & Hargittai, 2010). However, sensitive information that is deleted or encoded is still online for a period of time and logging out is only a temporal solution.

Privacy knowledge (i.e. privacy literacy) is also related to people's perceived control, which is a crucial factor influencing behavior. When aiming to support Internet users through technical privacy support it is helpful to get an impression of their current (perceived) states of literacy. Moreover, reflecting on problems of current privacy measures is one important step of requirement elicitation for a new measure or system.

Therefore, the third research question was as follows:

Research Question 3 (RQ3): Do users (think that they) know how to monitor and protect their privacy and do they know and use specific measures (e.g., the super-logoff) for this?

10.4 Elicitation of Requirements

Besides people's intentions and attitudes, their psychological needs for competence, autonomy, and relatedness can influence their engagement in a behavior (Ryan & Deci 2000; Yap & Gaur 2016). Privacy protective measures that are consulted for supporting the process of changing behavior (from unaware to aware privacy behavior) should be able to satisfy these needs. As outlined in Chapter 8.6.1, applying persuasive strategies might be promising to advance the approach of digital nudging aimed at guiding people's privacy behavior (e.g., Fogg, 2009; Kaptein et al., 2012).

In contrast to the goals of PET as they were described in Chapter 8, which mainly aim at protecting security (i.e. informational privacy), this work additionally aims at covering the multidimensionality of privacy by also considering social and psychological privacy (see Burgoon, 1982, Chapter 2.1).

Therefore, with a view to application, the consideration of users' needs and requirements will help to derive suggestions and guidelines for future privacy protection approaches. According to the theory of planned behavior (Ajzen, 1991), users' attitudes and behavioral intentions regarding privacy protection methods are correlated with the adoption of these methods. More precisely, Dienlin and Trepte (2015) showed that privacy attitudes influence privacy intentions, which are a pivotal factor for actual privacy behavior. Therefore, it is particularly important to ask participants to reflect upon which methods for modifying online privacy behavior they would accept and use. Furthermore, it is valuable to gain knowledge about characteristics that would probably not be accepted. Hence, the following crucial research question was formulated:

Research Question 4 (RQ4): Which features should a privacy support application (not) provide in order to get accepted and adopted by users?

10.5 Method

Based on an interview guide referring to the four research questions, ten in-depth interviews with SNS users were conducted. Interviews took between 45 and 60 minutes and were recorded and transcribed. Transcribed interviews were examined with the software MAXQDA12. The study was approved by a local ethics committee.

Participants were asked about their online privacy and their opinions about the concept of a technical privacy support measure. The first and second research question were addressed quite openly. For the third research question, printed screenshots explaining the procedure of the super-logout were prepared in order to talk about this measure even if participants did not know it. However, at first, participants were asked whether they knew the procedure or not without seeing the screenshots. For the fourth research question, users were asked to think aloud of a perfect SNS including privacy measures without giving them any instructions or constraints. Afterwards, the idea of persuasive privacy support messages was introduced by explaining the hypothetical functionality and giving an example of a system's privacy message ("You are going to provide sensitive information. Do you really want to continue?").

Analyses were conducted based on semantic categories (codes) relating to the research questions (see Mayring 2010). The code system was constructed via a mixed method. The basic structure was defined alongside the research questions and previous research findings, before conducting the interviews. During qualitative analyses, the predefined codes were modified and some were excluded because they were not pivotal for the underlying main questions. This was done by exploring the transcribed interviews line-by-line. Four final main codes; (1) *privacy awareness*, (2) *worries and perceived consequences*, (3) *privacy knowledge*, (4) *acceptance of technical privacy support*, which are divisible into particular sub-codes, were developed. Table 1 gives an overview of all codes and sub-codes according to respective research questions.

Table 1

Overview of all codes related to the research questions (Study 1).

Research questions and guiding questions	Codes
<p>RQ1: (To what extent) are users of SNSs aware of online privacy?</p> <ul style="list-style-type: none"> - Do users think about their privacy? - How do they evaluate their privacy behavior? - Can they estimate the range of their contributions? - Do they feel safe? If not, why not? 	<p>Privacy awareness (main code)</p> <ul style="list-style-type: none"> - General awareness - Perceived behavior / self-evaluation - Perceived range - Perceived safety
<p>RQ2: (Whereof) do users want to be protected and what are their motives and reasons for required protection?</p> <ul style="list-style-type: none"> - What are the perceived consequences and risks? <ul style="list-style-type: none"> - Based on the company (Facebook) - Based on 3rd parties (data theft, advertising) - Based on other users (mobbing, fraud, etc.) - Have the users already experienced negative consequences? 	<p>Worries and perceived consequences (main code)</p> <ul style="list-style-type: none"> - General consequences <ul style="list-style-type: none"> - Consequences: Facebook - Consequences: 3rd Parties - Consequences: Other users - Experienced negative consequences
<p>RQ3: Do users (think that they) know how to protect/monitor their privacy and do they know specific measures for this?</p> <ul style="list-style-type: none"> - Do users have knowledge regarding online privacy protection? <ul style="list-style-type: none"> - Do they know/use whitewalling? - Do they know/use social steganography? - Do they know/use the super-logoff? - Do they know/use Facebook measures 	<p>Privacy knowledge (main code)</p> <ul style="list-style-type: none"> - General knowledge <ul style="list-style-type: none"> - Whitewalling - Social steganography - Super-logoff - Facebook measures
<p>RQ4: Which characteristics should a privacy-aware SNS or a privacy support measure (<i>not</i>) provide in order to get accepted and adopted by users?</p> <ul style="list-style-type: none"> - Which characteristics/properties and functionalities do participants want/need /accept? - Which characteristics/properties and functionalities do participants think, other users want/need/accept? - Which characteristics/properties and functionalities do participants not want/need/accept? - Which characteristics/properties and functionalities do participants think, other users don't want/need/accept? 	<p>Acceptance of technical privacy support (main code)</p> <ul style="list-style-type: none"> - Personal acceptance - Perceived acceptance - Not accepted properties - Perceived not accepted properties

In order to test the reliability of the codes, a second rater coded five complete transcripts, following the defined code system. Besides the code system, the second rater was provided with explanations referring to every code and sub-code. Agreement between coders was only reached if at least 90% of an identified text passage concurred exactly. According to Landis and Koch (1977), and to Altman (1991), the intercoder-reliability revealed moderate ($\kappa = .41-.60$) to substantial ($\kappa = .61-.80$) kappa (κ) and agreement (%) values ($\kappa_1 = 0.52$ [54.74%], $\kappa_2 = 0.55$ [57.78%], $\kappa_3 = 0.62$ [64.35%], $\kappa_4 = 0.50$ [53.00%], $\kappa_5 = 0.51$ [54.00%]).

Before conducting the interviews, participants were informed about the topic, conditions, and procedure of the interview, including the fact that they could cancel the interview at any time and that the conversations were going to be recorded and transcribed. Subsequent to the interviews, participants were informed about the topic and research questions of this study in more detail.

Recruitment and sample

Participants ($N = 10$) were recruited through a forum of the university and the social network Facebook. Following Ritchie and colleagues (2014), this sample size is sufficient for qualitative examinations such as conducting in-depth interviews. Interviewees received either 10 euros or a student incentive for participating. Seven participants were female. They were aged between 19 and 27 years, $M = 23.00$, $SD = 3.01$. Most of them were students ($n = 7$), two of them were research associates, one was a teacher. The precondition for participating was to have a Facebook account or to have had one in the past. Nine persons were Facebook users and one participant was an ex-Facebook user. All of them were active on additional social online networks or messaging applications such as WhatsApp ($n = 9$), Instagram ($n = 8$), Snapchat ($n = 2$), Threema ($n = 2$), Twitter ($n = 2$), Pinterest ($n = 2$), LinkedIn ($n = 1$), ResearchGate ($n = 1$), Tumblr ($n = 1$), or Google+ ($n = 1$).

10.6 Results

In the following, the results of qualitative investigations are summarized alongside the stated research questions. Participants' age and gender is indicated for each statement.

Privacy awareness (RQ1)

The first research question addressed interviewees' current level of privacy awareness. Participants reported being aware of the importance of one's online privacy. On the one hand, their awareness referred to general norms and on the other hand, to specific types of information, as the following quotations demonstrate:

“Not everyone must know about it.” (female, 27 years)

“That's the most important thing [to keep privacy in mind].” (male, 27 years)

“I don’t disclose my last name.” (male, 21 years)

These statements represent users’ attitudes referring to the dimension of informational privacy. However, most statements demonstrate that even though participants sporadically reflect on what (personal) information they disclose through statements like “Recently I checked, what is still on my Facebook profile from the past.” Persons who explicitly claimed to be aware of privacy issues said for example:

“Some people save their passwords, but I do not. I must type it in every time I want to login [i.e. informational privacy]. Because I learned that this is secure [i.e. social norms]” (female, 27 years)

“I am also aware that Facebook and WhatsApp are somehow connected. But as I said, I think it is exaggerated having too many worries about it. It's part of Facebook. I use it anyway.” (male, 27 years)

These statements are not evidence of comprehensive privacy awareness (as the participants thought) but rather of general thoughts on privacy (related to social norms) that do not trigger comprehensive engagement in privacy protection but a superficial reflection on a topic of public interest. One person did not seem to be aware of privacy at all, saying:

“I think that my profile is completely public. But to be honest – I don’t even know exactly.” (male, 21 years)

This mirrors the findings by Trepte and Masur (2016) that many people do not know whether their profiles are publicly searchable. Despite the fact most participants claimed to be aware of privacy issues, some respondents ($n = 5$) even suppressed possible risks by ignoring or trivializing them:

“Yes, it could become dangerous. But actually, one ignores that in everyday life.” (male, 21 years)

“Well maybe I am too naive. I did not think much about that privacy thing before.” (male, 21 years)

“I’m a bit uninformed because I never read the policies. If I would read it, then I would be well informed... I guess it would be sufficient if one would read it?” (female, 23 years)

Altogether, interviewees' level of privacy awareness was found to be not sufficiently high to result in conscious online privacy behavior. Conscious online privacy behavior would require a higher level of awareness in order to pronounce and increase the intention to engage in privacy protection. But this was lacking. The observation after this first part of the interview was that participants considered the topic of privacy protection merely on the surface, whereby respective attitudes referred to internalized social norms.

Worries and perceived consequences (RQ2)

In order to analyze users' privacy concerns, they were asked whether they were afraid of online privacy violations. Most participants ($n = 8$) were afraid of negative consequences affecting their social lives (online as well as offline), such as cyber-mobbing or elimination of (Facebook-) friendships, as well as exclusion from social groups. Referring to perceived consequences of laissez-faire privacy behavior with regard to one's social life, one participant said:

“It could be dangerous to publish personal stuff because it could go wrong. Other users could say that my photo looks stupid or that I get no likes. I actually have no experiences with mobbing but every time when you upload something there is the hazard of being excluded or disliked.” (male, 21 years)

As demonstrated by this quotation, as well as by the next one, people are concerned about being excluded or not liked (anymore) by other users:

“I am actually afraid of what other users can get to know about me. For example, when I like something on a newspaper website and I am logged in with my Facebook account at the same time, others could see what I like or comment on the news site. If they don't agree with me it could become an uncomfortable situation.” (male, 27 years).

Furthermore, anxieties concerning online firestorms, hate speech dynamics and cyber-mobbing were stated by six persons as well, whereby the likelihood of actually becoming a victim of a firestorm or mobbing is assigned to other users rather than to oneself:

“Moreover there is the fear of a firestorm, which could arise if you post your personal opinion in the network. I don't do that!” (male, 21 years)

“One is afraid of negative responses.” (female, 23 years)

“Especially for teenagers that’s an issue.” (male, 21 years)

These statements indicate a third-person effect in line with the findings by Baek, Kim, and Bae (2014).

In contrast to anxieties on a horizontal level, concerns on a vertical level referring to third parties misusing their data were considered as an unpleasant but necessary condition. This was described as a general concern that one has to live with. In line with this, perceived control regarding privacy harms based on third parties was considered as very low.

Five persons mentioned consequences that could arise based on third parties, but in the sense of the possibility that consequences could occur instead of pointing out, that they are directly afraid of it. For example, one person stated:

“[...] They pick you for particular advertisement and news. Through your likes you somehow give up your privacy.” (male, 21 years)

From this quote, it can be derived that this particular person knows (at least generally) about the effects and consequences of online actions. Furthermore, he stated:

“In the past, one thought that one has more privacy, but nowadays there is no real privacy.” (male, 21 years)

But following the person’s next quote it emerges that he nevertheless does not pay attention to what he provides to third parties and, in line with that, his concerns do not cause cautious privacy behavior:

“You are still doing it. I don’t know why. I would say, for instance, if there is a shoe that I like, of which I think ‘awesome’ then I do click the like-button, but I don’t know why.” (male, 21 years)

Persuasive privacy messages could help those persons whose behavioral intention is not sufficiently pronounced as is the case for this interviewee because it can raise awareness and situational motivation (e.g., Acquisti, 2009, Acquisti et al., 2017). One other person mentioned possible consequences referring to third parties by saying:

“I know a little bit about it, for example, that your personal profile is sold to other companies, for \$42 they said in the news. And in general you know, when you sign in [to a SNS] and read the terms of condition, you lose the rights to your photos, if you publish them.” (male, 20 years)

This person also stated having some knowledge concerning possible consequences based on third parties and he indeed felt a little uncomfortable about it:

“Of course you try to act like it doesn’t matter to you, but it’s a little frightening and you also feel uncomfortable, somehow.” (male, 20 years)

But in the end, he was either not seriously afraid or her intentions to change behavior were not incisive, probably due to a biased view of his own risk assessment (see Baek, Kim, & Bae, 2014):

“This couldn’t happen to me, because I’m not a very active user. But in general, it can happen to people.” (male, 20 years)

A privacy alert that is persuasive could help to adjust such biased perceptions by intervening in critical situations of sensitive information disclosure.

Moreover, participants believed to have no influence on whether their data will be used or forwarded by institutions and providers like Facebook or Google anyway. Thus, they fade out the risks concerning third parties, noticeable through statements like:

“I think that they know far too much about me and thus, they actually have power over me. They have all the data and theoretically can sell it. I believe that this is forbidden, but, they could do it. This is a bit creepy.” (female, 23 years)

Some participants even reported about earlier personal experiences that led to feelings of regret, which for most users would be the trigger to change something;

“Of course, at that time I didn’t have constant control, because it was a new medium (...). And, of course, at that time I *liked* many things for which I am almost ashamed now. But I do think that I have it under control nowadays.” (male, 20 years)

“One can provide almost everything on Facebook nowadays. Favored music, movies, favorite news... and I really don’t endorse this. But in the past, when I was younger, I did that. I filled in everything – I *like* this and that, this is my football club.” (male, 20 years)

In line with the assumptions of the theory of planned behavior (Ajzen 1991), the lack of perceived control results in a lack of behavioral intentions and required protective behavior. Following participants’ reports, perceived consequences that could hypothetically affect their social lives and relationships indeed influence the way some of them behave, for instance, in terms of not sharing personal opinions on a specific topic

if they perceive the disclosure to be inappropriate (but it might not be evaluated as such by others). However, foregoing posting one's opinion on a single issue only once or twice does not imply that one is fully engaged in privacy protection. There is still further information disclosed concerning other topics and additional networks are used to disclose as well (all interviewees were registered in at least one additional social network). Users' perception that other persons are more endangered than they are themselves indicates a third-person effect on the one hand and a lack of awareness and knowledge on the other hand. In sum, interviews revealed that participants are indeed afraid of negative consequences of online disclosure on a general level but there seems to be a barrier that hinders them from converting these fears into constant privacy protective behaviors. Technical privacy support measures need to break through this behavioral barrier.

Perceived privacy knowledge (RQ3)

Previous research (e.g., Bartsch & Dienlin 2016) was underpinned in the way that interviews revealed that *if* users do have some privacy knowledge (privacy literacy) they tend to behave in a more secure way than if they do not. For example, one person who shared some key points of his privacy knowledge said:

“You can decide whether to share something with the public or with a smaller group, e.g. friends or friends of friends. You can do this for every posting and every photo. One can try to keep everything at least a little private. The phone number for example – Facebook doesn't need it.” (male, 20 years)

This interviewee actually did not provide his phone number but carefully decided which information to publish and which not. Furthermore, persons claiming to have privacy knowledge tend to have an increased general willingness to learn about new methods for protecting privacy like the super-logoff or whitewalling and would be interested in testing such measures as well:

Ok, the account is deactivated but not deleted? You can reactivate it and then the data are back again? [...] I find it quite good, actually.” [referring to the super-logoff] (female, 27 years)

In total, two persons knew the procedure of the super-logoff but were not familiar with the concrete wording. One participant actually performed the procedure:

“I know it somehow, I guess. I had an account which I wanted to delete but it was complicated. Facebook told me that it will be deleted after 14 days.” (male, 20 years)

Three participants also performed a light version of whitewalling but again, without knowing this term. However, instead of deleting all previous postings, they only deleted one or two carefully chosen comments. By contrast, no person performed any kind of social steganography. Participants evaluated this method as “senseless” and “childish”. One person stated:

“Against the background of privacy protection this is nonsense. Then I would rather create lists of people who are allowed to see my stuff.” (male, 27 years)

Nevertheless, the mentioned methods were not evaluated to be sufficiently helpful for privacy protection by participants. One interviewee stated that even though the super-logoff method sounded quite interesting she would not use it because of the implicated disadvantages which would be that other persons cannot find or contact her during the time her profile is deactivated, even though she potentially would like these special people to find her.

To sum up, most interviewees who initially showed interest in the super-logoff and whitewalling nevertheless concluded that it is either not practical or simply not adequate for guaranteeing privacy. Social steganography was not liked at all. It further turned out that privacy knowledge can indeed help to enhance users’ intention to modify their online privacy behavior and particularly to engage in protective measures, if triggered (and not under stress or emotionally affected). However, it was transmitted by participants that privacy protection measures need to be effortless and easy to handle, and at best without bringing any disadvantages.

Acceptance of technical privacy support (RQ4)

Participants were asked two questions regarding the acceptance of technical privacy support and privacy-aware SNS. Specifically, they were asked regarding their opinion of a warning message acting as situational technical privacy support (i.e. “What would you think about a warning message for drawing your attention to privacy protection issues before you disclose information on an SNS?”). Furthermore, requirements for a desirable future privacy-aware social network were examined rather openly (“Imagine 5 years

ahead without all the currently existing SNSs. How should your perfect SNS look like with regard to privacy protection?”).

The idea of having technical privacy support in terms of a system-based warning message was evaluated carefully by interviewees. Most participants liked the idea but after having communicated the advantages, almost all of them struggled with the disadvantages (except one person). Thereby they were trying to tackle a paradox, namely, the desire for privacy protection in contrast to the mistrust in the supportive system providing warning messages for specific content. This will be referred to as *protection paradox* in this work. Furthermore, participants raised the idea of an *undo-button*, being able to withdraw disclosures. In the following, the positive and negative statements referring to the warning message are reported, illustrating participants’ attempt to evaluate benefits and detriments in order to derive a final opinion of the suggested idea.

The first participant positively referred to the warning message by stating:

“I can imagine that this would be helpful because if one wants to post something which could be misunderstood or might be controversial, or one discloses political attitudes, which I actually do not want to disclose, then it would be ok as a kind of reminder.” (male, 27 years)

“I like that [referring to an undo-button]. I had such a feature in my mail program. If I wanted to send a mail between 01:00 am and 05:00 am I had to solve a maths calculation and only if I was able to solve it was I able to send the mail. I set a control for myself.” (male, 27 years)

Perceived disadvantages were expressed by this participant in the following statements:

“On the other hand I think that many people who spread such opinions [referring to strong political opinions] publicly on Facebook would not be interrupted by that (...) I do not think that it would prevent them from disclosing because people with such characteristics and opinions would not care anyway.” (male, 27 years)

“This implicates that Facebook directly analyzes what I am writing – which I actually do not like. But I know that Facebook does it anyway and if they are doing it – then they can warn me anyhow.” (male, 27 years)

The second participant did not believe that he personally would need privacy support but that this measure would be interesting for others. In addition, he was very

critical, and elaborated on the disadvantages more intensely than on the advantages. Positive statements by this participant were:

“Of course, it would be a useful feature...” (male, 27 years)

“For people who are more vulnerable this might be helpful. Well, generally, this would be a useful feature...” (male, 27 years)

“This can be a solution for the problem as well.” [referring to an undo-button] (male, 27 years)

Critical statements referring to the mistrust into the system and the importance of user-friendliness were formulated by this interviewee as follows:

“...But I would ask myself how the system identifies that what I am doing is sensitive. It would need to scan the message and use an algorithm and assess the content.” (male, 27 years)

“...If it works well and does not bother me. When I sit in the train and want to post something completely innocuous it should not bother me by saying, ‘Do you really want to share now?’ Because then I would feel patronized and I would think, ‘yes, of course’, otherwise I would not have clicked the share-button.” (male, 27 years)

“It is definitely important to mention the consequences of my online behavior, because just saying ‘delete this because I tell you’ would be almost a commanding tone. Simply explaining, and giving reasons in order to initiate the target group to think about it, and then allowing for individual decisions to be made. Because one cannot decide for others, but rather give advice.” (male, 27 years)

The third participant had neither a very positive view on the suggested system-based support measure nor a very critical one. The person just questioned the impact of a warning message on users who excessively disclose themselves:

“I think that people who are posting something do not care about it. (...) they would close the popup and it would not matter to them.” (female, 27 years)

Like the second participant, the fourth participant believed he was less prone to privacy violations than other users and therefore ascribed the need for the suggested system-based privacy support rather to others than to him. Nevertheless, he communicated more benefits of the measure than detriments by saying:

“I think I am very cautious with regard to what I *like*, share, and disclose. Therefore it would not be relevant for me personally.” (male, 24 years)

“I think that some people do not need to know my location data. (...) One has to be careful so that no conclusions can be drawn resulting in potential incursions” (male, 24 years)

“Yes [friends would need that]! There are people whom I am intentionally not following anymore because their disclosures are doubtful. Because of their political attitudes for example.” (male, 24 years)

The fifth interviewee believed she was sufficiently careful regarding her disclosures as well. Still she did not reject the idea but communicated to the interviewer that her Facebook friends would need more support than she does. With regard to advantages, she stated:

“On the one hand, this would be quite good...” (female, 23 years)

“...If I consider what other people are posting I think ‘hoo, pay attention and care about yourself’.” (female, 23 years)

On the other hand, she critically reflected on the processes behind the warning messages as well, like the other participants did beforehand:

“...But on the other hand, from where should they know? Then really someone would need to be there and carefully read the stuff or look at the pictures.” (female, 23 years)

The next interviewee really liked the idea of system-based privacy support and even came up with their own ideas like a *confirm-button* for final disclosures and key information presented in a warning message:

“Yes, actually that would be a good idea. Maybe like ‘Hey, do you want to disclose this?’ or ‘Do you really want to like this?’ It is not only your online life being affected.” (female, 19 years)

“Or a confirm button: ‘Are you really sure?’ Yes, a good idea!” (female, 19 years)

“Maybe, if you want to send something, a textbox with information with regard to the decision if one wants to disclose and then confirm or cancel.” (female, 19 years)

As transmitted by the aforementioned statements, this participant explicitly wished for additional information within a warning message or prompt. The only negative aspect for this person was the doubt about whether the warning message would be effective or not by stating:

“People who really want to post something would simply close the reminder.” (female, 19 years)

The seventh interviewee had, similar to the previous participants, a very positive opinion about the concept of a warning message. Furthermore, he was the only person who basically mentioned no disadvantages or doubts at all. The person was enthusiastic about having a control instance enabling a step between formulating a disclosure and finally disclosing.

“Yes, I really think that this would be very good because sometimes it is really the case that one accidentally clicks the send-button so that you do not have a chance anymore.” (male, 21 years)

“One has no restraint or support saying ‘Hey, that was stupid. You should delete this!’ [referring to the situation without having the warning message].” (male, 21 years)

“For sure, messengers are developed for fast communication and the fact that you cannot take it back if it is sent is clear as well. But something like ‘Do you really want to post?’ would be an intermediate step.” (male, 21 years)

The eighth interview revealed once more the importance of user-friendly systems by stressing the risk of users’ being annoyed by technical interventions. The interviewee did not have a strong opinion concerning the potential protection measure but stated distantly:

“...Although it would probably help to think about it, I think it would be annoying.” (male, 21 years)

The ninth participant thought more elaborately about the measure. Again, the topic of politics came up, pointing out that this is perceived to be highly sensitive by users. He communicated anticipated benefits of the measure through the following statements:

“The advantage would be that you do not click the wrong thing that often...” (male, 20 years)

“The advantage with regard to political postings is that one reconsiders whether this is really good what one is going to do.” (male, 20 years)

“In general, I think that it would be rather advantageous to have a confirm-button because the disadvantages [of not posting] are not that severe compared with the advantages [of protective measures].” (male, 20 years)

Negative aspects were referred to by this participant via the statement:

“The disadvantage would be that every time you click *like* you have to think again and then you do not *like* things you would have wanted to *like*. And that it would be laborious to click *ok* every time.” (male, 20 years)

The tenth participant did not have a clear opinion on the suggested hypothetical support measure.

The perfect privacy-aware SNS

Also referring to *RQ4*, and in order to get even more insights regarding requirements for privacy-aware technologies, the interviewees were asked to think about a future in which their currently used social networks do not exist anymore. This being imagined they were asked to think about a perfect SNS they would like to use with regard to user-friendliness and provided privacy support. The most relevant statements, which will also be used for the requirement elicitation for technical privacy support measures, are listed in the following. One main issue was transparency concerning data storage and processing:

“It would be quite cool to know what data get stored and what data get deleted immediately” (female, 19 years)

Moreover, it became clear that some participants were not familiar with Facebook’s current privacy settings in detail because they wished to have some settings that in fact already exist, for instance:

“I want to have privacy, meaning, that you can adjust everything on your profile as private and that you have control over the visibility of your profile and who is allowed to follow you.” (female, 23 years)

This statement stresses the problematic nature of missing knowledge of privacy protection (Bartsch & Dienlin, 2016; Egelman et al. 2016). Facebook in fact provides security measures like the one that was described by this person⁸. Furthermore, participants would like to have background information on privacy and security issues, illustrated via visual cues allowing for an easy access to information and sensitive topics:

⁸ See <https://www.facebook.com/settings?tab=privacy> (last access: 14th October, 2018)

“Maybe highlighting important fields in red.” (male, 21 years)

More precisely, two participants suggested a kind of instructional tutorial for unexperienced Facebook users:

“For example, before one creates a profile one is asked precisely what one wants to share and what not.” (male, 20 years)

“Actually, it should be like this: A user signs in and the first thing that happens is that the system guides the user through the website, tells them all the functions of Facebook, and then there is a kind of step-by-step tutorial. Then you can decide what you want to share with whom under what circumstances. And that is currently not done by Facebook and I criticize that.” (male, 27 years)

These ideas are in line with the approach by Egelman and colleagues (2016), who proposed the “teaching privacy project curriculum” informing teachers how to transmit ten important principles of privacy protection to their students (see Chapter 5.1). In line with these statements and the approach by Egelman and colleagues (2016), interviewees responded with regard to the need of protecting children and younger Facebook users:

“Maybe it depends on the age group. The younger generation uploads more private data than older persons.” (male, 21 years)

“Child-friendlier. Because, of course, more and more young people sign in to Facebook and because of the timeline layout they perhaps don’t know what is to be found and where.” (male, 21 years)

“I think that's important that you could perhaps make it child-friendlier.” (male, 21 years)

In addition, participants made clear that they want to be supported in a nice and gentle manner rather than be dominated by the social network or its security settings:

“Maybe if it [referring to initial privacy information] is nicely formulated like it was done for Windows: “Hello, I am Windows 8” (male, 20 years)

“Actually, it is quite nice now – with the dinosaur [referring to a figure introduced by Facebook, guiding through particular settings]. But I don’t know whether everything is clear with it.” (male, 21 years)

Something that was criticized by almost all respondents ($n = 8$) was the usability of Facebook’s privacy settings. Participants complained that specific settings are neither

easy to find nor understandable. Some statements referring to the structure of Facebook's security settings are listed here:

“You have to click through a lot to find and understand the guidelines and even after finding it you cannot have everything perfectly under control and some things you cannot decide.” (male, 20 years)

“It is written in a way that you do not understand. We talked about this in an economic law seminar last semester – that it is written intentionally in a way that no one understands.” (male, 21 years)

“That would be a cool thing [referring to an alert from Facebook if security settings have been changed] because one does not really recognize when Facebook is changing something. I actually don't know, does one receive a mail from them?” (female, 19 years)

“It could be better. Sometimes one is searching for things but it is kind of ramified. (...) But Facebook could do a better job.” (male, 27 years)

“I did not look for the settings for a long time. I think it is somehow tricky. One has to search a lot.” (female, 27 years)

Following these statements, for participants in this sample, the privacy policies of Facebook are too boring, too long, and confusing. Participants ignored the relevance of reading the policies rather than making the huge effort of reading, processing, understanding, and applying the security information.

Responses to the fourth research question emphasized that respondents showed interest in being supported with online privacy protection. No participant evaluated the supposed approach of technical privacy support as being superfluous or useless. Participants even compared technical privacy support to social situations in which they want to be warned by their friends if there is any danger:

“Yeah, I think looking at privacy issues from another point of view would be helpful! Because, well, I also would like my friends to call my attention when I am doing something stupid.” (male, 21 years)

“I definitely would have a better feeling regarding my privacy when being technically supported.” (female, 23 years)

To sum up, the reported findings demonstrate that there is interest in technical privacy support. Especially the results concerning *RQ4* revealed promising insights with regard to users' acceptance and assumed likelihood to utilize technical privacy support.

Three main aspects to be considered for technical privacy support measures emerged (see Figure 3). The first aspect regards the *content* transmitted through a support measure or from a social network. From the participants' statements, it was derived that clear information should be provided on data storage and on the audience as well as potential negative consequences of online self-disclosure. Secondly, three main methods of transmitting relevant information were revealed (*method*). Owing to the background of this study and the example given in the interviews, the most prominent method was a warning message, triggering privacy protective behavior in a given situation. Further aspects that came up with regard to the method were a virtual agent (like a supportive friend) and visual cues (e.g., highlighting text, providing icons). Thirdly, results clearly show the importance of considering user-centered demands such as autonomy, desire for transparency, and good user experience without any disturbance (*demand*).

The protection paradox identified here resembles the contradiction between users' desire for privacy provided by an external entity and their mistrust toward the system that is providing the privacy support, which might be a further construct influencing users' intention to protect their privacy via a support system and also their actual behavior in utilizing system-based privacy support or not (see Figure 3). In 2013, Sutano and colleagues also identified a paradox with regard to online privacy protection when analyzing users' concerns about commercial information technology. They found that the gratifying effect of personalization for making suggestions suited to the user is related to privacy concerns. On the one hand, users enjoy personalized feedback but on the other hand, the better a system recommendation suits the users, the more they would scrutinize the underlying mechanisms and methods for gathering personal data, resulting in more pronounced privacy concerns. The authors referred to this paradox as the *personalization-paradox*. Although Sutano and colleagues (2013) analyzed data tracking driven by a different motivation than was done in this work, which focused on users' privacy protection instead of adaptation to the user in order to make commercial information technology applications more enjoyable to use, the protection-paradox and the personalization-privacy paradox seem to be closely related.

Considering these aspects might help to improve the impact of technical privacy support measures and succeed in strengthening users' behavioral intention to engage in

privacy protection as well as increasing the likelihood that protective behavior actually is indeed performed.

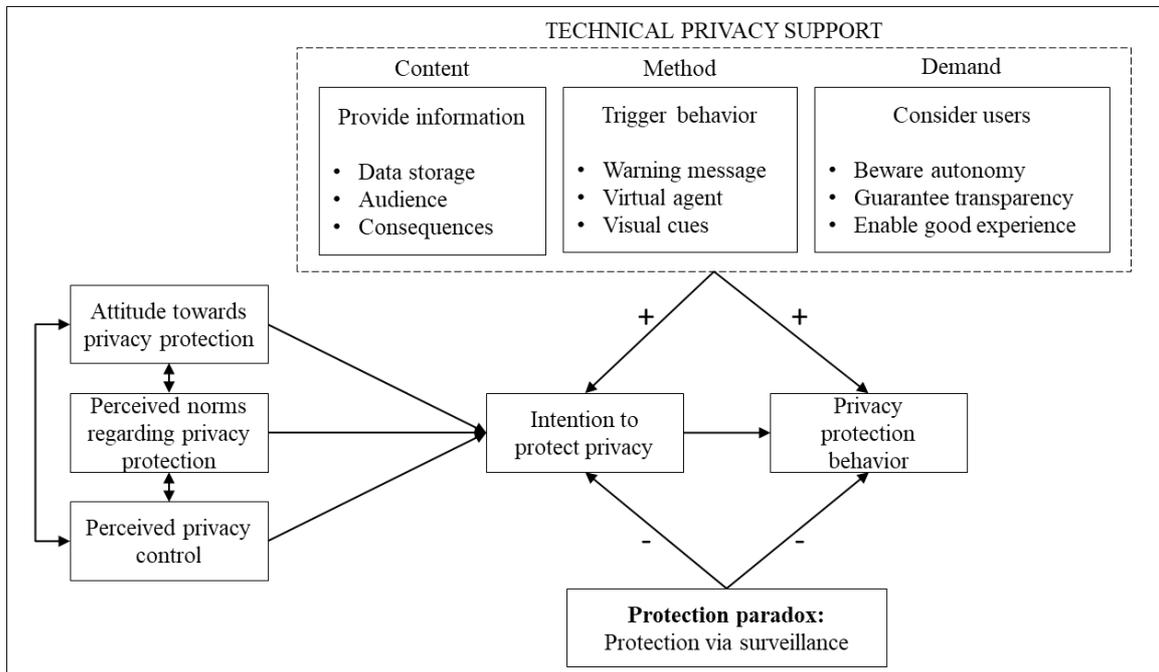


Figure 3: Requirements for a technical privacy support system derived from interviews on the theoretical basis of the theory of planned behavior (Ajzen, 1991).

10.7 Discussion

This study aimed at identifying features and characteristics that would be necessary to increase users' intention to act in a more privacy-aware way after being alerted by a privacy warning message if a sensitive disclosure to an online audience was about to happen. Analyses of current research questions offered several insights serving as a fruitful ground for elaborating a technical privacy support feature, as was introduced to participants of this study.

Privacy awareness (RQ1)

Interviewees' privacy awareness was shown to be very situational. When asked directly, they stated they were aware of privacy risks. Respective statements illustrated participants referring to internalized norms. As explained in Chapter 8.6.1, social norms are strong predictors of behavior if corresponding attitudes, perceived self-control, and behavioral intentions are pronounced as well (Ajzen, 1991). If the internalized social norm is detached from these behavioral elements, the probability of the behavior

conforming to the norms is relatively low. This is often detected in privacy research with regard to privacy-related norms and protective behavior, and was also found in this study. People report being privacy-aware because, according to their statements, this is important and one should care about it. Still, the actual behavior of interviewees contradicts reported opinions. When asking for privacy protection routines in everyday life it became clear that users' awareness is not a constant state and privacy protection is not implemented comprehensively. Users neither completely stop disclosing sensitive content nor adapt privacy settings regularly. In addition, some users are even unaware of their own settings, for instance, concerning the searchability of their profiles on the Internet, which is a pattern that was also observed by Trepte and Masur (2016). For most users, the topic of privacy protection arises sporadically but disappears quickly, when perceived benefits of information disclosure and short-term advantages outweigh the risk awareness (e.g., they stated being aware of risks but ignoring them in everyday life). This is in line with findings by Dienlin and Metzger (2016), who found that the extent of concerns is crucial for self-disclosure decisions because the anticipation of benefits increases the likelihood of self-disclosing activities. If users are in an aware state, it might be more likely that perceived risks and damages lead to a decrease in self-disclosure (Dienlin & Metzger, 2016). This evaluating process is referred to as privacy calculus in the literature (Culnan & Armstrong, 1999). As interviews revealed, such aware states are very rare in comparison with unaware states. A system-based support measure working in real-time would be beneficial in such situations because it can interrupt this unawareness.

RQ1 focused on the participants' current privacy situation, allowing to derive their level of awareness and individual value of privacy. Participants indeed think that privacy is important (i.e. privacy attitude) and they generally know that one must be careful regarding privacy issues (i.e. subjective norms). Nevertheless, the situational absence of privacy awareness is one relevant factor for careless privacy behavior. To conclude, analyses concerning the first research question revealed that general privacy awareness is present but situational privacy awareness is missing. Therefore, system-based real-time privacy support is needed to raise the situational awareness of privacy.

Worries and consequences (RQ2)

Reflecting on participants' concerns and worries (RQ2), it becomes clear that for them, being protected from harmful consequences stemming from other users (horizontal privacy, see Chapter 2.2, Bartsch & Dienlin 2016) seems to be more important than trying to eliminate negative consequences based on institutions like Google or Facebook, for instance (vertical privacy, see Chapter 2.2; Bartsch & Dienlin, 2016). This does not mean that users are not afraid of vertical privacy risks but rather that they feel especially helpless in that case. Participants believed that there is no chance to protect oneself against surveillance through providers and companies anyway. Based on this perceived lack of control, there are two different consequences of the perception of powerlessness. On the one hand, users ignore the risks that they believe they cannot prevent. On the other hand, they tend to attribute the risks to other users, replacing their fears.

However, in line with the findings by Ahn, Kwolek, and Bowman (2015), Bartsch and Dienlin (2016), Dienlin and Trepte (2015), Vitak (2015), and Osatuyi (2015), privacy concerns can also be considered as a driver (besides behavioral intentions and attitudes) for engaging in online privacy protection (see Chapter 6.2.3). Consequently, one possibility to encourage users engaging in privacy protection is by confronting them with their concerns, either related to vertical (e.g., data theft) or horizontal privacy (e.g., becoming a victim of an online firestorm). This can be implemented by providing particular information and examples of the most likely negative impacts of sensitive information disclosure within a privacy prompt, for instance (e.g., "Disclosing information like the one you are going to disclose has been identified as an initiator for a firestorm in 30% of all cases. Do you want to continue?"). Furthermore, persuasive strategies like the ones introduced by Bang, Torstensson, and Katzeff (2006) could be promising for enhancing privacy awareness as well. For example, a *privacy-meter* could give an indication regarding the level of sensitiveness of the respective piece of information or the hypothetical harmful consequences.

As was shown, interviewees tend to underestimate their personal privacy risks while they overestimate those of other users (which in some cases even reduced users' concerns). This is reflected in the findings regarding the third-person effect by Baek, Kim, and Bae (2014). One countermeasure against this biased view could be to implement self-monitoring persuasive support measures that confront users with their personal risks.

Through the visualization of the risks of personal behavior, the users' intentions to reduce sensitive self-disclosure might be strengthened and thus, following the TPB, they may be more likely to modify their online behavior. Referring to findings by Dienlin and Trepte (2015), users' privacy concerns are one driving factor for privacy behavior and therefore might be a key element for raising awareness and inducing privacy-related behavioral changes.

Similar to interviewees' privacy awareness, privacy concerns are present but do not lead to sufficient privacy protective behaviors because they are not specific enough. Analyses revealed that even though participants sporadically think about adapting privacy settings, it seldom results in comprehensive secure privacy behavior. Only one of the biggest fears—namely, being misunderstood and disliked because of having controversial opinions (e.g., regarding politic)—was identified as a driver for not disclosing information in particular situations. However, this can also be explained by findings concerning the spiral of silence, namely, that people do not disclose information if they perceive themselves to be in a minority regarding a specific topic (Noelle-Neumann, 1974). Participants pointed out having strong short-term concerns that were volatilized after a particular period of time and changed into constant slight concerns in the background. Such concerns induce feelings of insecurity but do not make people change their behavior.

Moreover, most interviewees never experienced negative consequences of information sharing. It seems as if the human basic need for privacy (e.g., DeCew, 1997) is not fully present in online environments for those people who never experienced privacy violations in the past. This is related to prior findings by Wang and colleagues (2011), who reported that users' regrets of posting something on Facebook were the main trigger for paying more attention to privacy. Without a trigger, reminder, or personal involvement (e.g. based on negative experiences), the behavioral intention to protect oneself is not sufficiently pronounced to result in privacy protective behaviors (see Fogg, 2009; Xie & Kang, 2015).

It can be concluded that users' privacy concerns can be translated into privacy support. If users are confronted with their own concerns and receive suggestions for improving the situation at the same time, this can increase their perceived level of control (see TPB; Ajzen, 1991) as well as their protection motivation (see PMT; Rogers, 1975)

and the likelihood of a behavioral change. Substantial privacy support that spurs the transition from concerns to actual behavior is needed.

Privacy knowledge (RQ3)

Even though this study revealed support for previous findings showing that privacy literacy is highly relevant for modifying privacy behavior (see Chapter 5.1, e.g., Bartsch & Dienlin 2016), analyses also indicate that it might be beneficial to not solely build on educational approaches (which are related to high effort and therefore not preferred by users) but rather to support users regarding spontaneous disclosures. For instance, by informing users via persuasive pop-ups containing relevant information or providing rewards for accepting and implementing privacy suggestions.

Furthermore, in line with Moll, Pieschl, and Bromme (2014), it is reasonable to not only focus on increasing users' privacy literacy per se but also to enlighten them about their actual level of privacy knowledge, which is often not equal to their perceived level of knowledge. If people know what they know (and what they do not know), they can engage in respective behaviors.

With the examination of the third research question it was underpinned that privacy literacy is important, but situational information transmission regarding potential consequences of single postings and the audiences of that posting are more expedient in terms of raising awareness and control behavior.

Acceptance of technical privacy support (RQ4)

Participants evaluated the concept of technical privacy support positively (in contrast to Facebook's privacy settings that are described as confusing because of bad usability and missing clarity). Although interviewees liked the idea of being supported, their reported willingness to consult this technical privacy support would depend on particular conditions. From the participants' point of view, user-friendly privacy support needs to be transparent, gentle, as well as comprehensible whereby it should not be disturbing or too boring (according to users' opinions: in contrast to the Facebook settings). Following Fogg's statement that "pop-ups, ads, and other annoying artefacts (...) rarely convert to behavior because we have low motivation to do what they say

(2009, p. 3)”, a persuasive privacy measure must meet users’ needs and skills (abilities) and motivate them adequately (motivation) in crucial situations (trigger).

Most importantly, users’ efforts with regard to a privacy protection measure should be as low as possible. This is in line with conclusions by Taneja, Vitrano, and Gengo (2014), who state that enjoyable usage of privacy control measures is related to the attitude toward using such a measure as well as to a positive perception of the respective measure. In line with Fogg (2009), the likelihood of a behavioral change increases if people perceive control over a situation, which can be ensured by making a task as easy as possible. He states that “increasing ability (making the behavior simpler) is the path for increasing behavior performance” (2009, p. 3). The challenge is to help users to satisfy their psychological needs for competence and autonomy (Ryan & Deci 2000), by allowing them to make the final privacy decision by themselves, albeit guided through technical privacy support. Interviewees do not want to be patronized (“[...] Simply explaining and giving reasons in order to initiate the target group to think about it and then allow to make own decisions. Because one cannot decide for others, but rather give an advice”), thus, technical privacy support measures should guide the users (back) on the right track by still empowering them to make self-determined, but supported, privacy decisions.

Moreover, interviewees would like to directly perceive benefits demonstrating the advantage of following the system’s suggestion. Positive feedback (e.g., emoticons / textual commendation) after accepting a privacy suggestion and a subsequent behavioral change could empower the users. Textual rewards in terms of affirmative feedback can increase the individual’s perceived autonomy and strengthen him/her regarding the rewarded behavior (Deterding, 2014). However, if the feedback is perceived as too controlling this positive effect as well as the perceived autonomy of the individual are likely to decrease (Deci & Ryan, 2000). Therefore, persuasive privacy feedback should inform about risks without being reproachful. This can be realized by using particular persuasive styles for the formulation of supportive privacy messages (e.g., Kaptein et al., 2012).

Participants wish to have a kind of trigger for privacy protection. One solution for this problem could be to enhance users’ awareness and involvement by sensitizing them, for example via persuasive self-monitoring measures and real-time privacy

recommendations combined with information regarding the consequences that could occur when not following the recommendations, serving as initiating events (triggers) for privacy protection before a regret will be experienced. To make it more understandable and to meet the users' needs, graphs and visualizations could serve as clarifying elements.

The paradoxical disadvantage of being observed by the system that generates privacy feedback can be diminished by making the system transparent and – as a consequence – trustworthy. If it is explained transparently and honestly that user data are only employed for the users' advantages and will not be transferred to other parties (which is perceived as an almost indispensable circumstance), trust in the system can be established. Since users currently assumed that having control over one's personal data is impossible, they do not know whom to believe or which system to trust.

Summing up, in line with Ajzen (1991) as well as Dienlin and Trepte (2015), users' privacy behavior, and therefore also the likelihood of adapting privacy measures, cannot sufficiently be predicted by their general attitudes toward privacy. Instead, perceived control, behavioral intentions, subjective norms, as well as privacy concerns are related to users' actual privacy behavior. As stated earlier, the users' perceived control can also be distorted and thus lead to false risk estimations and consequently in risky privacy behavior. This can happen when the person has too little information regarding the situation and behavior, when required preconditions have changed or when the situation is totally new, for example, when the social network world is new (primary) for children and (so far) non-users. Furthermore, it became clear that either activating a single privacy setting or trying to reduce the extent of personal information being shared only several times does not mean that a person is fully aware of his/her privacy or that this person is not endangered by privacy risks.

It can be concluded that a privacy support measure should cover privacy concerns (e.g., directly demonstrating consequences of sensitive disclosures), intentions (e.g., being inviting and prompting without being disturbing), perceived control (e.g. giving recommendations for action), as well as individual attitudes and usage habits (e.g., asking for it in a short questionnaire before implementing a support measure).

In sum, this work shows that online privacy is important in human–computer interaction and that users' need and want to be supported in maintaining their basic right

to control the distribution of their thoughts, emotions, and cognitions. For the development of a supportive privacy measure, it is necessary to address the questions of what the person should be informed about (e.g., data storage, audience, negative consequences), how the user should be informed (e.g., trigger messages, virtual agents, visual cues) and why the information should be given (e.g., to guarantee autonomy, transparency, good experiences).

10.8 Limitations

The current study revealed several important insights. However, some limitations have also been identified. Although a sample size of ten participants is acceptable for a qualitative interview study, the current findings do not allow for a generalization but need to be further analyzed by means of quantitative studies with bigger samples. Furthermore, interviewees had almost the same educational backgrounds. It would be interesting to find out more about the acceptance of the introduced system using a more heterogeneous sample. As is the case for all studies based on self-reports, it is possible that third-person effects distort findings regarding perceived risks and the need for privacy support. Moreover, the concept of technical privacy support was only explained verbally to participants, which could have led to uncertainty or vagueness regarding the concept. Therefore, follow-up studies will be conducted in order to analyze users' actual acceptance and online behavior directly, by means of an experimental approach in which the technical privacy support measure will be simulated. Thereby it can also be examined whether the functionalities people would like to have are equal to those they actually need.

Users' personality plays an important role for privacy behavior and the adoption of privacy-preserving measures. Since a qualitative study was conducted, there are no clear values regarding the users' personality. Nevertheless, future studies will also consider users' personality by means of personality scales.

A further overarching issue is the ethical question concerning intervening in people's personal lives. In some cases, the line between persuading (here, helping) and manipulating people (e.g., by exploiting them) is fine. Nevertheless, when using the privacy measure as it is intended, people can still decide freely whether to accept the recommendations and to use the suggested system at all. If the user decides to take care

of his/her privacy and to use such a system by downloading the respective application or ad-on, then this can be considered a voluntary action that is ethically acceptable.

10.9 Future Research

Future work will – based on current results – empirically investigate users' experience and evaluation of interacting with a technical privacy support measure that alerts the user if he or she is going to provide sensitive information to the public as was introduced theoretically in this study. Based on the interview results, this measure will be a privacy support message informing about the riskiness of a disclosure and pointing out potential risks by means of persuasively formulated alerts. A further step will be to enrich supportive messages with particular persuasive elements (e.g., self-monitoring features) as mentioned in the current work.

10.10 Conclusion

To conclude, this work is a starting point for answering the question of how to enlighten users of SNSs concerning potential negative consequences of their online actions and how to give users an indication of what would put them at less risk. It needs to be clear for users that simply thinking occasionally about privacy is not sufficient for ensuring a harmless online environment. Since there are situations, in which users are not aware of privacy risks – regardless of being literate or not – this study focused on a real-time solution, empowering users in privacy decisions. With the foundation of the interviewees' statements, this study paves the way for comprehensive technical privacy support which in the future should be enriched by findings regarding users' personality and adapted to the multidimensionality of privacy.

Summary Study 1

In sum, the first study of this dissertation revealed that users of SNSs do not feel sufficiently protected. Although some participants engaged in sporadic privacy protection they nevertheless did not engage in comprehensive and steady privacy-aware behavior. Given that interviewees said they are not satisfied with the privacy settings provided by Facebook and the way Facebook transmits terms of conditions to its users, it might be interesting to evaluate users' efforts to engage in alternative privacy protective methods

as well. The first step in that direction was made by asking participants about their knowledge of a self-driven privacy protection method, namely, the super-logoff. The opting-out measure was known by two persons from the sample of Study 1. After talking about this opting-out method, a diverse picture emerged. On the one hand, the super-logoff was evaluated as being an interesting alternative to merely relying on the usual privacy settings. On the other hand, it was perceived as disadvantageous because it would impede gathering benefits from using SNSs. Thus, there are two main issues arising from Study 1. First, a collection of users' requirements for system-based privacy support was compiled. These requirements will be referred to in more detail in Study 3 and Study 4. Second, a diverse picture regarding the perceived effectiveness of the super-logoff was revealed. Therefore, Study 2 will examine this measure in more detail by means of a quantitative investigation. The study will determine whether users would consider this self-driven privacy protection method of opting out of the network; it will also discuss in what sense this method could truly affect users' perceived control over their privacy and how it relates to users' privacy concerns.

IV OPTING-OUT FROM SNSs

11 Study 2: Time-Out for Privacy Concerns - Investigating Motives and Influencing Factors for Deactivating One's Facebook Account as an Alternative Strategy for Regulating Online Privacy

SNSs provide their users with manifold opportunities for social interaction and self-presentation (Debatin, Lovejoy, Horn, & Hughes, 2009; Ellison, Steinfield, & Lampe, 2007; Smock, Ellison, Lampe, & Wohn, 2011; see Chapter 1 and Chapter 2.2). To benefit from all these positive characteristics of SNSs, users need to provide personal and sometimes sensitive information to other users (i.e., horizontal privacy) and to the SNS itself (i.e., vertical privacy; see Chapter 2.2).

As outlined in Chapter 6, there is a considerable amount of research examining factors that influence privacy behavior such as privacy concerns (e.g., Dienlin & Trepte, 2015; Hoy & Milne, 2010), or individual characteristics like need for popularity or impression management motivation (see Chapter 6.2). Furthermore, online privacy literacy has been revealed to play an influencing role in users' online privacy protection behavior (see Chapter 5.1). However, when and why users decide to use self-regulative privacy measures instead of relying on usual settings such as restricting access to the profile remains under question.

Privacy protection in the scope of this work refers to avoiding risky online actions such as self-disclosing sensitive and personal information. The fact that different communication circles – consisting of friends, family, acquaintances, colleagues, but also strangers – can have access to users' information poses a serious threat (e.g., Marwick & boyd, 2011). As outlined in Chapter 2.2, social boundaries can become blurred (Petronio, 2010) and communication contexts can collapse (Marwick & boyd, 2011). These blurred conditions can bear privacy risks and result in privacy harms for users who are disclosing personal information to diverse and unknown audiences (e.g., Lawler & Molluzzo, 2010; Vitak, 2012). Moreover, people who consume information disclosed by other users can become co-owners of that information (Petronio, 2010) and may spread it to another, broader and more heterogeneous audience, which puts the original sender at risk (see

Chapter 2.2). Against this background, privacy researchers strived to learn about people's privacy attitudes and intentions, their protective or non-protective behaviors, and correlations among these variables (e.g., boyd & Hargittai, 2010; Dienlin & Trepte, 2015; Taddicken, 2014).

As described in Chapter 7.2, it some Facebook users consider the Facebook setting for deactivating one's account as a protective shield against privacy harms though still being able to temporally share information and gather social support. This setting deactivates the Facebook account of the user, so that he or she is not visible for other users anymore. The procedure of using this setting as a privacy measure is called *super-logoff* (boyd, 2007, 2010). This method is quite radical because a user who deactivates his/her account completely withdraws from the network for a given period⁹. Users who take this "social retreat" are not able to gather social gratifications anymore, because through opting-out they are neither searchable nor addressable by other users. The radical character of this measure calls for research with regard to the motives to opt-out and the influencing factors for considering this "social retreat" as alternative measure for privacy protection.

danah boyd (e.g., 2007, 2010) initially investigated the super-logoff. She found that young SNS users perceive opting-out from Facebook to be a helpful protection strategy to avoid privacy invasions with little effort – related to time and cognitive effort.

There is a lack of knowledge on whether users' privacy attitudes and concerns are related to their individual intentions to deactivate their accounts and the motives for opting-out. The goal of Study 2 was to answer the question whether the super-logoff contributes to a perception of online safety and consequently might even override users' privacy concerns. In addition to that, direct predictors for using the super-logoff shall be investigated. This work argues that examining the factors influencing the intention to use this radical measure provides practical insights for understanding influencing variables for users' protection behaviors and the design of future privacy protection measures.

11.1 Motives for Opting-Out

As outlined in Chapter 2.1, by regulating privacy, people are able to distinguish themselves from other persons or groups (Altman, 1975). According to Altman's theory

⁹ See https://www.facebook.com/help/delete_account/ (last access: 14th October, 2018)

of privacy boundary regulation, people's desire for privacy can depend on current situations, environmental cues, or social interaction partners (Altman, 1975; boyd & Marwick, 2011; Masur & Scharkow, 2016). The optimal level of privacy does not imply total anonymity and isolation but instead means finding the balance between a maximum and a minimum of privacy and self-disclosure, affected by personal characteristics, experiences and the given context (Masur & Scharkow, 2016). According to Masur and Scharkow (2016) people try to achieve a particular level or state of privacy. Hence, they engage in an individual dynamic process of interpersonal boundary control. The super-logoff can be located near the maximum of privacy. So far, the super-logoff has not been investigated quantitatively (Masur & Scharkow, 2016). Knowledge regarding this strategy is mainly based on qualitative research (boyd 2010).

According to boyd's (2011) analyses, one motive for using the super-logoff is to be unsearchable for parents, teachers and other adults because the teenagers who were asked regarding the usage of the super-logoff do not trust them. Some users even reported to only reactivate their profiles at night because they think that the likelihood that adults search for them during the night might be lower than during the daytime (boyd, 2010). Consequently, one advantage of using the super-logoff might be to feel unobserved and more relaxed.

Given that (a) this strategy has been investigated mainly in the United States with little knowledge regarding the usage of the super-logoff in other countries, and (b) users' online privacy behaviors in fact differ between countries and cultures (e.g., Trepte, Reinecke, Ellison, Quiring, Yao, & Ziegele, 2017), there is a high demand for research in this area. Trepte and colleagues (2017) found, for instance, that in individualistic cultures, people find it less important to get social gratifications through SNSs (compared with collectivistic cultures) and that for people in collectivistic cultures, privacy risks do play a greater role. Moreover, it was revealed that users in the south of Europe handle their disclosures differently (as a choice) than in the eastern part of Europe (as forced; Miltgen & Peyrat-Guillard, 2014).

In sum, the reasons and circumstances for Facebook users to deactivate their accounts seem to be manifold. boyd (2011) identified the fear of being observed as potential motive for using the super-logoff. In order to support her qualitative findings and to identify even more motives, this study investigates the motives to use the super-

logoff as regulatory measure. This issue was addressed in an explorative way via two research questions asking for potential motives to use the presented opting-out measure.

Research Question 1 (RQ1): What are the motives to use the super-logoff?

Research Question 2 (RQ2): Can certain motives to use the super-logoff predict the actual intention to opt-out from the network?

11.2 Maintaining Privacy Through Regulating Self-Disclosure?

The need for privacy regulation is related to users' extent of self-disclosure, perceived risks, and perceived benefits as consequences of disclosing the self (e.g., Lee, Park, & Kim, 2013). Self-disclosure can vary according to the extent, intimacy, honesty, and awareness of the revealed information (Altman, 1975; see Chapter 4). The extent to which people disclose information that is perceived as private by them, is accompanied by the risk to lose privacy, calling for engagement in privacy protection (see also Masur & Scharrow, 2016; Walther, 2011). However, disclosing information is a necessary precondition for using the tools provided by SNSs (Ellison, Steinfield, & Lampe, 2011). In line with this, privacy is an interplay of disclosing, hiding, withdrawing, knowing, protecting, and regulating.

When trying to regulate online privacy by weighing individual risks and benefits of (sensitive) information disclosure, users assess risks subjectively and might be biased (see Chapter 5.3). Gratifications of disclosing the self are directly perceivable and immediately rewarding (e.g., social feedback, recognition). In contrast, risks and privacy violations often occur delayed and might even induce long-term consequences such as job loss or the exclusion from a peer group. The privacy calculus (Culnan & Armstrong, 1999; see also Dienlin & Metzger, 2016; Krasnova & Veltri, 2010) describes the attempt of users to balance online self-disclosure and self-withdrawal (e.g. delete photos or links, unfriending) driven by anticipated gratifications, experiences, concerns and expectations (see Chapter 6.2).

Nevertheless, self-disclosure is a precondition for every social relationship (Taddicken, 2011) but might endanger users' online privacy (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011). Following the findings by boyd (2011), one opportunity to control one's online privacy without abandoning self-disclosure is to deactivate one's SNS

account. Research by Debatin and colleagues (2009) and Krasnova, Spiekermann, Koroleva, and Hildebrand (2010) suggests that individuals who perceive themselves as having more control over their data (as boyd's participants did by using the super-logoff), disclose more personal data about themselves. This assumption is further stressed through findings by Brandimarte, Acquisti, and Loewenstein (2013) who examined the *control paradox* claiming that users who believe to be in control of disclosed information actually disclose more information, which becomes a problem if the perceived control was based on a biased perception. In this work, it is assumed that the extent of self-disclosure influences the perceived need to control one's own privacy boundaries and consequently the intention to deactivate one's Facebook account. Therefore, the following hypothesis was stated:

Hypothesis 1 (H1): There is a positive relation between the extent of online self-disclosure and the intention to use the super-logoff.

11.3 Privacy Concerns as Driver for Privacy Protection

Disclosing personal information online can cause privacy threats, which is one reason why users of SNSs might be concerned about their privacy (Petronio, 2010). Following Dienlin and Trepte (2015), users' privacy concerns are related to their privacy attitudes which subsequently impact their privacy intentions and actions (see Chapter 5.2.3). Moreover, Facebook users with strong privacy concerns tend to use more self-withdrawal mechanisms, such as not friending someone or limiting disclosures on Facebook, compared with unconcerned users (Dienlin & Metzger, 2016). These relations between concerns and behavioral intentions to utilize privacy settings, or to engage in withdrawing strategies, are important when examining privacy protection behavior because behavioral intentions are one relevant predictor of actual behavior (Ajzen, 1991).

Online privacy concerns can evolve based on different variables, such as prior negative experiences (Wang et al, 2011), or users' computer anxiety (Osatuyi, 2015). A concern itself is a unipolar construct that is always associated with negative outcomes (Dienlin & Trepte, 2015; see Chapter 6.2.3). However, in the context of online behavior, concerns can encourage necessary privacy protection, which is actually desirable (see Chapter 6.2.3). Although privacy concerns do not always directly influence online privacy behavior, they nevertheless influence people's privacy attitudes, which are

related to their privacy intentions and privacy behaviors (Dienlin & Trepte, 2015). Therefore, it is suggested that participants' privacy concerns are also positively related to the attitude toward (using) the super-logoff. In this study, the relation between users' privacy concerns and their attitudes and intention toward the use of the super-logoff will be investigated by the following hypotheses:

Hypothesis 2 (H2): Users' privacy concerns positively influence their attitude toward (using) the super-logoff.

Hypothesis 3 (H3): Users' privacy concerns positively influence their intention to use the super-logoff.

11.4 The Role of Online Privacy Literacy

Some people have difficulties to implement privacy protection strategies due to missing online privacy literacy (Bartsch & Dienlin, 2016; Trepte et al., 2015).

As outlined in Chapter 5.1, Trepte and colleagues (2015) define online privacy literacy as a combination of two different types of knowledge: the declarative (i.e. knowing measures and settings for protection) and the procedural knowledge (i.e. knowing how to implement these measures). Hence, privacy literacy comprises knowledge about technical aspects, concrete protection strategies, legal conditions and how to consider these aspects for privacy protection (Trepte et al., 2015). Users who are lacking privacy literacy are less able to protect their online identity which explains why people with high privacy literacy feel safer than people with low literacy (see Bartsch & Dienlin, 2016). However, even if users are literate and configure their privacy settings from time to time, disclosed information can still leak through other parts of the network.

boyd (2008) concluded that users of the super-logoff seem to have limited privacy protection skills which might be the original reason for consulting this drastic strategy. Users who have limited privacy literacy might use the super-logoff because they do not know of (or how to use) provided settings for privacy protection such as limiting their audience, forbidding other users to tag them or providing less sensitive information. Hence, they might perceive deactivating their account as an adequate compromise because they would not be able to actively counteract potential privacy harms if the account is activated but they are not online. However, even during the time in which users

are online, they do not have total control because privacy violations are typically not announced but instead occur in the background. Furthermore, frequently changing one's privacy settings on an SNS can contribute to increased online privacy literacy (Bartsch & Dienlin, 2016). This could in fact be an indicator that people who use the super-logoff have rather low privacy literacy because instead of adapting their settings regularly, they completely switch off the network (boyd, 2010). This might be a typical behavior for those users who are concerned and want to feel more secure but do not know how to use privacy settings because of missing declarative and procedural knowledge (Trepte et al., 2015). Thus, self-adapted strategies like the super-logoff might be grounded in the mismatch of concerns and literacy. Low literacy might be correlated with the intention to use the super-logoff because people with high literacy are able to protect themselves via regular privacy settings, which would make the super-logoff unnecessary for them. However, if people know where to find the setting to deactivate the account, they might at least have some declarative privacy knowledge (see Trepte et al., 2015) because the setting is difficult to find for unexperienced users (see also Study 1). These apparent opposites of possible explanations regarding the relation between privacy literacy and the intention to use the super-logoff lead to the following research question:

Research Question 3 (RQ3): Is there a negative or a positive relation between users' online privacy literacy and the intention to use the super-logoff?

11.5 Situational Impression Management Behavior

As described in Chapter 5.2.3, Goffman (1959) compares people's everyday behaviors to the actions of actors in a theater. He claimed that people strive to build and attend to a specific facade or impression (Goffman, 1959; see Chapter 6.2.3). People engaging in impression management aim to present themselves as how they would like to be or how they would like to be perceived by other people (Goffman, 1959, see Chapter 6.1). SNSs provide manifold opportunities and tools for self-presentation, impression construction, and impression management (e.g., Bazarova & Choi, 2014; Haferkamp, 2010; Hogan, 2010; Utz & Krämer, 2009). In this study, the focus lies on situational impression management behaviors as being an influencing factor for deactivating one's Facebook account in order to not endanger a developed impression by leaving the profile unattended.

Users' self-disclosure and impression management relate to and often involve each other, because without disclosing information about oneself it is hardly possible to create and maintain a positive impression (Krämer & Haferkamp, 2011; Utz, 2015). Research already revealed that users engaging in impression management on SNSs tend to have less restricted online profiles (Utz & Krämer, 2009; see Chapter 6.2.3).

This study examines the relation between users' situational impression managing behavior on Facebook and their intention to use the super-logoff. It was assumed that users who engage in impression managing behaviors might be concerned that the positive impression they created could be damaged by other people, for instance, through negative comments being added or any information that could damage their positive appearance in their profiles. Therefore, the super-logoff might be a relevant measure for users with pronounced impression management motivation. More precisely, the relation between users' self-disclosure and the intention to use the super-logoff (see *HI*) might be mediated by situational impression management purposes:

Hypothesis 4 (H4): The relation between the extent of online self-disclosure and the intention to use the super-logoff is mediated by users' situational impression management behavior.

11.6 Method

In order to address the stated hypotheses and research questions, a quantitative online study was conducted ($N = 124$). All variables that were hypothesized to influence the intention to use the super-logoff as well as previous knowledge regarding that measure were examined. Since not all participants already had experiences with deactivating their Facebook account, a small part of the questionnaire (three items) could only be answered by a subsample ($n = 22$). However, an explanation of the super-logoff was presented to all participants in order to guarantee that all persons had the same level of knowledge regarding the measure of interest in Study 2. For descriptive statistics, patterns and frequencies of using the super-logoff were examined as well as whether users had profiles on additional social media platforms such as Instagram, Twitter, or LinkedIn. Preconditions for participating were to have a Facebook account and to be at least 18 years old. Every person had the chance to participate in a lottery to win 4×10 euros. A local ethics committee approved all conditions.

11.6.1 Measures

Knowledge concerning the super-logoff

For estimating the users' knowledge and experiences concerning the super-logoff and further regulatory strategies, particular items addressing awareness, related behavior, and perceived usefulness of such measures were included (e.g., "I know how to deactivate my Facebook account" or "I already deactivated my account for a specific period of time"). Answers to these questions were dichotomously (*yes/no*), whereby the particular item "I know other methods than the typical privacy settings to protect my privacy" provided space for individual text inputs.

Online self-disclosure

For examining the extent of online self-disclosure, the categories *amount* (four items, $\alpha = .874$, e.g., "I have a comprehensive profile on Facebook"), *honesty* (three items, $\alpha = .486$, e.g., "I am always truthful when I write about myself on Facebook"), and *conscious control* (five items, $\alpha = .841$, e.g., "I think carefully about how much I reveal about myself on Facebook") of disclosure of the Information Disclosure Scale (Krasnova, Günther, Spiekermann, & Koroleva, 2009) were initially considered. Participants responded on a 7-point Likert scale (1 = *I don't agree at all* to 7 = *I totally agree*). Overall reliability was $\alpha = .819$ for all items. The low value for the category honesty did not change by excluding single items so that it was decided to exclude this category from the scale and to consider only the categories amount and conscious control. Therefore, overall reliability was $\alpha = .801$.

Situational impression management behavior

To investigate users' situational impression management behavior on Facebook, items were adapted to those used by Utz and Krämer (2009). Two original items by Utz and Krämer (2009) were considered, namely, "I use the Internet to influence my image" and "I like the Internet because more people can notice me and my profiles" and five further items for particularly measuring situational impression management behaviors such as "If I don't like a comment on my Facebook profile, I delete it" were added. An overview of all items can be found in Table 2. Participants were asked to respond on a 7-point Likert scale ranging from 1 = *I don't agree at all* to 7 = *I totally agree* ($\alpha = .805$).

Table 2

Items for measuring situational impression management behavior, including mean values and standard deviation (Study 2).

	<i>M</i>	<i>SD</i>
I use the Internet to influence my image.	2.85	1.61
I like the Internet because more people can notice me/my profiles.	2.73	1.53
I like to have control over my profile at any time.	5.73	1.44
On my profile, I want nothing left to chance.	5.25	1.52
My profile mirrors me very well.	3.58	1.62
I want that my profile displays me.	3.63	1.62
If I don't like a comment on my Facebook profile, I delete it.	5.03	1.82

Online privacy literacy

Participants' online privacy literacy was examined through the Online Privacy Literacy Scale (OPLIS; Masur, Teutsch, & Trepte, 2017), comprising 20 questions related to knowledge of data collection and storage, knowledge of data protection laws, knowledge of technical aspects of data protection and knowledge regarding strategies for data protection (each five items). Participants were asked to assess certain statements concerning these topics (*true/false/don't know/different response options*). Correct answers were counted and were summed up and used to estimate participants' privacy knowledge (according to the provided tables for analyses). According to the norm scales by Masur, Teutsch, and Trepte (2017), the OPLIS values for investigation were inferred by considering for participants' age and sex. Four persons did not specify their sex. Therefore, their values were calculated by means of the unspecified OPLIS scale for the whole population. An OPLIS value of 100 displays the mean of the population, values lower than 100 displays a performance below average.

Privacy concerns

Participants' privacy concerns were investigated by using a privacy concerns scale by Buchanan and colleagues (2007). Ten items regarding the extent of privacy concerns were used. Users responded on a 5-point Likert scale, ranging from 1 = *not concerned at all* to 5 = *highly concerned*, for example: "How concerned are you in general regarding your privacy when you use the Internet?" ($\alpha = .896$).

Attitude toward the super-logoff

Participants' attitudes toward the super-logoff were investigated via three adapted items (e.g., "I think the super-logoff is a good idea") from the scale of the Technology Acceptance Model by Kuo and Yen (2009), which was originally used for measuring the attitude toward mobile phones. Participants responded on a 5-point Likert scale ranging from 1 = *I don't agree at all* to 5 = *I totally agree* ($\alpha = .883$).

Intention to use the super-logoff

The intended behavior of deactivating the Facebook profile was also measured via an adapted subscale by Kuo and Yen (2009), consisting of three items such as: "I plan to use the super-logoff in the future," on a 5-point Likert scale (1 = *I don't agree at all* to 5 = *I totally agree*, $\alpha = .792$).

Motives to use the super-logoff

To investigate the potential motives for using the super-logoff, several items asking for different reasons to potentially deactivate one's Facebook account were created and factorial analyses were calculated. Participants responded to the question: "For what reasons would you use the super-logoff instead of logging out the usual way?" on a 5-point Likert scale ranging from 1 = *I don't agree at all* to 5 = *I totally agree* (e.g. "I don't want to be searchable on Facebook"). To extract concrete motives for using the super-logoff, factorial analyses, following the criteria by Horn (1965), were conducted. A principal axis extraction with varimax rotation was executed. The number of factors was determined by comparing empirically found eigenvalues with given eigenvalues by Horn (1965). Four factors, which had an empirically found eigenvalue that was greater than the one by Horn (1965), were considered. Afterwards, a second factor analysis was conducted using principal axis extraction and promax rotation with a determined number of four factors. All factor loads can be found in Table 3. Subsequently, items with factor loads below .5 were excluded. One item loaded on a single factor (.558, "I don't think that Facebook is useful – I only have an account because it is popular"), which is why it was decided to exclude this item as well. Consequently, three main motives, namely, "avoidance of pressure" (five items, $\alpha = .789$), "protection from personal attacks" (eight items, $\alpha = .874$), and "avoidance of distraction" (two items, $\alpha = .821$) were identified.

Table 3

Factor loads of factor analysis examining the motives for using the super-logoff (Study 2).

	Factor			
	1	2	3	4
Avoidance of distraction ($\alpha = .821$)				
I want to find my peace from time to time.	.065	-.059	.628	.114
I don't want to be informed about everything my community does.	-.003	.006	.847	.047
I don't want to be distracted during working time.	.168	.277	(.478)	.162
I don't want my profile to be unattended when I am offline.	.279	.029	(.307)	-.342
Avoidance of pressure ($\alpha = .789$)				
Without the super-logoff I would feel forced to be online all the time.	-.101	.557	.494	-.081
I spend too much time on Facebook.	-.245	.775	.041	.077
I want to prove to myself that I am able to live without Facebook. (It causes me stress when I don't have my profile in mind.)	-.197	.534	.396	-.173
The flood of information is emotionally charging for me.	-.020	(.478)	.275	-.134
I had negative experiences with Facebook.	.050	.689	-.044	.213
	.102	.714	-.099	.418
Dissatisfaction with Facebook (items excluded)				
I don't think that Facebook is useful – I only have an account because it's popular.	.064	.054	.074	.558
I am unsatisfied with Facebook.	.251	.291	.282	(.439)
Protection against personal attacks ($\alpha = .874$)				
I do not want other people to be able to post negative comments on my Facebook wall at any time.	(.431)	.056	.222	-.147
I don't want to be searchable on the Internet.	.544	.023	.108	.146
I want to avoid that someone embarrasses me in the internet.	.524	-.003	.137	-.351
I don't think that Facebook is useful – I only have an account to gather information.	(.329)	.076	-.023	.242
I get too many mails and requests from Facebook.	.651	-.273	.250	.160
(I want to be able to directly react if someone tries to link me or post a photo of me.)	(.383)	.355	-.140	-.142
I don't want to be searchable before a job interview.	.757	.302	-.384	-.122
I want to protect myself against firestorms.	.586	.401	-.170	-.094
I don't want to push myself to the foreground.	.932	-.182	-.009	.084
I don't want to be like anyone else.	.758	-.131	.248	.116
I want to control who writes what at what time on my Facebook wall.	.776	-.078	-.016	.083

Note. Bold values indicate that the item was included in the analysis. Values and items in parentheses were excluded.

11.6.2 Sample

In sum, $N = 128$ participants took part in the online survey. One data set was excluded because it was incomplete and three outliers were excluded as well. In the end, 124 full data sets were considered for investigation (53% female). Participants were aged between 19 and 48 years ($M = 25.28$, $SD = 3.50$). Persons who already had experiences with the super-logoff ($n = 22$, 41% female) were aged between 20 and 36 years ($M = 25.55$, $SD = 4.07$).

11.7 Results

In the following, the descriptive statistics of Study 2 will be outlined. In the subsequent sections, calculations testing the stated hypotheses and research questions will be presented.

11.7.1 Descriptive Results

Privacy behavior

One hundred seventeen (94%) participants already had adapted their privacy settings at least once. Besides the super-logoff, self-reported measures used for privacy protection by participants (by means of free text inputs) were the Tor-browser or proxy-server, providing little or false information, hiding the timeline, “thinking before posting”, creating friend lists, and not providing a profile picture. Overall, 22 persons (18%) stated that they had already used the super-logoff. Four of the 22 persons even knew this strategy by name, while eight persons from the whole sample ($N = 124$) knew the strategy by name. Overall, 94 persons (76%) knew that it is possible to deactivate ones’ Facebook profile for using it as a privacy-regulating measure. However, three of the persons who already had experiences with using the super-logoff stated that they did not perceive this measure as a privacy regulating measure but rather as a “Facebook time-out”. This could indicate that privacy protection is not the only reason why people choose to temporarily deactivate their profiles. In sum, 105 persons stated they knew how to delete or deactivate their account (85%). Nine of those who already used the super-logoff only used the measure once, four persons used it twice, two persons used it three times and one person used it four times.

Intention and attitude toward using the super-logoff

The attitude towards using the super-logoff was medium to positive ($M = 3.43$, $SD = 1.06$), 52 persons (41%) thought that the super-logoff is a good strategy in general. However, only 39 participants (31%) thought that this strategy was a good method to guarantee privacy ($M = 3.50$, $SD = 1.15$). Although the measure was generally evaluated positively, 43 persons (34%, $M = 2.15$, $SD = 1.08$) stated that they probably would not use the super-logoff in the future.

Online privacy literacy

For calculating participants' online privacy literacy, the correct answers of the online privacy literacy scales were summed up for every person. Male participants reached OPLIS values between 85 and 122 ($M = 106.63$, $SD = 1.13$), displaying a mean value above average. Female participants reached values between 76 and 122 ($M = 103.63$, $SD = 1.26$), displaying a mean value above average as well. Descriptively, male participants had slightly better OPLIS values. Participants with unspecified sex reached values between 84 and 96 ($M = 90.50$, $SD = 2.75$), displaying a result below average.

Social networks

In addition to Facebook, most participants were also active on other social networks. Besides Facebook, the most popular network among participants was Instagram (63 persons of the whole sample and 15 persons of the subsample). Further networks participants engaged in were Pinterest (21 [4] persons), LinkedIn (12 [3] persons), Xing (32[6] persons), and Twitter (24 [7] persons). This is especially interesting when considering that the super-logoff is a measure to hide, because active accounts on additional networks seem to be contradicting to this function of the super-logoff. It will be referred to that in the discussion.

11.7.2 Testing of Hypotheses and Research Questions

Motives for using the super-logoff

To extract the motives for using the super-logoff, factorial analyses were conducted (*RQ1* and *RQ2*). Three motives were identified, namely, "avoidance of pressure," "protection from personal attacks," and "avoidance of distraction." Analyses of regression revealed strong positive relations between the motives for using the super-

logoff and the actual behavioral intention to opt-out of the network; avoidance of distraction: $R^2 = .234$, $F(1, 122) = 37.33$, $\beta = .48$, $p < .001$, avoidance of pressure: $R^2 = .138$, $F(1, 122) = 19.48$, $\beta = .37$, $p < .001$, protection against personal attacks: $R^2 = .181$, $F(1, 122) = 27.03$, $\beta = .43$, $p < .001$. According to Cohen (1988), all effect sizes were large.

For further investigation, a hierarchical analysis of regression was conducted. In the first block, the motive that correlated most strongly with the intention to use the super-logoff was included (avoidance of distraction). Subsequently, protection against personal attacks and avoidance of pressure were included as well. The first model was found to be statistically significant, $R^2 = .234$, $F(1, 122) = 37.33$, $\beta = .48$, $p < .001$, explaining 23% of the variance in the intention to use the super-logoff based on the motive avoidance of distraction. The effect is large. By adding the second motive, protection against personal attacks, into the second model, almost 30% of the variance in the intention to use the super-logoff could be explained with statistically significant results, $R^2 = .298$, $F(2, 121) = 25.70$, $\beta = .28$, $p < .001$, displaying a large effect. The third model that finally included the third factor, avoidance of pressure, did not yield statistically significant values, $R^2 = .307$, $F(3, 120) = 17.74$, $\beta = .11$, $p = .210$. In summary, all motives are positively correlated with the actual intention to use the super-logoff. However, when considering them together in one regression model, only avoidance of distraction and protection against personal attacks were found to be statistically significant predictors of participants' actual intention to deactivate their Facebook accounts.

The relation between self-disclosure and the intention to use the super-logoff

The more users disclose, the more they might perceive that they have to hide. Therefore, it was suggested that the extent of participants' self-disclosure is positively related to their intention to use the super-logoff (*H1*). A bivariate analysis of correlation was conducted. It revealed that there is in fact a statistically significant positive correlation between participants' self-disclosure behavior and their intention to use the super-logoff ($r = .29$, $p < .01$), supporting Hypothesis 1. According to Cohen's (1988) guidelines for interpreting effect sizes, this is a medium-sized effect.

The relation between privacy concerns and the attitude towards the super-logoff

Hypothesis 3 suggested a positive relation between privacy concerns and the attitude toward (using) the super-logoff. That is, it was supposed that the attitude toward the super-logoff can be traced back to users' privacy concerns. To test this hypothesis, a linear regression analysis was conducted. It revealed that the attitude toward (using) the super-logoff can be predicted by participants' concerns by about 17%, $R^2 = .17$, $F(1, 122) = 24.13$, $\beta = .41$, $p < .001$, supporting the third hypothesis. The effect size was large.

The relation between privacy concerns and the intention to use the super-logoff

In line with the finding that privacy concerns can be indirectly related to privacy intentions (Dienlin & Trepte, 2015), it was supposed that users' concerns might be a predictor of their intention to use the super-logoff (*H2*). An analysis of regression was conducted to test this assumption and revealed that participants' privacy concerns explained 15% of the variance in the intention to use the super-logoff, $R^2 = .15$, $F(1, 122) = 22.20$, $\beta = .39$, $p < .001$, displaying a medium-to-large effect size. Therefore, the second hypothesis was supported as well.

The relation between privacy literacy and the intention to use the super-logoff

In order to find out whether users' privacy literacy would be related to their intention to opt-out of the network, bivariate Pearson correlations were conducted. Analyses regarding the adapted OPLIS values and the intention to use the super-logoff did not show a relation between variables (*RQ3*). Neither a significant negative nor positive correlation between users' online privacy literacy and their intention to use the super-logoff was found ($r = .123$, $p = .175$). Answering the third research question, data showed that users' privacy literacy was unrelated to their intention to opt-out of the network.

The role of situational impression management behavior

In Hypothesis 4, it was assumed that the positive relation between the extent of participants' self-disclosure behavior and their intention to use the super-logoff (see *H1*) is influenced by their Facebook-related situational impression management behavior. Therefore, people's situational impression management behavior was regarded as a potential mediator for the relation between self-disclosure and the intention to use the

super-logoff. For analysis, the plugin PROCESS for SPSS by Andrew Hayes (1,000 bootstraps) was used. The model summary showed the a-path to be statistically significant, $b = 1.33$, $R^2 = .55$, $F(2, 122) = 150.33$, $p < .001$, LLCI = 1.1, ULCI = 1.54. The following model showed the b-path to be significant as well, $b = .03$, $R^2 = .11$, $F(2, 121) = 7.89$, $p < .05$, LLCI = .00, ULCI = .06, whereas the c'-path was not ($p = .46$, LLCI = -.03, ULCI = .08). There was no longer a direct effect of self-disclosure on the intention to use the super-logoff when users' situational privacy behavior was implemented, but a full mediation in terms of an indirect effect of self-disclosure on the intention to use the super-logoff was mediated by situational impression management behavior ($b = .94$, LLCI = .10, ULCI = 2.10). These values imply that situational impression management behavior mediates the relation between self-disclosure and the intention to use the super-logoff.

11.8 Discussion

The aim of Study 2 was to explore in what sense the super-logoff is known by German Facebook users and how many people are currently using it in order to regulate online privacy. Furthermore, it aimed at shedding light on the mechanisms related to the deactivation of one's Facebook account in terms of analyzing the motives for opting-out from the social network Facebook as well as corresponding attitudes, intentions, and concerns. Additionally, the role of users' online privacy literacy was investigated in order to illustrate potential relations between online privacy knowledge and the intention to opt-out of the network.

Descriptive results revealed interesting insights regarding participants' privacy behavior. Ninety-four percent of the sample adapted their privacy settings at least once, including all participants who already used the super-logoff ($n = 22$ persons). This might have led to the impression that users of the super-logoff do not perceive the super-logoff as an ultimate solution but rather as an extension of privacy protection (by adapting the settings). However, adapting the privacy settings once or twice does not imply that the person is highly engaged in privacy protection. Most users adapt their settings when they register for a network and then they maintain this setting. Ninety-five participants stated that they knew the functionality of the super-logoff (although not all knew the term super-logoff) as a privacy protective measure.

All participants had additional accounts on other online social networks, whereby most participants used Instagram. Thus, participants' self-disclosure activities do not only take place on Facebook. This is interesting against the background that users intend to opt-out of the network owing to reasons of privacy regulation (among others). The super-logoff does actually not prevent online privacy harms in general but covers instead those risks related solely to Facebook. Consequently, the question arises of whether users think that they need to be especially careful on Facebook while other social networks might be less dangerous. However, participants' were asked about the behavioral intention to opt-out of the network instead of measuring actual behavior. It might be conceivable that the reported intention would not be implemented into action in reality.

Motives for using the super-logoff (*RQ1* & *RQ2*)

Via factorial analyses, three main motives for using the super-logoff were identified, namely, protection against personal attacks, avoidance of pressure, and avoidance of distraction. However, only one motive can directly be associated with privacy protection motives, which is protection against personal attacks. Consequently, privacy motives might not be the only reason for users to use the super-logoff. It is open to investigation whether users who employ that measure driven by the motive avoidance of pressure are simply overwhelmed by the daily flood of information or whether they want to reduce stressful factors such as being continuously on the alert regarding potential privacy risks on the Internet. However, although almost half of the sample expressed that the super-logoff would be an adequate strategy, only 34% of the participants stated they would probably use the super-logoff (again) in the future. This is in line with findings from Study 1 in which it was found that people evaluate the idea of the super-logoff positively when hearing it for the first time but later conclude that the measure does not protect privacy sufficiently; it might instead soothe people's conscience.

Further motives suggest that people would like to avoid distractions by Facebook or to have some distance to the network. The question arises of why people do not choose to completely delete their accounts but reactivate it now and then. One consideration is that they still want to benefit from online networking and self-presentation (see Chapter 2.2 and Chapter 6.2.3) but feel overwhelmed with privacy issues and the flood of information (e.g., Eppler & Mengis, 2004; see Chapter 2.4). The motives for using the super-logoff should not only be considered as hiding from others but also as regulating

social affordances and avoiding exhausting regulatory measures manually. This study implies that the super-logoff can function as a retreat from social media threats.

The relation between self-disclosure and the intention to use the super-logoff (*H1*)

Analyses revealed a positive correlation between users' self-disclosure behavior and their intention to use the super-logoff. This is in line with findings by Krasnova, Günther, Spiekermann, and Koroleva, (2009) and Tufekci (2008), who stated, that people who disclose a lot of information might also be interested in reducing the risks that come along with the disclosures. However, the intention to protect the high amount of disclosed information does not always result in comprehensive protective behavior. In this study, participants reported having the intention to temporarily hide their profiles when they disclose too much information. Users might have the impression that they can rely on the super-logoff as a privacy buffer. If the account is deactivated from time to time, the user can continue disclosing information when he or she is online that cannot be accessed when the user does not want others to see it, namely, when he or she uses the super-logoff. When considering the privacy calculus (Culnan & Armstrong, 1999, see Chapter 5.2), the possibility to use the super-logoff might reduce the perceived risks, increase perceived controllability (see Debatin et al., 2009) and allow for semi-protected self-disclosure in order to still gather benefits such as social support. It might be sufficiently calming for users if they perceive to have at least some extent of control over their disclosures by using the super-logoff, indicating that the perception of control might be similarly satisfying as having real control (Debatin et al., 2009). This perception of control might function as a kind of free ticket for sporadic self-disclosures in an apparently semi-protected environment.

The relation between privacy concerns and the attitude toward the super-logoff

In *H2* it was suggested that a positive relation exists between participants' privacy concerns and their attitudes toward (using) the super-logoff. This hypothesis was supported. Dienlin and Trepte (2015) found in their studies that people who have strong privacy concerns do not like to provide identifiable information to their networks (informational privacy) and, further, people who are concerned regarding their online privacy have the opinion that it is better to have a restricted Facebook profile in order to regulate access for other people (social privacy). Dienlin and Trepte (2015) concluded

that privacy concerns influence users' privacy attitudes, which in turn influence their behavioral intentions to protect themselves. Similar results were attained in this study in the sense that privacy concerns influenced participants' attitudes toward a specific privacy-regulating measure (the super-logoff). People with privacy concerns may perceive a dilemma because they need to weigh up the risks and benefits of information disclosure (see Masur & Scharkow, 2016; Petronio, 2010). The privacy calculus states that users of online SNSs evaluate risks and benefits of information disclosure in order to assess whether it would be reasonable to disclose an information or not and whether to use protective strategies or not (Dienlin & Metzger, 2016; Krasnova & Veltri, 2010). Using the super-logoff can make the users perceive they hold the balance between contradicting needs or perceived risks and benefits because they are able to communicate with other people (i.e. benefits) but also to decide when other users can contact them, or in the worst case, damage their image on Facebook (i.e. risks) and directly react to it. This cognitive evaluation process can be one reason why people who are concerned about their privacy have a positive attitude about the super-logoff as a privacy protective measure.

The relation between privacy concerns and the intention to use the super-logoff

Analyses regarding *H3* revealed, that the intention to use the super-logoff can be predicted by participants' concerns by around 15%. This does not indicate actual behavior but gives insights into the effects of privacy concerns on privacy-related behavioral intentions (see also Dienlin & Trepte, 2015). The positive direct correlation between concerns and the intention to use the super-logoff indicates that concerns influence the self-reported behavioral intention to engage in this specific measure, whereby this does not imply that this intention is followed by actual privacy behavior in terms of actually using the super-logoff or engaging in even more protective strategies. In contrast to editing the personal privacy settings, using the super-logoff is related to lower cognitive effort because it is basically just one click. Comprehensive privacy behavior would indicate more activities such as controlling for informational, social and psychological privacy (Burgoon, 1982) by adapting friend lists, restricting access for specific persons or deleting sensitive information from one's profile. This would require privacy literacy (Trepte et al., 2015) and high motivation to translate concerns into protective actions (see also Study 1).

Since participants read an instruction explaining how to use the super-logoff during the survey, this might also have had an influence on perceived ease of use and have led to a spontaneous intention to use the super-logoff than to a sophisticated long-lasting behavioral intention for general privacy protection. Consequently, the super-logoff might be perceived to be an attractive and easy-to-adopt time-out for privacy concerns.

The relation between privacy literacy and the intention to use the super-logoff

Analyses regarding the third research question demonstrated that there was neither a positive nor a negative correlation between participants' privacy literacy and their intention to use the super-logoff. What is more, an explorative analysis of the relation between privacy literacy and the actual use of the super-logoff (calculation with the sub-sample $n = 22$) did not reveal significant results. This might be attributable to the small size of the sub-sample on the one hand and on some further restrictions regarding the examination of privacy literacy on the other hand. Since gathered data are based on an online study, there was no control regarding participants' responding behavior. Results for the online privacy literacy questionnaire (Masur, Teutsch, & Trepte, 2017) therefore could be distorted because participants could have searched on the Internet for the correct answer or asked other persons during the study. Interestingly, only four of the 22 participants who already used the super-logoff knew further protection measures. This would rather indicate low privacy literacy and indeed could have been an indicator of the assumption that people with low literacy tend to use the super-logoff because otherwise they would not know how to protect themselves. However, there were no significant results in the current study. People who know where to find the deactivation setting might at least have declarative privacy knowledge (see Trepte et al., 2015). They know that particular settings exist but they might not know how to implement all settings combined to guarantee privacy protection (i.e. procedural knowledge, Trepte et al., 2015).

The role of situational impression management behavior

The positive relation between self-disclosure and the intention to use the super-logoff was further investigated by considering people's situational impression management behavior as a mediating variable (*H4*). Analyses revealed that impression management behavior can in fact be considered as a mediator in this relation. By using

the super-logoff, users have the chance to manage their Facebook profiles in a more sophisticated manner. If they perceive the need to maintain a particular impression that might be endangered in a given situation, deactivating the account can be an adequate impression management strategy. Certainly, people with strong impression-managing motivations want many other people to notice their positive impression (Goffman, 1959), which makes it paradoxical to deactivate one's account at first glance. As already mentioned, users with a high impression management motivation tend to restrict the access to their online profiles less intensely (Utz & Krämer, 2009), probably so as to be seen and admired. However, users might also be concerned about someone destroying their formerly created positive image and therefore decide to use the super-logoff as an impression management strategy. This explanation also fits with the findings of *HI*, in the sense that the extent of self-disclosure (e.g., for impression management motives) is related to the intention to use the super-logoff. Users' need to have the visibility of their profiles in their own hands strongly depends on their impression management motivation and can explain the mediating effect of impression management behavior on the relation between self-disclosure and the intention to use the super-logoff.

11.9 Limitations and Future Work

Future studies should consider bigger samples including people who already used the super-logoff allowing for more comprehensive conclusions regarding users' actual behavior. Since most participants were recruited through Facebook itself, it is possible that some people who use the super-logoff were actually offline during the time of recruitment. Therefore, more alternative recruitment channels should be used. Furthermore, a long-term study would provide the most useful insights because users' actual logoff behavior would be detectable. Moreover, people's perceived control was not directly investigated but a relation between using the super-logoff and perceived control was assumed based on current findings. Future studies should examine people's actual perceived control concerning their online privacy in order to draw more concrete conclusions. The role of perceived control and users' general self-control will be further investigated in Study 3 and Study 4. Most interestingly, people used the super-logoff not only for obvious privacy protection reasons but also for having a Facebook time-out. Future studies should investigate whether such a time-out might also be an indirect

privacy protection reason. It is conceivable that people need this time-out because otherwise they are constantly concerned and worried about risks such as impression damages or being observed. Furthermore, the intensity and frequency of Facebook usage by those users who perform the super-logoff might be of further interest. There might be a difference in the motives for using the super-logoff between high-frequency and low-frequency users.

11.10 Conclusion

The super-logoff is one of the most radical and ultimate self-regulating strategies for controlling one's online presence. To date, research has not considered this method systematically in a quantitative way, which was identified as a major disadvantage. Although danah boyd presented a body of qualitative research on this measure, it has been neglected by numerous studies regarding online privacy protection. According to the data of the current study, people intend to use this strategy to protect and maintain their privacy but also to allow themselves a time-out, possibly from privacy concerns. People seem to perceive to have more control over their profile and over potential risks when using the super-logoff. Still, analyses revealed the importance of considering privacy protection in an even more differentiated way. So far, privacy has been defined as a reciprocal process of withdrawing and disclosing information, related to different dimensions of privacy and potential privacy violations (see Dienlin & Metzger, 2016; Masur & Scharkow, 2016). The motive of allowing oneself a time-out from concerns and pressures can contribute to a feeling of privacy, too. Social media applications and SNSs are ubiquitous so that withdrawing in terms of distancing from the whole network from time to time instead of solely withdrawing specific pieces of information needs to be considered as a further privacy protection motive in online privacy research. In conclusion, Study 2 points out different motives for using a self-regulating privacy protection measure and demonstrates relations between opting-out of the network and users' attitudes, intentions, concerns, and impression management motivations. This study contributes to privacy research in terms of considering alternative protection strategies that are often neglected when analyzing privacy behavior.

Summary Study 2

As outlined in Chapter 2.2, the myriad of disclosed information on online SNSs makes it more important than ever to focus on users' awareness of online privacy and measures employed for privacy protection. Study 2 investigated the fact that some users implement self-developed risk-reducing strategies such as temporarily deactivating their Facebook account. Analyses revealed a positive relation between privacy concerns and the attitude toward the super-logoff as well as between privacy concerns and behavioral intentions to use the super-logoff. Moreover, Study 2 revealed self-disclosure behavior to be positively correlated with the intention to use the super-logoff, mediated through situational impression management behavior. Three different motives for deactivating ones' Facebook account have been identified, namely, avoidance of distraction, avoidance of pressure, and protection against personal attacks. In sum, Study 2 as well as Study 1 revealed that users of SNSs seek for alternative protection strategies in order to have more comfortable online experiences. Both studies indicate that participants indeed wish for more privacy protection. Strikingly, the desire for protection does not induce comprehensive protection efforts. In order to examine whether derived requirements from Study 1 and knowledge regarding users' concerns which go hand in hand with the intention to opt-out of an online social network from Study 2, an experimental investigation regarding the impact of privacy interventions as they were derived from users' desires in Study 1 was conducted (Study 3). Study 3 aimed at combining knowledge regarding users' desire for particular protective features with users' privacy related personal traits, needs and concerns.

V THE IMPACT OF PERSUASIVE PRIVACY SUPPORT MEASURES ON USERS' ACTUAL PRIVACY BEHAVIOR

In the context of this dissertation, the idea of utilizing system-based privacy support in terms of warning messages or prompts occurring in real-time within users' social network environments is not only addressed from a psychological perspective but also from a software engineering viewpoint. Specifically, the topic of self-disclosure in social media and the opportunity for supportive and user-centered self-adaptive systems was approached by means of an interdisciplinary consideration of users' desires concerning privacy support (see Study 1) and the systems' possibilities and preconditions (see Chapter 8). In the context of these efforts, a self-adaptive awareness system was suggested that is able to monitor users' sharing habits and intervene if the disclosed information is highly sensitive and hypothetically could induce privacy harms (Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016). It was proposed to consider a system-based notification system that interacts with a user who is going to disclose information by means of a feedback-loop in the sense that the system informs the user regarding potential harms related to the potentially shared information. Thereby, the user has the ability to either adopt behavior or ignore the notification. The declaration of particular information as sensitive or not sensitive would be based on underlying knowledge that includes rules for identifying the sensitivity of information on the basis of prior research (see Chapter 3.3). The functionality of self-adaptability of the support system was suggested in order to provide a satisfying usability and suitable feedback due to taking the users activities and their responses to the recommendations into account. As outlined in Chapter 8.2, system notifications would be based on a loop between the user input (a potential posting), and the monitoring, analyzing, planning, and executing phase of the system (providing the user with the information that potential harms might happen based on publishing the posting). The implementation of such a system would require high technical effort in terms of providing functioning databases and algorithms for processing data and giving suitable recommendations. Besides these technical requirements, users' desires for technical privacy support would also need to be met, for instance, the transparency, and user-friendliness of the system in order not to be annoying but helpful and trustworthy (see Study 1). Study 1 revealed that users' in fact

can imagine using a system that provides adapted privacy feedback. However, in Study 1, insights regarding users' willingness to utilize such a measure were only given through self-reported intentions. Therefore, Study 3 will examine users' actual behavior when being notified about potentially dangerous self-disclosure by a system by means of an experimental investigation. In this study, the privacy notifications provided (persuasive privacy prompts) were not fully functional adapted support methods based on algorithms, but dynamic notifications based on the kind of users' self-disclosed information in a self-developed registration form of an SNS. Therefore, it was predefined which kind of information was considered as sensitive (e.g., political attitude) in order to decide for which disclosed information a privacy notification would be given. In the following chapter, an experimental study about the effectiveness of such privacy notifications in terms of persuasive privacy prompts and potentially influencing personality traits will be reported and implications for practice will be given.

12 Study 3: Do You Really Want to Disclose This? - Examining User-Oriented Variables that Influence the Impact of Persuasive Privacy Prompts for Reducing Online Privacy Risks

As stated in Chapters 8.5 and 8.6, the advantage of utilizing nudges and prompts for behavioral changes with regard to online privacy protection is that they can raise users' awareness by calling their situational attention. Given that there is a lack of knowledge about which user-specific characteristics such as need for privacy or need for popularity (see Chapter 6.1) influence the impact of privacy protection measures, Study 3 focuses on effects of system-based persuasive privacy prompts on actual privacy behavior. More precisely, Study 3 aims at analyzing the influence of persuasive privacy prompts that are formulated alongside specific persuasive styles (i.e. authority or consensus; see Kaptein et al., 2012) on users' actual privacy behavior (i.e. self-disclosure or withdrawal). Moreover, this study examines whether persuasive privacy prompts will be more effective (i.e. users provide less sensitive information) if prompts contain reasons for respective suggestions, as it was derived to be one requirement for trustworthy privacy

support from Study 1. Following these aims, users' actual privacy behavior after receiving persuasive privacy prompts in a non-artificial social network environment is investigated in this study. In sum, it is strived to learn about relevant user-oriented variables influencing the effects of persuasive privacy prompts and appropriate measures for empowering users of SNSs.

12.1 Increasing Privacy Through Reasoned Persuasive Prompting

The privacy support concept that is introduced in Study 3 focuses on persuasive and informative nudging and prompting. To be more precise, it is argued that prompts are even more effective if they consider particular persuasive strategies. As outlined in Chapter 8.5, persuasion can be considered as a promising method for increasing users' engagement in behavioral changes and actions for different areas, for instance, energy saving (e.g., Kappel & Grechenig, 2009) or regarding a healthier lifestyle (e.g., Kaptein, et al., 2012). In Study 3, persuasive strategies for the realm of online privacy protection will be examined.

Kaptein and colleagues (2012) investigated the effects of tailored persuasive messages for inducing behavioral changes, more precisely, to reduce unhealthy snacking behavior. They found that persuasive messages that are adapted to a user's preferred persuasive style are more efficient than non-adapted messages. According to Kaptein and colleagues (2012), there are six main strategies that can be used for persuading a person, namely, reciprocity, scarcity, authority, commitment, consensus, and liking. For their study, Kaptein and colleagues (2012, p. 10:11) created persuasive messages such as "The World Health Organization advises not to snack. Snacking is not good for you" (authority) or "Everybody agrees: not snacking between meals helps you to stay healthy" (consensus). The most relevant persuasive strategies in the case of the current study are authority and consensus because they are most closely transferrable to privacy-related decisions, not at least illustrated through respective items for investigating the preference for these strategies (e.g., authority: "I am very inclined to listen to authority figures", consensus: "I often rely on other people to know what I should do"). With the help of persuasive strategies, potential privacy risks of particular actions (e.g., sensitive information disclosure on SNSs) can be presented even more convincingly, which might increase the likelihood that the presented privacy-related information is processed and

implemented into protective action by individuals (e.g., presentation ; Acquisti et al., 2017).

Users' characteristics and privacy behavior

As already stated in Chapter 6.2, users' online privacy behavior can depend on various personal characteristics and traits (Ahn, Kwolek, & Bowman, 2015; Baek, Kim, & Bae, 2014; Bansal, Zahedi, & Gefen, 2016; Junglas, Johnson, & Spitzmüller, 2008). Therefore, with regard to the impact of persuasive privacy prompts on users' behavior, it was focused on the influence of those personality characteristics that have oftentimes been identified to be related to privacy behavior, namely users' need for privacy and popularity (e.g., Hofstra, Corten, & van Tubergen, 2016; Yao, Rice, & Wallis, 2007) as well as their expression of vulnerable and grandiose narcissism (e.g., Ahn, Kwolek, & Bowman, 2015). Users behavior was examined by means of an experimental setting in which participants interacted with a registration form of an SNS that provided persuasive privacy prompts if users disclosed information. The concrete setting will be explained in the following paragraph.

12.2 Setting: The Social Network Site

For Study 3, a registration form of a social network for students was developed. The experimental functionality of the network was to provide persuasive privacy prompts if a user was going to disclose sensitive information (i.e. information referring directly to him- / herself) during the process of registration. Overall, there were 17 text input fields (e.g., *name* or *birthdate* as well as free text fields asking for a personal or political statement), ten checkbox menus and four radio button menus (e.g., asking for religion or politics), allowing for disclosing various kinds of information regarding potentially sensitive topics concerning different dimensions of privacy. Overall, each participant had the chance to provide 32 inputs in free-text input fields, checkbox menus or radio button menus. In order to investigate users' behavior regarding particular dimensions of privacy, disclosures regarding the different dimensions of privacy (informational, social, psychological; see Burgoon, 1982) were sought through the provided input spaces and questions that have been stated. However, the social dimension is only distantly covered in this study through the information regarding the social life and contact (or distance,

respectively) to other people, for instance, by asking for stays at the university and meeting other people, indicating insights into the regulation of distance and proximity to others (i.e. people who are rarely at the university or seldom go to parties might need to engage less in distance or proximity regulation than people who meet others more frequently). Based on prior research (Burgoon, 1982; Wang et al., 2011), the following six categories of content were supposed to be sensitive and consequently considered for prompting:

- (1) Contact information (e.g., birthdate) and (2) work and education (e.g., side job), both relating to informational privacy.
- (3) Leisure time (e.g., partying) and (4) availability at university (e.g., available at Mondays), both distantly attributable to social privacy.
- (5) User details (e.g., describe yourself) and (6) religion and politics (e.g., partisanship), both relating to psychological privacy.

Privacy prompts were only provided if a user entered information to an input field of one of these categories. For every category, two prompts occurred at maximum. Within the categories of interest, the prompts occurred randomly for different input fields. It was decided to provide two further categories allowing for disclosures in which no prompts appeared in order to disperse the situation and avoid information overload for participants. These additional categories were music and films and social media preferences. In an even distribution, all participants were randomly assigned to conditions with different persuasive privacy prompts (authority/consensus/authority with additional information/consensus with additional information/no prompt [control group], see Table 4).

Table 4
Absolute numbers and percentages of participants in each experimental group (Study 3).

	<i>n</i>	%
Authority	37	19.8
Authority with information	38	20.3
Consensus	37	19.8
Consensus with information	38	20.3
Control	37	19.8
Total	187	100.0

In order to provide suitable feedback and to make the prompts more credible, the prompts were also adapted to the dimension of privacy associated with the disclosed information. Therefore, they differed slightly in the formulation. The formulation of persuasive privacy prompts was adapted to persuasive messages by Kaptein and colleagues (2012). For instance, it was written:

“Rethink what you are going to provide. Privacy researchers from Harvard University identify the disclosure of your contact information as highly sensitive!” (authority, informational privacy) or *“Everybody agrees: To protect your privacy you should pay attention to what contact information you reveal on the Internet! Thus, reflect on what you disclose”* (consensus, informational privacy). Provided reasoning was for example: (...) *“Because you don’t have control over the further processing of your identifying data anymore”* (informational reasoning) or (...) *“Because you don’t have control over the further processing of your attitudes and emotions regarding sensitive topics anymore”* (psychological reasoning) (see Figure 4). For an extensive overview over all prompt messages see Table 5.

Table 5
Overview of the persuasive privacy prompts (Study 3).

	Authority	Consensus
Informational privacy	“Rethink what you are going to provide. Privacy researchers from Harvard University identify the disclosure of your contact information as highly sensitive!”	“Everybody agrees: To protect your privacy you should pay attention to what contact information you reveal on the Internet! Thus, reflect on what you disclose”
Reasoning	“(…) Because you don’t have control over the further processing of your identifying data anymore”	“(…) Because you don’t have control over the further processing of your identifying data anymore”
Social privacy	“Rethink what you are going to provide. Privacy researchers from Harvard University identify the disclosure of information regarding your private social life as highly sensitive!”	“Everybody agrees: To protect your privacy you should pay attention to what information regarding your private social life you reveal on the Internet! Thus, reflect on what you disclose”
Reasoning	“(…) Because you don’t have control over the further processing of the information regarding your private social life anymore”	“(…) Because you don’t have control over the further processing of the information regarding your private social life anymore”
Psychological privacy	“Rethink what you are going to provide. Privacy researchers from Harvard University identify the disclosure of your personal attitudes and emotions as highly sensitive!”	“Everybody agrees: To protect your privacy you should pay attention to what information regarding your attitudes and emotions you reveal on the Internet! Thus, reflect on what you disclose”
Reasoning	“(…) Because you don’t have control over the further processing of your personal attitudes and emotions regarding sensitive topics anymore”	“(…) Because you don’t have control over the further processing of your personal attitudes and emotions regarding sensitive topics anymore”

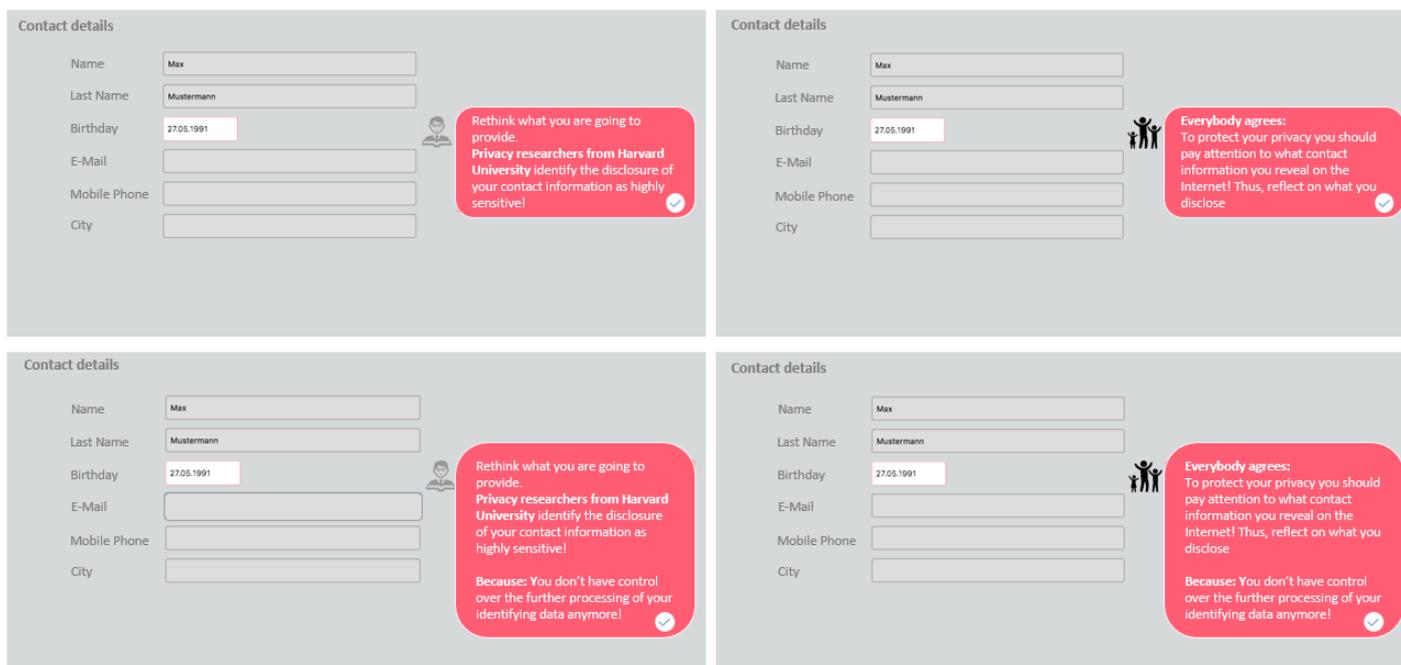


Figure 4: Persuasive privacy prompts (Study 3).

12.3 Hypotheses

Based on the reported research findings, the following hypotheses concerning users' privacy behavior were stated. In all hypotheses, *privacy behavior* is defined as disclosing no/only sparse sensitive information. In line with reported studies regarding the effectiveness of persuasive messages by Acquisti and colleagues (2017), Wang and colleagues (2013), and Kaptein and colleagues (2012), this work hypothesizes that a persuasive privacy prompt can influence users' actual privacy behavior in terms of withdrawing sensitive information. It is assumed that users' disclosure behavior is interrupted by the prompt intervention and that their attention is drawn to the persuasive privacy prompt and in consequence on current privacy behavior. Therefore, the following hypothesis states:

Hypothesis 1 (H1): Participants receiving persuasive privacy prompts disclose less information than participants receiving no persuasive privacy prompt.

In line with Kaptein and colleagues (2012), the impact on participants' privacy behavior depending on the persuasive style of the provided privacy prompts was expected. Persuasive styles can induce behavioral changes varying in persistence and

general impact. This can, for instance, depend on varying susceptibility to persuasive styles across individuals (Kaptein et al., 2012). There is little knowledge regarding the effectiveness of persuasive styles for privacy protection measures. In this study, it was hypothesized that there is a difference in behavioral outcomes depending on the persuasive style. It was aimed at finding out which style is most effective for this realm. Consequently, the following hypothesis states:

Hypothesis 1a (H1a): There is a difference in privacy behavior depending on the persuasive style (authority/consensus) of the persuasive privacy prompt received.

Furthermore, the persuasive privacy prompt is suggested to be more effective if it contains additional information justifying the behavioral privacy suggestion. This is due to the finding that people wish to have information regarding personal suggestions given from a supporting entity (Acquisti et al., 2017; see Study 1). Since people like to act based on reasoned considerations (e.g., Fishbein, 1979), the likelihood of adopting a suggestion within a persuasive privacy prompt might increase if it is reasoned, resulting in the following hypothesis:

Hypothesis 1b (H1b): Participants receiving persuasive privacy prompts including reasoning (a) disclose less information and (b) change their disclosures more frequently than participants receiving persuasive privacy prompts without reasoning.

As was revealed by Kaptein and colleagues (2012), behavioral suggestions are even more effective if they are formulated in line with a person's preferred persuasive style. That is, a persuasive message formulated in a communication style to which a person is susceptible to will more likely lead to the behavioral outcome intended by the message. Therefore, it is hypothesized that the impact of the persuasive privacy prompt on subsequent behavior is moderated by the evaluation of the persuasive style that is used in the persuasive privacy prompt:

Hypothesis 2 (H2): The impact of persuasive prompts on the number of changes is moderated by users' susceptibility to the persuasive styles (authority / consensus).

Following findings by Ahn, Kwolek, and Bowman (2015), Utz, Tanis, and Vermeulen (2012), and assumptions by Buss (2001), it was hypothesized that users' privacy behavior depends on their personality, namely, narcissism, need for popularity, and need for privacy (see Chapter 6). In a prior study, it was revealed that the intention to control for one's online privacy is higher for vulnerable narcissistic persons than for grandiose narcissistic persons (Ahn, Kwolek, & Bowman, 2015). Furthermore, this work suggests that users with a high need for privacy tend to control their online actions more intensely (e.g., Blanchio, Przepiorka, Boruch, & Balakier, 2016) than do users with a high need for popularity, since privacy control in terms of reduced self-disclosure decreases possibilities for receiving positive feedback by other persons and consequently decreases popularity. These assumptions led to the following hypotheses:

Hypothesis 3a (H3a): Users' need for privacy and expression of vulnerable narcissism positively influence their privacy behavior.

Hypothesis 3b (H3b): Users' need for popularity and expression of grandiose narcissism negatively influence their privacy behavior.

Since users' personality can influence online privacy behavior and disclosure habits, the impact of the provided privacy prompts on users' behavior might be positively or negatively affected by their personality traits. In line with this, the effect of the persuasive privacy prompts on current privacy behavior is hypothesized to be moderated by users' personal characteristics:

Hypothesis 4 (H4): The impact of persuasive privacy prompts on users' privacy behavior is moderated by their (a) need for privacy, (b) need for popularity, (c) vulnerable narcissism, and (d) grandiose narcissism.

Hypothesis (H4a): A greater need for (a) privacy and (b) vulnerable narcissism will intensify the effect of the persuasive privacy prompt on users' privacy protective behavior.

Hypothesis (H4b): A greater need for (c) popularity and (d) grandiose narcissism will diminish the effect of the persuasive privacy prompt on users' privacy protective behavior.

Following the findings by Dienlin and Trepte (2015) and the definition of privacy by Burgoon (1882), this work argues that privacy behavior differs regarding the dimension of privacy of disclosed information and associated privacy concerns, attitudes and intentions. Furthermore, persuasive privacy prompts might have different effects on privacy behavior, depending on the privacy dimension that is going to be violated and corresponding privacy intentions, concerns, and attitudes of the users:

Hypothesis 5 (H5): Users' informational, social, and psychological privacy behavior (i.e. withdrawal of informational, social, psychological privacy-related information) is positively correlated with their informational, social, and psychological privacy concerns, attitudes, intentions, and self-reported privacy behavior.

12.4 Method

To analyze psychological mechanisms that influence the effects of persuasive privacy prompts and users' actual privacy behavior in a non-artificial environment, an experimental study with a 2×2 design (varying the persuasive style and presence of reasoning) and a control group (no prompt) in which participants interacted with a self-developed SNS was conducted. Participants came to the laboratory and were told that, for reasons of usability testing, they would be carrying out a registration process for a new social network for students of the university. Participants did not know that the prompts were a pivotal element of the investigation. They were also told that they did not have to enter all information but that they should act as naturally as possible. Otherwise, the contradiction between the task to disclose and the warning not to disclose would have been too drastic. In an even distribution, all participants were randomly assigned to experimental manipulations with different persuasive privacy prompts. Participants either got a student credit or ten euros for participating. They were recruited via online forums, SNSs, and advertisements on the university campus. A local ethics committee approved all the conditions.

12.4.1 Measures

Susceptibility to persuasive strategies

Participants' susceptibility to persuasive strategies was measured by means of the Susceptibility to Persuasion Scale (Kaptein et al., 2012), consisting of six principles (reciprocity, scarcity, authority, commitment, consensus, liking) and 32 items in total ($\alpha = .794$). The principles of interest for this study consisted of six items for *authority* (e.g., "I am very inclined to listen to authority figures," $\alpha = .580$) and five items for *consensus* (e.g., "I often rely on other people to know what I should do," $\alpha = .709$) and were rated on a 7-point Likert scale ranging from 1 = *completely disagree* to 7 = *completely agree*.

Narcissism

The scale for measuring vulnerable narcissism (Hendin & Cheek, 1997) included ten items such as, "I easily become wrapped up in my own interests and forget the existence of others." Each statement was rated on a 7-point Likert scale ranging from 1 = *strongly disagree* to 7 = *strongly agree* ($\alpha = .741$). Grandiose narcissism was investigated through adapting the NPI-16 short measure of narcissism by Ames, Rose, and Anderson (2006). Participants rated statements on semantic differentials, ranging from 1 = *narcissism-consistent* (e.g., "Everybody likes to hear my stories") to 4 = *narcissism-inconsistent* (e.g., "Sometimes I tell good stories"). Testing for reliability revealed a satisfactory value of $\alpha = .833$.

Need for popularity

Participants' need for popularity was investigated via the scale by Utz, Tanis, and Vermeulen (2012), consisting of eight items, for instance, "I would do almost anything to not be perceived as a loser" ($\alpha = .788$). Statements were rated on a 5-point Likert scale ranging from 1 = *I don't agree at all* to 5 = *I totally agree*.

Need for privacy

In this study, the scale by Buss (2001), including the dimensions self-disclosure (e.g., "I find it hard to talk about myself," $\alpha = .662$), concealment (e.g., "I don't like to do a phone call if others in the same room could listen to me," $\alpha = .704$), and personal space (e.g., "I prefer working alone than in the company of others," $\alpha = .766$) was used.

Statements were rated on a 7-point Likert scale ranging from 1 = *I totally disagree* to 7 = *I totally agree*.

Privacy attitudes

The privacy attitudes were investigated using the items by Dienlin and Trepte (2015). Participants' attitudes were investigated by means of semantic differentials (e.g., from 1 = *not useful* to 7 = *very useful*) separated into informational (e.g., "I think that giving information on FB that identifies me is...", $\alpha = .875$), social (e.g., "I think that restricting access to one's FB profile is...", $\alpha = .878$) and psychological (e.g., "I think that communicating personal information is...", $\alpha = .903$) privacy attitudes. Low values for informational and psychological privacy attitudes indicate strong privacy attitudes, whereas strong social privacy attitudes are indicated by high values.

Privacy intentions

Privacy intentions were measured with items by Dienlin and Trepte (2015) as well. Participants had to display their agreement or disagreement (either *none–very much*, *not at all–very much*, or *very impersonal–very personal*) on a 7-point Likert scale for each, informational (e.g., "How much identifying information do you currently want to provide on Facebook?" $\alpha = .826$), social (e.g., "How strongly do you want that the visibility of content on your Facebook profile is restricted?" $\alpha = .862$), and psychological privacy (e.g., "How personal do you want your Facebook profile to be?" $\alpha = .788$) intentions. Low values for informational and psychological privacy intentions demonstrate strong privacy intentions, whereas strong social privacy intentions are indicated by high values.

Self-reported privacy behavior

Items for investigating participants' self-reported privacy behavior also stem from Dienlin and Trepte (2015). Participants rated on a 7-point Likert scale how strongly they agree or disagree with certain statements regarding informational (e.g., "How much identifying information have you now posted on an SNS?" $\alpha = .844$), social (e.g., "How strongly is the visibility of content on your SNS profile restricted?" $\alpha = .722$), and psychological (e.g., "How personal is your SNS profile?" $\alpha = .846$) privacy behavior,

following the same scheme as for privacy intentions. Low values for informational and psychological privacy behavior demonstrate strong privacy behavior, whereas strong social privacy behavior is indicated by high values.

Privacy concerns

Items for privacy concerns were adapted to the privacy measures by Dienlin and Trepte (2015). Instead of using unspecified items asking for general privacy concerns, items for informational (e.g., “How concerned are you to provide identifying information about yourself on your profile on a social network?”, $\alpha = .775$), social (e.g., “How concerned are you to be visible for strangers through your online profile?” $\alpha = .804$), and psychological (e.g., “How concerned are you regarding other persons getting to know your personal emotions, thoughts and values?”, $\alpha = .772$) concerns (each three items) were created. No items are recoded. Items are reported in Table 6.

Table 6
Items measuring privacy concerns regarding different dimensions of privacy (Study 3).

	Informational	Social	Psychological
1	How concerned are you about revealing identifying information about yourself on your social network profile?	How concerned are you if you don't limit your FB profile?	How concerned are you about communicating personal things to your FB community?
2	How concerned are you that strangers are misusing the information from your FB profile?	How concerned are you about being visible to strangers through your profile?	How concerned are you that your profile accurately reflects your personality?
3	How concerned are you that your identifying information will be stolen?	How concerned are you if you do not restrict your FB profile for certain people?	How concerned are you that strangers also learn about your emotions, thoughts and values?

Actual privacy behavior

The pivotal dependent variable was users' actual privacy behavior. Therefore, participants' inputs in respective fields, selections of radio buttons and check boxes were stored before and after receiving a prompt so that it was possible to analyze the differences between behavior_{t1} and behavior_{t2} (i.e. the changes of disclosures). The number of changes after receiving a prompt was documented for modifications in each, informational, social, and psychological privacy-related fields. Therefore, a score for all

changes in total as well as the changes regarding each privacy dimension was available for analyses. These values were not considerable for all users because there was also a control group who received no messages. However, a second variable representing participants' privacy behavior was considered, namely, the number of empty fields at the end of the registration process. More empty fields implied more aware privacy behavior in terms of providing less information (applicable for all groups).

Future usage

With six self-developed items, users' individual intention regarding future usage of a privacy system that would provide persuasive privacy prompts as presented in the study was measured. Participants responded on a 5-point Likert scale ranging from 1 = *I don't agree at all* to 5 = *I totally agree* ($\alpha = .748$, e.g., "The prompts would certainly help me in the future to pay more attention to my privacy," or "The prompts would probably annoy me" [recoded]). For an overview of all items, see Table 7.

Table 7

Items for measuring intended future usage of a privacy support system (Study 3).

I would be happy to see such or similar prompts in the future on my social network online.

The prompts would certainly help me in the future to pay more attention to my privacy.

The prompts would probably annoy me. (r)

If the prompts were different, they would certainly help me.

The prompts make no sense in my opinion. (r)

The prompts would be helpful for other people, but not for me. (r)

Note. (r) indicates reversed items.

Evaluation of persuasive privacy prompts

Users' evaluation of the persuasive privacy prompts was measured by means of items on an 11-point-Likert Scale ranging from 1 = "I don't agree at all" to 11-point Likert scale ranging from 1 = *I don't agree at all* to 11 = *I totally agree* ($\alpha = .888$, e.g., "helpful," "supportive," "annoying," "irritating"). For an overview of all items, please refer to Table 8.

Table 8
Items evaluating the persuasive privacy prompts (Study 3).

1	Helpful
2	Supportive
3	Disturbing (r)
4	Instructive
5	Useful
6	Informative
7	Annoying (r)
8	Unnecessary (r)
9	Redundant (r)
10	Desirable
11	Restrictive (r)
12	Irritating (r)

Note. (r) indicates reversed items.

Effects of findings are reported in terms of correlation coefficients (r) for correlation analyses and β -values for regression analyses. Following Field's (2009) guidelines for effect size classification, a value of .10 was considered small, .30 medium and .50 large. The partial eta-squared (η_p^2) demonstrates the effects for analyses of variance and can be interpreted as follows: small effect for $\eta_p^2 = .01$, medium effect for $\eta_p^2 = .06$, and large effect for $\eta_p^2 = .14$ (Cohen, 1988).

12.4.2 Sample

Two hundred and four persons participated in this experimental study. After excluding cases with missing data and outliers (regarding age), the sample consisted of 191 full data sets. However, owing to manipulation checks that asked if participants recognized the persuasive privacy prompts or not, four further cases needed to be deleted resulting in a final sample size of $N = 187$ participants. Most of them were students ($n = 177$). One hundred and sixty-four participants studied at the university where the experiment was conducted, 13 studied at another university. Two persons were research associates and eight persons stated to do something else. They were aged between 18 and 40 years ($M = 22.96$, $SD = 3.55$) and 68% of the sample was female ($n = 127$). The sample was subdivided into five groups, whereof four groups were exposed to privacy prompts with different persuasive styles (authority, consensus, authority with reasoning, consensus without reasoning) and one group did not receive privacy prompts (control group). Descriptive statistics with regard to age and sex for each experimental as well as the control group are summarized in Table 9.

Table 9

Descriptive statistics of participants for all experimental groups (Study 3).

	Authority	Authority with reasoning	Consensus	Consensus with reasoning	No prompt	Full sample
Age	$M = 24.03$ $SD = 4.41$	$M = 22.97$ $SD = 3.16$	$M = 21.97$ $SD = 2.55$	$M = 22.46$ $SD = 3.77$	$M = 23.41$ $SD = 3.44$	$M = 22.96$ $SD = 3.55$
Sex	32% male 68% female	37% male 63% female	27% male 73% female	42% male 58% female	22% male 78% female	32% male 68% female
<i>n</i>		75		75	37	187

All persons used at least one online social network, mostly Facebook ($n = 183$), Instagram ($n = 119$), and Snapchat ($n = 83$). Social networks used by test subjects and absolute numbers of users for each are represented in Figure 5.

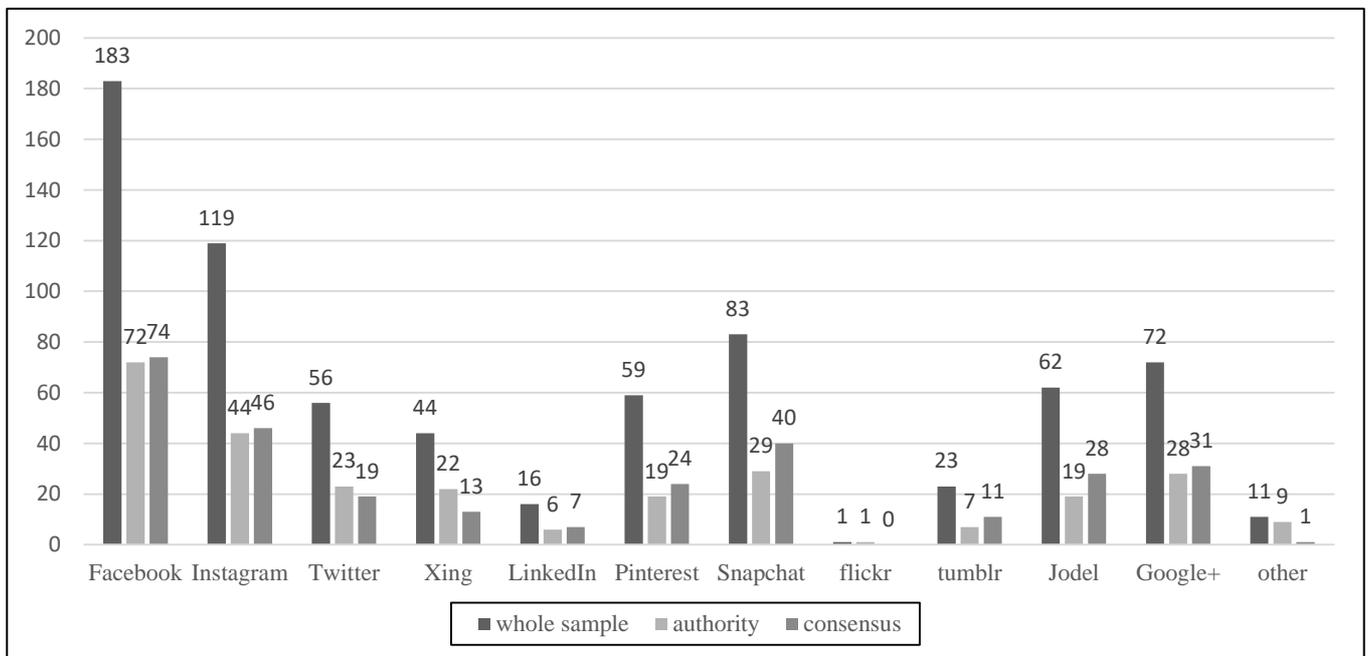


Figure 5: Absolute numbers of participants using the specific SNS (Study 3).

12.5 Results

In this study, privacy behavior was examined by means of two variables. On the one hand, privacy behavior was operationalized as the number of changes in input fields in the registration form after being exposed to persuasive privacy prompts (only available for $n = 150$ because there was one control group who did not receive prompts). On the other hand, privacy behavior was operationalized as the amount of empty input fields in the end of the registration process, including all input spaces such as text fields,

checkboxes, and radio-buttons (available for full sample, $N = 187$). One-hundred-sixty-seven changes ($M = 1.11$, $SD = 1.01$) were made by those participants who were in experimental groups receiving persuasive privacy prompts ($n = 150$). Eighty-eight changes were made by participants in the group receiving prompts in an authoritarian style ($M = 1.17$, $SD = .99$, $n = 75$) and 79 changes by participants in the group receiving prompts in a consensual style ($M = 1.05$, $SD = 1.04$, $n = 75$). The total number of empty fields for all participants in the end was 2607 ($M = 13.94$, $SD = 6.09$, $N = 187$). Participants in the group receiving authoritarian prompts ($n = 75$) left 1145 fields empty ($M = 15.26$, $SD = 5.61$), and participants in the group receiving prompts in the consensual style ($n = 75$) left 1089 fields blank ($M = 14.52$, $SD = 6.11$). In the control condition ($n = 37$) the total number of empty fields was 373 ($M = 10.08$, $SD = 5.54$). All absolute numbers of changes and empty fields for male and female participants of each group are represented in Figure 6 and Figure 7. For reasons of clarity, the experimental groups will be referred to as *authority*, *authority with reasoning*, *consensus*, *consensus with reasoning*, and *control group* in the following.

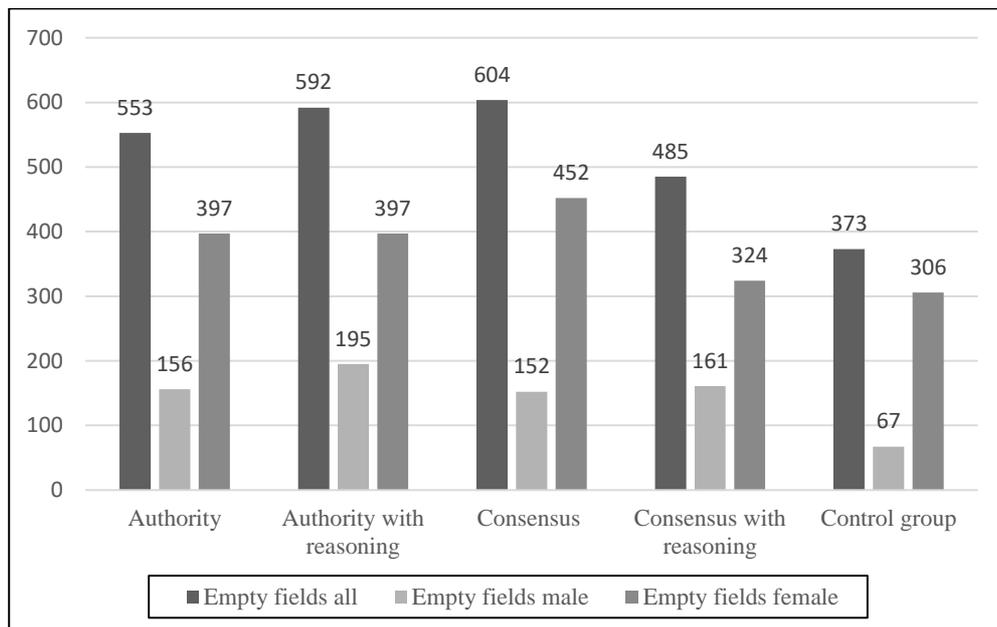


Figure 6: Absolute numbers of empty fields (Study 3).

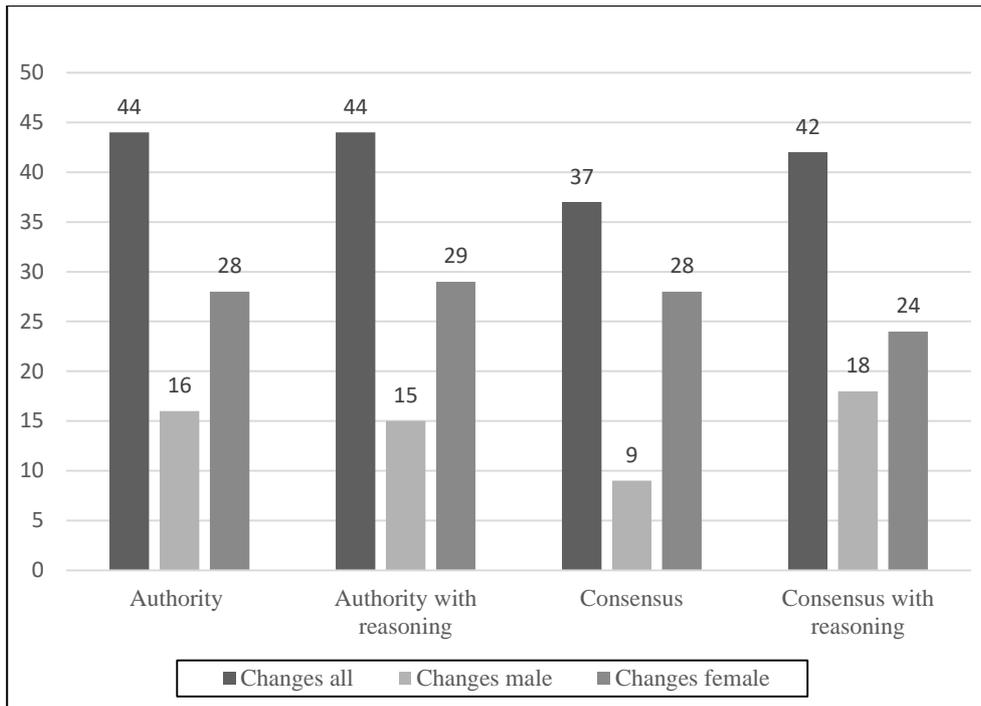


Figure 7: Absolute numbers of changes (Study 3).

According to the Shapiro Wilk test, the dependent variable *empty fields* was approximately normally distributed ($p > .05$). Furthermore, the Levene test revealed variance homogeneity for the dependent variable *empty fields* ($p > .05$). For the dependent variable *number of changes*, the assumption of normal distribution was violated; however, owing to the sample size of more than 30 persons per condition, this violation can be neglected (see Ghasemi & Zahediasl, 2012). According to the Levene test, variance homogeneity for the *number of changes* was given ($p > .05$). The significance level for all calculations regarding the hypotheses was $p < .05$.

Hypothesis 1 (H1)

In order to examine whether users' privacy behaviors differed depending on receiving persuasive privacy prompts versus not receiving prompts, a two-way analysis of variance comparing the mean values of empty fields between the factors prompt and no prompt was conducted ($N = 187$). Since there were more female than male participants in the sample and prior research indicated differences in privacy behavior between male and female users in terms of female users paying more attention to their privacy (e.g., Youn & Hall, 2008), it was controlled for participants' sex by including it in the analysis

as a second factor. For this hypothesis, it was not tested for differences regarding the number of changes in input fields after receiving prompts (i.e. the second dependent variable representing privacy behavior) because the number of changes is only available for users who received persuasive privacy prompts.

Analysis revealed significant main effects for the experimental manipulation prompting, $F(1, 183) = 16.16, p < .01, \eta_p^2 = .081$, and the control variable sex, $F(1, 183) = 4.90, p < .05, \eta_p^2 = .026$, indicating that both prompting ($M_{\text{prompt}} = 14.89, SD_{\text{prompt}} = 5.86, M_{\text{no_prompt}} = 10.08, SD_{\text{no_prompt}} = 5.54$) and the control variable sex ($M_{\text{male}} = 12.18, SD_{\text{male}} = 5.85, M_{\text{female}} = 14.77, SD_{\text{male}} = 6.05$) do significantly influence the number of empty fields. The effect for prompting was medium ($\eta_p^2 = .081$) whereas the effect of the control variable sex can be considered as small to medium ($\eta_p^2 = .026$). However, there was no interaction effect between prompting and sex, demonstrating that men and women are not differently influenced by the persuasive privacy prompts in the current study. As visualized in Figure 8, both, men and women had less empty fields if they were not confronted with persuasive privacy prompts ($M_{\text{men}} = 8.38, SD_{\text{men}} = 4.66, M_{\text{women}} = 10.55, SD_{\text{women}} = 5.74$) than if they saw persuasive privacy prompts during the registration process ($M_{\text{men}} = 12.78, SD_{\text{men}} = 5.83, M_{\text{women}} = 16.02, SD_{\text{women}} = 5.58$).

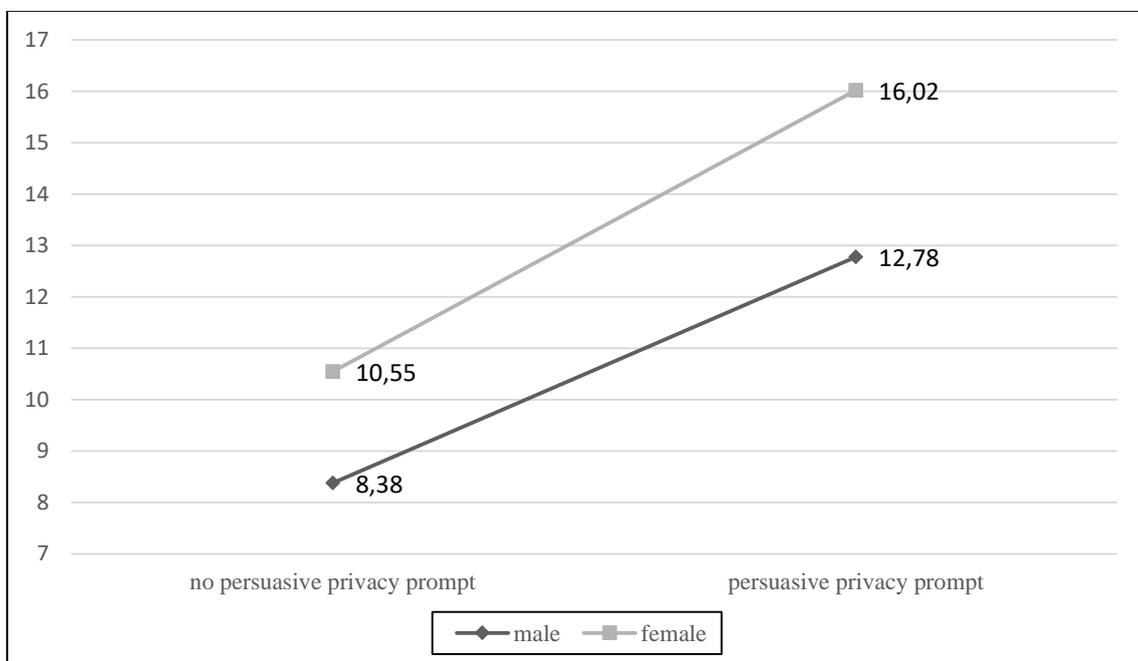


Figure 8: Mean values for male and female participants receiving a persuasive privacy prompt versus not receiving a persuasive privacy prompt (Study 3).

For examining both the influence of the persuasive style of the prompt and the factor reasoning versus no reasoning on the number of empty fields, a two-way ANOVA was conducted with the experimental manipulation with five factors (authority, authority with reasoning, consensus, consensus with reasoning, and no prompt), sex as second factor, and the number of empty fields as dependent variable (*H1a* and *H1b*). Results show that there is a significant effect for sex, $F(1, 177) = 9.53, p < .01, \eta_p^2 = .05$, indicating that participants' sex affects the number of empty fields when not considering the experimental condition. The effect was small to medium. There was a main effect for the condition as well, $F(4, 177) = 6.06, p < .001, \eta_p^2 = .12$, indicating that the experimental condition significantly affected the number of empty fields. Partial eta square indicates a medium-sized effect ($\eta_p^2 = .12$). Post hoc analysis (Bonferroni) revealed that there is a significant difference regarding the number of empty fields between the control group in which participants did not receive persuasive prompts and each group in which participants received privacy prompts. By contrast, there was no significant interaction effect between the control variable sex and the experimental manipulation, $F(4, 177) = .37, p = .83, \eta_p^2 = .01$. Results indicate that the impact of the persuasive privacy prompts was not different for male and female participants but that privacy behavior (i.e. leaving input fields empty), independently from the prompt intervention, differs between males and females in this study. For all descriptive values please, refer to Table 10. In sum, Hypothesis *H1* can only partly be accepted.

Table 10
Number of empty fields for female and male participants (Study 3).

	authority <i>M (SD)</i>	authority reason <i>M (SD)</i>	consensus <i>M (SD)</i>	consensus reason <i>M (SD)</i>	control <i>M (SD)</i>
Male (<i>n</i> = 60)	13.00 (5.80)	13.93 (4.98)	15.20 (7.13)	10.06 (5.08)	8.38 (4.66)
Female (<i>n</i> = 127)	15.88 (5.55)	16.54 (5.75)	16.74 (5.52)	14.73 (5.66)	10.55 (5.74)
Full sample (<i>N</i> = 187)	14.95 (5.72)	15.58 (5.56)	16.32 (5.93)	12.76 (5.84)	10.08 (5.54)

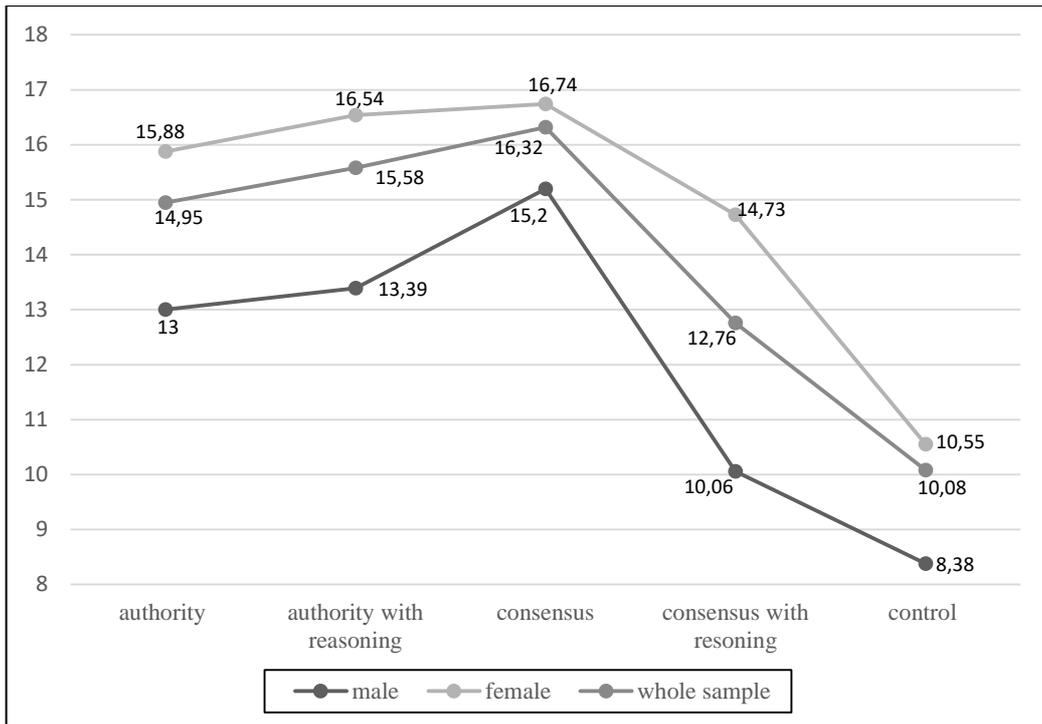


Figure 9: Mean values of the number of empty fields (Study 3).

In order to examine whether there is an interaction effect between the persuasive style (authority/consensus) and reasoning (with/without), a univariate analysis of variance was conducted considering the factors style and reasoning (controlling for sex) and the dependent variable number of empty fields ($n = 150$). Data reveal a significant interaction effect between persuasive style and reasoning, $F(1, 142) = 5.01, p = .027, \eta_p^2 = .03$ (see Figure 9). Data indicate that a persuasive privacy prompt in a consensual style was more effective without reasoning whereas a persuasive prompt in an authoritarian style was more effective with additional information (please refer to Table 7 and Figure 10 for mean values). Most empty fields (i.e. most pronounced privacy behavior) was found for participants receiving a persuasive prompt in a consensual style without information ($M = 16.32, SD = 5.93$).

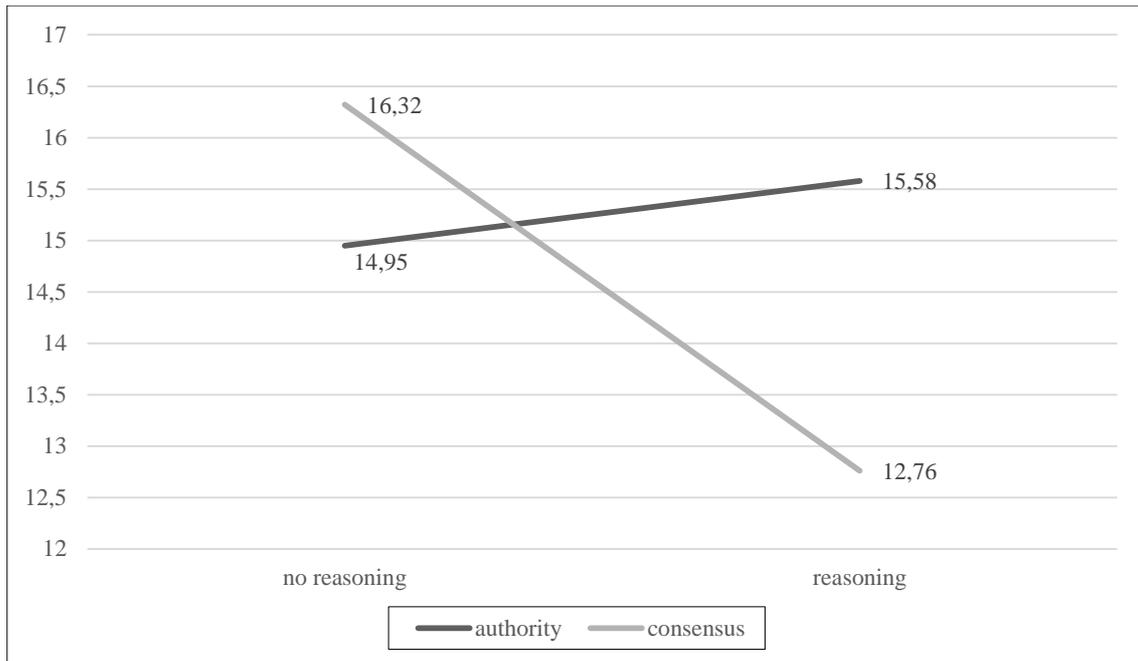


Figure 10: Interaction effect between the persuasive style and provided information (Study 3).

Hypothesis 2 (H2)

Two moderation analyses were conducted to test whether the effectiveness of a particular persuasive style of a privacy prompt is influenced by users' susceptibility to the utilized persuasive style. More precisely, it was examined whether the influence of the particular prompt on users' privacy behavior was moderated by users' susceptibility to the utilized persuasive style of communication. Therefore, the group variable "style" (consensus/authority) was used as a predictor, participants' susceptibility to each persuasive style consensus and authority as moderator variables, and the number of changes as dependent variable in each analysis of regression (for $n = 150$). For mean values and standard deviations of test subjects' susceptibility to the persuasive styles, please refer to Table 11.

Table 11

Means and standard deviations for participants' susceptibility to the persuasive styles authority and consensus (Study 3).

Group	<i>N</i>	Susceptibility to authority <i>M (SD)</i>	Susceptibility to consensus <i>M (SD)</i>
Authority	75	4.63 (.85)	4.09 (1.06)
Consensus	75	4.74 (8.46)	4.45 (.97)
Full sample	187	4.71 (.83)	4.36 (1.03)

It was controlled for sex in both analyses. Values were centered and interaction terms were created (style \times susceptibility_{authority} and style \times susceptibility_{consensus}).

In the first step of each regression, sex was considered as control variable. In the next step, the predictor variable style of the persuasive prompt (authority/consensus) was included, followed by participants' susceptibility to the persuasive style authority or consensus as potential moderators. In the fourth step, the interaction terms of the persuasive style of the prompt and users' susceptibility to the particular style were included.

As summarized in Table 12, there was neither a main effect of the susceptibility to the persuasive style authority on the number of changes after being exposed to persuasive privacy prompts ($\beta = .11, p = .190$), nor a significant interaction effect between the prompt's style and users' susceptibility to the persuasive style authority ($\beta = -.11, p = .202$). Furthermore, the control variable sex had no significant impact on the number of changes. In sum, the suggested moderation model did not reveal any significant results.

Table 12

Statistics of the coefficients of the moderated regression analysis examining the interaction between the persuasive style of a privacy prompt (-1 = authority, 1 = consensus) and the number of changes, considering the susceptibility to the persuasive style authority (SuAu) as moderator variable and controlling for sex (-1 = male, 1 = female) for n = 150 (Study 3)

		Number of changes						
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2	ΔF
<i>Step 1</i>							.000	.000
	Sex	-.00	.09	-.00	-.02	.986		$F(1,148) = .00, p = .986$
<i>Step 2</i>							.004	.520
	Sex	-.00	.09	-.00	-.02	.986		$F(2,147) = .26, p = .771$
	Style	-.06	.08	-.06	-.72	.472		
<i>Step 3</i>							.012	1.74
	Sex	-.00	.09	-.00	-.01	.990		$F(3,146) = .76, p = .521$
	Style	-.07	.08	-.07	-.81	.419		
	SuAu	.13	.09	.11	1.32	.189		
<i>Step 4</i>							.011	1.64
	Sex	-.00	.09	-.00	-.01	.994		$F(4, 145) = .98, p = .421$
	Style	-.07	.08	-.07	-.81	.418		
	SuAu	.13	.10	.11	1.32	.190		
	Style \times SuAu	-.13	.10	-.11	-1.28	.202		
<i>Total R²</i>							.026	

As can be seen in Table 13, the second moderation analysis indicates that there was a significant main effect of the susceptibility to the prompt's persuasive style consensus on the number of changes ($\beta = .17, p < .05$). However, there was no significant interaction between the predictor (style of the prompt) and users' susceptibility to the consensual style ($\beta = -.11, p = .202$). Again, the control variable sex did not significantly influence the number of changes. Overall, the suggested model did not significantly explain the number of changes based on the style of the persuasive privacy prompts. According to reported results, Hypothesis *H2* has to be rejected.

Table 13

Statistics of the coefficients of the moderated regression analysis examining the interaction between the persuasive style of a privacy prompt (-1 = authority, 1 = consensus) and the number of changes, considering the susceptibility to the persuasive style consensus (SuCo) as moderator variable and controlling for sex (-1 = male, 1 = female) for $n = 150$ (Study 3)

		Number of changes							
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2	ΔF	
Step 1	Sex	-.00	.09	-.00	-.02	.986	.000	.000	$F(1,148) = .00, p = .986$
Step 2	Sex	-.00	.09	-.00	-.02	.986	.004	.520	$F(2,147) = .26, p = .771$
	Style	-.06	.08	-.06	-.72	.472			
Step 3	Sex	-.04	.09	-.04	-.46	.636	.024	1.74	$F(3,146) = 1.40, p = .246$
	Style	-.09	.08	-.09	-1.06	.293			
	SuCo	.16	.08	.16	1.91	.058			
Step 4	Sex	-.05	.09	-.04	-.51	.608	.005	1.64	$F(4,145) = 1.25, p = .294$
	Style	-.09	.08	-.09	-1.07	.286			
	SuCo	.17	.08	.17*	1.99	.049			
	Style \times SuCo	.07	.08	-.07	.89	.373			
Total R^2							.033		

Note. * $p < .05$, bold value without asterix indicates a marginally significant effect.

Hypothesis 3 (H3)

Users' need for privacy ($M_{n=150} = 4.16, SD_{n=150} = .84$) and vulnerable narcissism ($M_{n=150} = 4.00, SD_{n=150} = .87$) were hypothesized to be positive predictors of their actual privacy behavior (*H3a*). In the following analyses, privacy behavior is represented by the number of changes in input fields after being exposed to persuasive privacy prompts ($n =$

150). Relations between each personality characteristic and privacy behavior represented by the number of empty fields will be investigated in Hypothesis *H4* ($N = 187$).

To address the stated hypotheses, two hierarchical analysis of regression were conducted. The variable sex was included in the first step in both models. In the first analysis of regression, vulnerable narcissism was included in the second model. The number of changes was used as dependent variable. The regression model did yield significant results. However, coefficients indicate a marginally significant effect of subjects' vulnerable narcissism on the number of changes ($\beta = .163$, $p = .051$) in the second model of regression. Values are summarized in Table 14.

Table 14
Hierarchical multiple regression analysis including vulnerable narcissism as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3)

		<i>Number of changes</i>					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.000	$F(1,148) = .00, p = .986$
	Sex	-.00	.09	-.00	-.02	.986		
Step 2							.026	$F(2,147) = 1.94, p = .147$
	Sex	-.04	.09	-.03	-.40	.693		
	Vulnerable narcissism	.19	.10	.16	1.97	.051		

Note. Bold value without asterix indicates a marginally significant effect.

A second hierarchical analysis of regression was calculated to analyze the influence of participants' need for privacy on the number of changes ($n = 150$). Again, sex was controlled for by including it in the first step in the first model. When only sex is used as a predictor, no variance in the number of changes can be explained. When the predictor need for privacy is included in the second step, the change in the amount of variance that can be explained gives rise to an F-ratio of 4.21. However, the main model is statistically not significant. Corresponding values are summarized in Table 15.

Table 15

Hierarchical multiple regression analysis including need for privacy as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3)

		Number of changes					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.000	$F(1,148) = .00, p = .986$
	Sex	-.00	.17	-.00	-.02	.986		
Step 2							.028	$F(2,147) = 2.10, p = .126$
	Sex	-.06	.18	-.03	-.36	.717		
	Need for privacy	.21	.10	.17*	2.05	.042		

Note. * $p < .05$

In Hypothesis *H3b*, negative relations were suggested between the number of changes in input fields after receiving persuasive privacy prompts and users' need for popularity ($M_{n=150} = 2.22, SD_{n=150} = .76$) and for grandiose narcissism ($M_{n=150} = 2.72, SD_{n=150} = .48$). Therefore, two hierarchical analyses of regression were conducted. It was controlled for sex in both analyses within the first step of regression, followed by each, users' need for popularity and for grandiose narcissism, in the second step. For both models, there were no significant effects. For an overview of the coefficients, please refer to Table 16 and Table 17.

Table 16

Hierarchical multiple regression analysis including need for popularity as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3)

		Number of changes					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.000	$F(1,148) = .00, p = .986$
	Sex	-.00	.09	-.00	-.02	.986		
Step 2							.000	$F(2,147) = .01, p = .991$
	Sex	-.00	.09	-.00	-.01	.990		
	Need for popularity	.01	.11	.01	.13	.895		

Table 17

Hierarchical multiple regression analysis including grandiose narcissism as predictor and sex (-1 = male, 1 = female) as control variable (n = 150; Study 3)

		<i>Number of changes</i>					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.000	$F(1,148) = .00, p = .986$
	Sex	-.00	.09	-.00	-.02	.986		
Step 2							.005	$F(2,147) = 2.10, p = .693$
	Sex	-.00	.09	.00	.12	.902		
	Grandiose narcissism	-.15	.18	-.07	-.86	.393		

Overall, Hypothesis *H3* can only partly be accepted. It was revealed that users' vulnerable narcissism had a marginally significant positive influence ($\beta = .16, p = .051$) and need for privacy had a significant positive influence ($\beta = .17, p < .05$) on the number of changes by participants who were exposed to persuasive privacy prompts during the process of registration to the SNS for students.

Hypothesis 4 (H4)

It was suggested that the effect of privacy prompts on actual privacy behavior is moderated by the personality characteristics that were identified as important factors for online privacy behavior in prior research (need for privacy, need for popularity, vulnerable narcissism, grandiose narcissism). Analyses with the dichotomous variable prompting (prompt/no prompt) as predictor and the number of empty fields as dependent variable ($N = 187$) revealed that the variable prompting can significantly predict the number of empty fields, $F(1, 185) = 20.45, p < .001, \beta = .32, R^2 = .10$. Hence, 10% of the variance in the number of empty fields can be explained by the predictor prompting. The effect was medium ($\beta = .32$). In order to examine if this relation is strengthened (e.g., due to the need for privacy or vulnerable narcissism) or weakened (e.g., due to the need for popularity or grandiose narcissism) by users' personality characteristics, four moderation analyses with the aforementioned characteristics as moderators were conducted. For an overview of descriptive statistics with regard to participants' expressions of personality, please consider Table 18. For moderation analyses, values were centered and interaction terms were created.

Table 18

Mean values and standard deviations of participants' personality traits (N = 187; Study 3)

	<i>M</i>	<i>SD</i>	Minimum	Maximum
Need for privacy	4.18	.86	1.83	6.52
Vulnerable narcissism	4.00	.86	1.73	6.09
Grandiose narcissism	2.75	.48	1.31	3.69
Need for popularity	2.26	.77	1.00	4.14

Need for privacy. To test whether the effectiveness of persuasive prompts is moderated by people's need for privacy, a moderation analysis was conducted with the predictor prompting (prompting / no promoting), the moderator need for privacy, and the dependent variable number of empty fields. Sex was considered as control variable in the first step of regression, followed by the predictor prompting in the second step, and the moderator variable need for privacy in the third step. The last step included the interaction term prompting \times need for privacy.

As summarized in Table 19, there was a main effect of the predictor prompting on the number of empty fields ($\beta = .34, p < .001$). In addition, the control variable sex significantly contributed to explaining the number of empty fields ($\beta = .26, p < .001$). However, there was neither a main effect of users' need for privacy nor a significant interaction effect between the predictor prompting and the moderator need for privacy ($\beta = -.08, p = .321$). In sum, the suggested model can significantly explain the number of empty fields $F(4, 186) = 9.42, p < .001$, by about 17%. However, in line with reported results in Hypothesis *H1*, this effect is mainly based on the predictor prompting, whereas the suggested moderation was not established by the current data.

Table 19

Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' need for privacy (NfPr) as moderator variable and controlling for sex (-1 = male, 1 = female) for $N = 187$ (Study 3)

		Number of empty fields					ΔR^2	ΔF	
		b	SE	β	t	p			
Step 1	Sex	1.29	.47	.20**	2.76	.006	.040	7.614	$F(1,185) = 7.61, p = .006$
Step 2	Sex	1.54	.44	.24**	3.47	.001	.115	25.127	$F(2,184) = 16.87, p = .000$
	Prompting	2.61	.52	.34***	5.01	.000			
Step 3	Sex	1.65	.45	.25***	3.69	.000	.012	2.646	$F(3,183) = 12.23, p = .000$
	Prompting	2.58	.52	.34***	4.99	.000			
	NfPr	-.79	.49	-.11	-1.63	.106			
Step 4	Sex	1.67	.45	.26***	3.74	.000	.005	.991	$F(4, 186) = 9.42, p = .000$
	Prompting	2.62	.52	.34***	5.04	.000			
	NfPr	-.50	.57	-.07	-.88	.381			
	Prompting \times NfPr	-.56	.56	-.08	-1.00	.321			
Total R^2							.171		

Note: ** $p < .01$, *** $p < .001$

Need for popularity. In a second moderation analysis, users' need for popularity was investigated as potential moderator. Again, sex was considered as control variable, followed by the predictor prompting in the second, the moderator need for popularity in the third, and the interaction term prompting \times need for popularity in the fourth step. Analyses revealed significant main effects for the control variable sex ($\beta = .23, p < .01$), the predictor prompting ($\beta = .33, p < .001$), as well as for the moderator variable need for popularity ($\beta = -.17, p < .001$). Overall, the model can predict the number of empty fields by about 22%, $R^2 = .218, F(4, 182) = 12.66, p < .001$. For a summary of all values please refer to Table 20.

Table 20

Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' need for popularity (NfPo) as moderator variable and controlling for sex (-1 = male, 1 = female) for $N = 187$ (Study 3)

		Number of empty fields							
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2	ΔF	
Step 1	Sex	1.29	.47	.20**	2.76	.006	.040	7.614	$F(1,185) = 7.61, p = .006$
Step 2	Sex	1.54	.44	.24**	3.47	.001	.115	25.127	$F(2,184) = 16.87, p = .000$
	Prompting	2.61	.52	.34***	5.01	.000			
Step 3	Sex	1.51	.43	.23**	3.51	.001	.055	12.737	$F(3,183) = 16.21, p = .000$
	Prompting	2.40	.51	.32***	4.73	.000			
	NfPo	-1.88	.53	-.24***	-3.57	.000			
Step 4	Sex	1.49	.43	.23**	3.45	.001	.008	1.793	$F(4,182) = 12.66, p = .000$
	Prompting	2.55	.52	.33***	4.92	.000			
	NfPo	-1.34	.65	-.17*	-2.11	.037			
	Prompting \times NfPo	-.87	.65	-.11	-1.34	.182			
Total R^2							.218		

Note: * $p < .05$, ** $p < .01$, *** $p < .001$

Vulnerable narcissism. In the third analysis of regression, participants' sex was considered as control variable in the first step, again. Step by step, the predictor prompting, the moderator vulnerable narcissism and the interaction term prompting \times vulnerable narcissism were added to the model (see Table 21). Again, the control variable sex ($\beta = .27, p < .01$), the predictor prompting ($\beta = .35, p < .01$), and the moderator vulnerable narcissism ($\beta = -.21, p < .05$) showed significant main effects on the number of empty fields. Yet, no interaction effect was found ($\beta = .03, p < .712$). In sum, the model explains 19% of variance in the number of empty fields based on the predictor prompting.

Table 21

Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' vulnerable narcissism (VulNa) as moderator variable and controlling for sex (-1 = male, 1 = female) for $N = 187$ (Study 3)

		Number of empty fields							
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2	ΔF	
Step 1	Sex	1.29	.47	.20**	2.76	.006	.040	7.614	$F(1,185) = 7.61, p = .006$
Step 2	Sex	1.54	.44	.24**	3.47	.001	.115	25.127	$F(2,184) = 16.87, p = .000$
	Prompting	2.61	.52	.34***	5.01	.000			
Step 3	Sex	1.77	.44	.27***	3.99	.000	.055	12.737	$F(3,183) = 14.26, p = .000$
	Prompting	2.64	.51	.35***	5.17	.000			
	VulNa	-1.33	.48	-.19**	-2.79	.006			
Step 4	Sex	1.77	.45	.27***	3.97	.000	.008	1.793	$F(4, 182) = 10.68, p = .000$
	Prompting	2.64	.51	.35***	5.16	.000			
	VulNa	-1.48	.61	-.21*	-2.41	.017			
	Prompting × VulNa	.22	.61	.03	.37	.712			
Total R ²							.190		

Note: * $p < .05$, ** $p < .01$, *** $p < .001$

Grandiose Narcissism. The last model included the control variable sex in the first step of regression as well. In the second, third, and fourth step, the predictor prompting, the moderator grandiose narcissism, and the interaction term prompting × grandiose narcissism were included. As presented in Table 22, significant main effects were found only for the control variable sex ($\beta = .23, p < .01$) and the predictor prompting ($\beta = .35, p < .01$). Overall, the suggested model predicts the number of empty fields by approximately 16% ($R^2 = .157, p < .001$).

Table 22

Statistics of the coefficients of the moderated regression analysis examining the interaction between the intervention prompting (-1 = no prompt, 1 = prompt) and the number of empty fields, considering users' grandiose narcissism (GraNa) as moderator variable and controlling for sex (-1 = male, 1 = female) for $N = 187$ (Study 3)

		Number of empty fields							
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2	ΔF	
Step 1							.040	7.614	$F(1,185) = 7.61, p = .006$
	Sex	1.29	.47	.20**	2.76	.006			
Step 2							.115	25.127	$F(2,184) = 16.87, p = .000$
	Sex	1.54	.44	.24**	3.47	.001			
	Prompting	2.61	.52	.34***	5.01	.000			
Step 3							.001	.136	$F(3,183) = 11.24, p = .000$
	Sex	1.52	.45	.23**	3.37	.001			
	Prompting	2.63	.52	.34***	5.01	.000			
	GraNa	.32	.87	.03	.37	.713			
Step 4							.002	.334	$F(4, 182) = 8.48, p = .000$
	Sex	1.52	.45	.23**	3.38	.001			
	Prompting	2.69	.54	.35***	5.01	.000			
	GraNa	.67	1.06	.05	.63	.528			
	Prompting × GraNa	-.61	1.06	-.05	-.58	.564			
<i>Total R²</i>									.157

Note. ** $p < .01$, *** $p < .001$.

Overall, no significant interaction effects between the persuasive prompt intervention and subjects' manifestations of personality were found. Analyses revealed positive main effects of the predictor prompting and the control variable sex in each model as well as significant negative main effects of users' need for popularity ($\beta = -.17, p < .05$) and vulnerable narcissism ($\beta = -.21, p < .05$) on the number of empty fields. Beta values indicate that the factor prompting is more influential for explaining the variance in the dependent variable than the control variable sex. To sum up, Hypothesis *H4* cannot be accepted.

Hypothesis 5 (H5)

In order to find out whether users' expressions of privacy concerns, attitudes, intentions, and general privacy behaviors influence the current privacy behavior in terms of changing or deleting disclosures during the registration process, several multiple regression analyses were conducted (for $n = 150$). Therefore, the influence of users' informational, social and psychological (a) privacy concerns, (b) privacy attitudes, (c) privacy intentions, and (d) general privacy behavior on their informational, social and psychological privacy-related behavior (i.e. changes in informational, social,

psychological privacy-related fields) were examined. In all calculations, sex was controlled for in the first step of regression analyses.

Hierarchical analysis of regression regarding the number of changes in psychological privacy-related fields revealed that sex was not a significant predictor of the number of respective changes. Including the actual predictor psychological privacy concerns in the second step revealed that the number of changes in psychological privacy-related fields can be predicted by psychological privacy concerns by approximately 5% ($R^2 = .047, p < .05$). Corresponding values are presented in Table 23. No further significant relations were found. Descriptive values are summarized in Table 24. In addition, Table 25 and 26 provide an overview of correlations between behavioral variables and the dependent variables in this study. Overall, Hypothesis *H5* can only partly be accepted.

Table 23
Hierarchical multiple regression analysis including psychological privacy concerns as predictor and sex (-1 = male, 1 = female) as control variable (Study 3)

		Changes in psychological privacy-related fields					
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2
Step 1	Sex	-.01	.04	-.10	-1.26	.211	.011
							$F(1,148) = 1.58, p = .211$
Step 2	Sex	-.06	.04	-.12	-1.49	.139	.036
	Psychological privacy concerns	.07	.03	.19*	2.36	.020	$F(2,147) = 3.60, p = .030$
<i>Final</i>							.047
<i>R²</i>							

Note: * $p < .05$

Table 24

Mean values and standard deviations of participants' self-reported privacy concerns, attitudes, intentions and behavior (Study 3)

	<i>N</i> = 187		<i>n</i> = 150	
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
Privacy concerns informational	4.56	1.36	4.51	1.36
Privacy concerns social	5.03	1.35	5.01	1.40
Privacy concerns psychological	4.40	1.32	4.36	1.35
Privacy attitudes informational	3.38	1.08	3.30	1.10
Privacy attitudes social	5.93	1.00	5.93	1.01
Privacy attitudes psychological	3.22	1.14	3.16	1.23
Privacy intentions informational	2.84	1.05	2.81	1.05
Privacy intentions social	5.16	1.30	5.18	1.33
Privacy intentions psychological	3.23	1.18	3.13	1.15
Privacy behavior informational	3.53	1.25	3.60	1.27
Privacy behavior social	4.95	1.40	4.88	1.42
Privacy behavior psychological	3.16	1.30	3.10	1.30

Table 25

Bivariate correlations between behavioral data and self-reports for the control-group (Study 3)

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
1. Number of changes	-														
2. Empty fields	.013	-													
3. Intentions inf.	-.007	-.334**	-												
4. Intentions soc.	.129	.231**	-.394**	-											
5. Intentions psy.	.042	-.238**	.593**	-.300**	-										
6. Attitudes inf.	-.062	-.182*	.485**	-.306**	.380**	-									
7. Attitudes soc.	.082	.101	-.250**	.185*	-.159	-.137	-								
8. Attitudes psy.	-.009	-.198*	.335**	-.293**	.342**	.467**	-.161*	-							
9. Behavior inf.	-.038	-.167*	.491**	-.243**	.411**	.354**	-.016	.263**	-						
10. Behavior soc.	.147	.169*	-.369**	.600**	-.297**	-.337**	.138	-.253**	-.289**	-					
11. Behavior psy.	.010	-.158	.623**	-.430**	.700**	.423**	-.165*	.421**	.581**	-.337**	-				
12. Concerns inf.	.043	.114	-.301**	.438**	-.160	-.395**	.025	-.350**	-.109	.312**	-.233**	-			
13. Concerns soc.	-.015	.220**	-.388**	.481**	-.229**	-.311**	.143	-.271**	-.162*	.422**	-.264**	.473**	-		
14. Disclosure (self) number of words	.010	-.368**	.238**	-.079	.217**	.030	.117	.113	.267**	-.032	.208*	.110	-.050	-	
15. Disclosure (politic) number of words	.056	-.273**	.115	-.158	.178*	.071	-.074	.213**	.129	-.138	.192*	.042	-.090	.496**	-

Note: * $p < .05$. ** $p < .01$.

Table 26

Bivariate correlations between behavioral data and self-reports for all experimental groups (Study 3)

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
1. Empty fields	-													
2. Intentions inf.	-.308	-												
3. Intentions soc.	.284	-.436**	-											
4. Intentions psy.	-.358*	.345*	-.498**	-										
5. Attitudes inf.	-.145	.459**	-.259	.510**	-									
6. Attitudes soc.	-.107	-.466**	.485**	-.440**	-.272	-								
7. Attitudes psy.	-.075	.239	-.195	.307	.291	-.023	-							
8. Behavior inf.	-.392*	.611**	-.678**	.479**	.276	-.446**	-.075	-						
9. Behavior soc.	.361*	-.212	.589**	-.236	-.169	.332*	.037	-.509**	-					
10. Behavior psy.	-.363*	.524**	-.462**	.611**	.236	-.377*	.186	.523**	-.250	-				
11. Concerns inf.	.041	-.324	.547**	-.374*	-.281	.147	-.299	-.413*	.274	-.357*	-			
12. Concerns soc.	.104	-.026	.515**	-.177	-.267	.147	.034	-.353*	.599**	.040	.450**	-		
13. Disclosure (self) number of words	-.347*	-.006	-.013	.180	.130	.148	.127	-.078	.149	-.063	.043	-.113	-	
14. Disclosure (politic) number of words	-.407*	.154	-.318	.379*	.042	-.069	.084	.399*	-.259	.114	-.301	-.282	.398*	-

Note: * $p < .05$. ** $p < .01$.

In sum, results from partial analyses of regression (controlling for sex) with the subsample ($n = 150$) demonstrate that strong informational, social and psychological privacy intentions, strong informational privacy attitudes, self-reported strong informational and social privacy behavior, and high concerns regarding social privacy were positively related to actual privacy behavior within the experiment (i.e. high number of empty fields).

Calculations with data from the control group showed that strong psychological privacy intentions, as well as self-reported strong informational, social, and psychological privacy behavior was positively related to actual privacy behavior in the current study (i.e. high number of empty fields).

Explorative analyses

Analysis of free-text input. In order to examine potential differences in disclosure behavior (disclosing / not disclosing) based on different prompts (authority, authority with reasoning, consensus, consensus with reasoning, $n = 150$) with regard to the self and political opinion, Pearson's chi-square tests were conducted. The dichotomous variable disclosure (disclosure / no disclosure) was considered as dependent variable. Analyses of disclosures in the input-field asking for political opinions ("Here you can disclose your opinion regarding current political events. Maybe this is a good starting point for an interesting discussion?") demonstrate that there is no significant difference regarding disclosure versus no disclosure of a political statement depending on the experimental manipulation. Descriptive values are summarized in Table 27. Four persons who received persuasive privacy prompts in the authoritarian style (authority and authority with reasoning) formulated a political statement whereas 71 persons receiving authoritarian prompts decided not to disclose a political statement. Eight persons exposed to the consensual manipulation (consensus and consensus with reasoning) disclosed a political statement, whereas 67 test subjects in that group did not disclose. By contrast, eight participants who received no persuasive prompt disclosed a political statement whereby 29 persons did not disclose one.

Table 27

Absolute numbers of participants regarding disclosure vs. no disclosure in free-text input fields about the political opinion (Study 3)

	<i>No disclosure</i>		<i>Disclosure</i>		<i>n</i>
	Male	Female	Male	Female	
Authority	10	24	2	1	37
Authority with reasoning	14	23	0	1	38
Consensus	8	26	2	1	37
Consensus with reasoning	12	21	4	1	38
No prompt	49	24	3	5	37
Sum	167		20		

The relationship between the style of privacy prompts and the disclosure about the self (“Here, you can tell something about you. What should other users get to know about you and why is it worth to get to know you?”) was analyzed by means of a Pearson’s chi-square test as well. Once more, there were no significant differences in the disclosures depending on the experimental condition. Descriptively, more participants decided not to disclose information about themselves ($n = 52$) than to disclose information ($n = 136$). The numbers of participants who disclosed information and those who did not disclose any information are summarized in Table 28.

Table 28

Absolute numbers of participants regarding disclosure vs. no disclosure in free-text input fields about the self (Study 3)

	<i>No disclosure</i>		<i>Disclosure</i>		<i>n</i>
	Male	Female	Male	Female	
Authority	6	20	6	5	37
Authority with reasoning	9	21	5	3	38
Consensus	7	23	3	4	37
Consensus with reasoning	8	17	8	5	38
No prompt	5	20	3	9	37
Sum	136		51		

Analysis of word count. By means of an analysis of variance, the number of words of disclosed statements regarding the self and politics were compared with regard to experimental manipulations ($N = 187$). There was neither a significant difference in the number of words of disclosures regarding the self nor for the number of words regarding politics between the experimental groups. Overall, 246 words were written for political statements ($M = 1.32$, $SD = 5.02$) and 680 words for statements about the self ($M = 3.63$, $SD = 9.90$).

Content of self-disclosures. If users decided to disclose a statement in the input fields, these disclosures indeed contained sensitive information in terms of referring to personal qualities or political opinions. Two independent raters rated the text inputs as either sensitive (being directly related to the person, being private, revealing clear political opinion) or not sensitive. The interrater-reliability for disclosures about the self was $\kappa = 0.3$ whereby it was $\kappa = 0.7$ for political disclosures. Examples for sensitive disclosures about the self are: “I’m a nerd and ready for everything as long as no sunlight is involved” and “I’m studying mechanical engineering for a very long time but I hope to be finished with my bachelor’s degree in the summer. Moreover, I play soccer a lot. At weekends, I go out, partying and stuff like that.” Examples of sensitive disclosures with regard to politics are: “Why have taxpayers to pay for refugees?” or “We are too relaxed with Erdoğan. We should be much more critical!”. However, there were some non-sensitive disclosures as well, for instance: “I am able to program” (regarding the self) or “I think 2017 is going to be an interesting political year” (regarding political opinion).

Evaluation of messages. Overall, users’ evaluation of persuasive privacy prompts revealed that the prompts were perceived as medium to positive ($M = 6.58$, $SD = 2.06$, 11-point Likert scale). However, male and female users differed regarding the evaluation of messages, $F(1,148) = 4.90$, $p < .05$, $\eta^2 = .03$, whereby female users evaluated the messages slightly better ($M_{\text{female}} = 6.85$, $SD_{\text{female}} = 2.00$; $M_{\text{male}} = 6.08$, $SD_{\text{male}} = 2.10$). Furthermore, users’ future intention to use a system that provides persuasive privacy prompts as they were introduced here, was medium to high ($M = 3.33$, $SD = 1.04$, 5-point Likert scale). Here, no difference between male and female participants was found. Explorative retrospective analyses revealed significant positive correlations between the number of changes and, users’ evaluation of persuasive privacy prompts ($r = .246$, $p < .01$) and of reported future intention ($r = .313$, $p < .001$). Nevertheless, participants also had the chance to provide suggestions for improvements of the privacy prompts. Most frequently they suggested to have only one prompt when starting the registration (21 persons), to provide the prompts less frequently (18 persons), at other positions (22 persons), or to depict them more attractively (15 persons). All suggestions are summarized in Table 29.

Table 29
Users' suggestions for improvement of persuasive privacy prompts (Study 3)

Users suggestions for improvement	Total
Just a general warning in the beginning	21
Less frequent	18
Other position	22
Better depiction	15
Less redundant	7
More specific message	9
No different warnings	5
Reasoning or example	11
No warnings at all	4
Give a source	3
Shorter messages	2
Only for specific topics	2
More personalized	1
Giving alternative suggestions	1
Link to privacy settings	1
Possibility to confirm each message	1
More variation	1
After confirming a message no further message	1

12.6 Discussion

The goal of this study was to investigate users' reactions to particular persuasive privacy prompts that varied regarding persuasive styles of communication (authority vs. consensus) and provided privacy-related information (reasoning vs. no reasoning) after individual disclosures. Persuasive privacy prompts were presented on a self-developed registration page of an SNS for students. It was aimed at investigating the moderating effects of users' personality traits (vulnerable and grandiose narcissism, need for privacy, need for popularity) on the relation between receiving a prompt and subsequent privacy behavior on a registration page of a social network (withdrawing a disclosure or not disclosing at all).

Analyses revealed several important findings for understanding users' perception of persuasive privacy prompts. Two dependent variables were considered as actual privacy behavior in the analysis. On the one hand, it was the number of changes in input fields and boxes after receiving a privacy prompt (for $n = 150$) and on the other hand, the number of empty fields in the end (for both, $N = 187$ and $n = 150$). Calculations showed

that participants indeed changed their inputs to the registration page after being provided with privacy prompts. Overall, participants changed their disclosures 167 times ($M = 1.11$, $SD = 1.01$). Descriptively, there were slightly more changes when receiving a prompt in an authoritarian style (88 changes, $M = 1.17$, $SD = .95$) than when receiving a prompt in a consensual style (79 changes, $M = 1.05$, $SD = 1.03$) but the difference was not statistically significant. Nevertheless, there was a significant difference regarding the number of empty fields between the groups receiving privacy prompts ($M_{\text{men}} = 12.78$, $SD_{\text{men}} = 5.83$, $M_{\text{women}} = 16.02$, $SD_{\text{women}} = 5.58$) and not receiving privacy prompts ($M_{\text{men}} = 8.38$, $SD_{\text{men}} = 4.66$, $M_{\text{women}} = 10.55$, $SD_{\text{women}} = 5.74$). Thus, if the number of empty fields is considered to represent a person's privacy behavior, then persuasive privacy prompts can indeed be helpful for users to implement a more sophisticated privacy behavior in terms of withdrawal of sensitive information (*H1*). This is in line with observations by Acquisti and colleagues (2017) and Wang and colleagues (2013), who argue that privacy nudges can help shaping users' online privacy behavior. But in contrast to investigations by Wang and colleagues (2013), the privacy prompts in the current study were adapted to the context of the provided information and they were formulated persuasively, anticipating an increased acceptance and a decreased level of disturbance for the test subjects. Results indicate that it is possible to call users' attention to a situation in which they are going to disclose personal information and that the action of disclosing can be interrupted or prevented by a persuasive privacy prompt. It is open to question whether this interruption of an action solely took place because the occurrence of the prompt was an unexpected happening or whether users truly reflected on the privacy-related hint that was given. The latter might have sharpened their awareness of privacy protection and led to a more central cognitive route of making privacy-relevant decisions. According to the Elaboration Likelihood Model (Petty & Cacioppo, 1986), people either use a central or a peripheral route of information processing that influences their decision-making and subsequent behavior. In the context of privacy, a more elaborated processing of privacy-related information might be an indicator of making privacy-aware decisions (Kobsa, Cho, & Knijnenburg, 2016).

In contrast to expectations (e.g., Kaptein et al.; 2012, Schäwel, 2017), neither the persuasive style of the prompt nor reasoning versus no reasoning showed a main effect on users' actual disclosing and withdrawal behavior (*H1a* and *H1b*). However, a two-way

factorial analysis of variance revealed a significant interaction term for persuasive style and provided information within the prompt intervention. It was observed that if the persuasive style was authoritarian, the behavioral difference based on present reasoning versus no reasoning was smaller than if the persuasive style was consensual. In an authoritarian persuasive prompt, additional reasoning led to slightly more information withholding (i.e. empty fields), indicating more pronounced privacy behavior than without information. This shows that a prompt in an authoritarian style is perceived almost equally persuasive with and without reasoning. In general, people tend to rely on authority figures when they need to make a risk-related decision and do not have valid knowledge regarding the decision object (Siegrist & Cvetkovich, 2000). Thus, there might be a basic trust in authorities so that additional information is not required. However, if it is given, the prompt can be even more effective. By contrast, if people have literacy regarding the current topic of interest, they might not be convinced by an authority's opinion (Siegrist & Cvetkovich, 2000). Thus, if people have privacy literacy they would rather rely on their own knowledge than on a system's recommendation. Indeed, social media users with high privacy literacy tend to engage more in privacy protection than do people with low literacy who might not know how to behave securely (e.g., Bartsch & Dienlin, 2016). In contrast to this finding, prompts formulated in a consensual style were shown to be even less effective in triggering information withdrawal if they included reasoning. This might be attributable to an anchoring effect, namely, that people tend to rely on friends and peers (as an anchor) whereby they do not require additional proof for validity (e.g., anchoring, Acquisti et al., 2017). Participants might have associated the amicable formulation of the consensual prompt with recommendations by friends or peers. Following Acquisti and colleagues (2017), users often rely on anchoring biases when making privacy related decisions; they "may tend to take the example of their trusted peers as a reference point for what is appropriate to post and emulate them" (Acquisti et al, 2017, p. 44:7). Utz and Krämer (2009) also concluded that users of SNSs would be more likely to follow a privacy recommendation more likely if it is given by peers instead of authority figures. In 2012, Acquisti, John, and Loewenstein found that users are more likely to make sensitive disclosures if their friends do so too, which would emphasize this assumption. It is open to question whether this reference point is sufficient in convincing users and initiating

behavior so that no further reasoning is needed or whether the message was ineffective in general. From another perspective, a conceivable explanation for the contradiction between users' stated desire to be informed about privacy risks (Schäwel, 2017) and current findings that more information within a privacy recommendation does not necessarily lead to more cautious privacy behavior, might be the often-observed phenomenon which is a gap between reported and actual attitudes and needs (Dienlin & Trepte, 2015; Fazio & Roskos-Ewoldsen, 1994). Objectively, people want to be informed about privacy risks (Schäwel, 2017). However, coping with given information in specific situations might be uncomfortable, especially if there are many words to process, as was the case for the persuasive privacy prompt with reasoning compared with the one without reasoning in the current study. Having more information to process can result in an information overload and subsequently in reactance (Rogers & Agarwala-Rogers, 1975). Nevertheless, the interaction effect for the persuasive style of a prompt and present reasoning demonstrates the relevance of considering the style of a prompt and the given information alike. Moreover, the prompts were not shown to be differently supportive for male and female users, although a general difference in privacy behavior between female and male users, when not considering the influence of the prompts, was observed. The difference between male and female users with regard to privacy behavior was also shown in prior research (e.g., Youn & Hall, 2008). To conclude, the effect of persuasive privacy prompts depends more on the prompt itself than on the variable sex. With a view to application, this indicates that there is no special need to create different prompts for females than for males. More interestingly, results suggest that users' cognitive capacities and routes of elaboration potentially have an influence on the impact of persuasive privacy prompts. This might be a research topic for future studies.

It was hypothesized that persuasive privacy prompts are more effective if they are tailored to the user, meaning that positive evaluations of the persuasive style that is used in the prompt influence the impact of the prompt (Kaptein et al., 2012, *H2*). There were no significant moderation effects for the authoritarian and consensual style. Mean values indicate that both persuasive styles were evaluated approximately equally positively by participants of the sample. It should be noted that participants were assigned to the experimental conditions independently of their preferences for persuasive styles. In contrast to the study by Kaptein and colleagues (2012), who examined the influence of

tailored persuasive messages on participants' behavior during a period of two weeks, subjects in the current study were provided with persuasive messages solely during a 10-minute interaction with a social network. Given that persuasive elements are especially influential during a long-term interaction or repeated usage (e.g., *macrosuasion*, Fogg, 2002), this might be a reason why participants' susceptibility to persuasive styles did not have a significant impact on the effectiveness of the persuasive prompts in the current study.

Calculated analyses of regression regarding the predictive power of participants' personality characteristics under consideration of their sex revealed only one predictor being significant and one predictor being marginally significant in explaining the number of changes (for $n = 150$), namely, need for privacy ($\beta = .17, p < .05$) and vulnerable narcissism ($\beta = .16, p = .051$, for $n = 150$). However, in both cases the whole regression model including sex as control variable was not significant. Still, the positive relation between test subjects' need for privacy and the number of changes as a consequence of the persuasive prompt intervention was in line with the stated hypothesis. The positive beta value indicates that persons with a high need for privacy tend to change their disclosures more frequently than those with a low need for privacy. Given that the overall model does not show a good degree of prediction of the number of changes, this result needs to be considered very carefully. The same is true for the predictor vulnerable narcissism, which had a marginally positive contribution toward explaining the variance in the number of changes. Despite this marginally positive predictive power of users' vulnerable narcissism, the overall model does not result in a significantly good degree of prediction. However, results indicate that persons with a high need for privacy and with a vulnerable narcissistic personality might be more prone to a privacy support intervention as was presented in the current study. As outlined by Blanchio, Przepiorka, Boruch and Balakier (2016), users' need for privacy is a negative predictor of their Facebook usage and the tendency to Facebook addiction. Furthermore, need for privacy is negatively related to online self-disclosure (Zlatolas, Wezler, Heričko, & Hölbl, 2015). The results of the current analyses support these findings in terms of users with a high need for privacy are less willing to disclose sensitive information to their online networks. Still, even users with a high need for privacy might find themselves in unaware situations in which their need for privacy is overridden by other situational factors such as short-

term gratification or strong emotions, for instance. Under such circumstances, users with a pronounced need for privacy might be more prone for privacy interventions than users with a low need for privacy. With a view to application it can be argued that privacy prompts for users with a high need for privacy would not necessarily need to be formulated as persuasively as for users with a low need for privacy.

Since personality characteristics in prior studies were shown to be related to online privacy behavior (e.g., Ahn, Kwolek, & Bowman, 2015; Bansal, Zahedi, & Gefen, 2016; Christofides, Muise, & Desmarais, 2009; Hofstra, Corten, & van Tubergen, 2016), it was hypothesized that the effect of the privacy prompt on users' actual privacy behavior is moderated by their personality (*H4*). Significant negative main effects of subjects' need for popularity ($\beta = -.17, p < .05$) as well as their vulnerable narcissism ($\beta = -.21, p < .05$) on the number of empty fields were found. Despite this effect, the interaction terms of all moderated regressions with regard to the relation between prompting and the number of empty fields, including reported personality characteristics as moderator variables, did not show significant beta values. Nevertheless, the final model of moderated regression considering the predictor prompting, the moderator need for popularity, and the control variable sex accounts for approximately 22% of the number of empty fields. In particular, it was observed that prompting ($\beta = .33, p < .001$) and the manifestation of users' need for popularity ($\beta = -.17, p < .05$) each can significantly predict the number of empty fields. But the assumption that the effect of a privacy prompt is moderated by test subjects' need for popularity was not supported by the data. It can be argued that this result depends on the restrictive circumstances of the current experiment. More precisely, people's manifestations of personality influence their behavior especially in a long-term manner. Personality characteristics are stable traits that influence long-term behavior (e.g., general privacy behavior), whereas situational cues might have a stronger impact on particular actions in a specific situation such as in the current experiment. Furthermore, other individual variables like people's cognitive capacities, thinking styles, and willingness to process given information might influence the impact of privacy prompts as well (e.g., Kehr, Kowatsch, Wentzel, & Fleisch, 2015). In line with the non significant results, it is conceivable that users' personality impacts their attitudes toward technical privacy protection interventions rather than particular actions based on the persuasive suggestions

of a system. Therefore, future studies should investigate the effectiveness of persuasive privacy prompts in a long-term experiment.

A similar pattern was observed when analyzing the potential moderating effect of users' vulnerable narcissism. The final model of moderated regression including the interaction between prompting and vulnerable narcissism accounts for 19% of the number of empty fields. However, beta values show that the predictor prompting was more important for explaining privacy behavior than the variable vulnerable narcissism. The interaction terms between prompting and vulnerable narcissism were not significant. Results indicate that vulnerable narcissism is an important factor for users' online disclosure behavior. But in contrast to the present hypothesis which is based on the findings by Ahn, Kwolek, and Bowman (2015) a negative relation between users' vulnerable narcissism and the number of empty fields (i.e. privacy behavior) was observed. One reason for not finding results in line with the aforementioned authors might be that the operationalization of the dependent variable in the present study differed from the analyzed variable in the work by Ahn, Kwolek, and Bowman (2015). They argued that vulnerable narcissistic persons engage more in restricting privacy settings on SNS (Ahn, Kwolek, & Bowman, 2015). In the present study, the type of privacy behavior, namely not providing personal information instead of self-disclosing, might be based on different motives. Furthermore, Ahn, Kwolek, and Bowman (2015) investigated self-reported intentions to control for privacy instead of analyzing actual behavior. As known from other studies, people's actual behaviors can differ from their reported attitudes and intentions (Dienlin & Trepte, 2015). Vulnerable narcissistic persons might indeed want to protect their privacy more strongly, based on their typically manifested fear and suspect (Wink, 1991). However, when analyzing real behavior, the desire for recognition and special treatment based on their belief to deserve more attention than other people, rooted in narcissistic personality tendencies (Wink, 1991), might outweigh their concerns and the willingness to control for online privacy. Strikingly, as reported with regard to Hypothesis 3, vulnerable narcissism was a positive predictor of the number of changes in input fields. This seeming contradiction between results regarding the two different operationalizations of privacy behavior can be integrated with the findings by Ahn, Kwolek, and Bowman (2015) as follows. The changes in input fields after receiving persuasive privacy prompts are more closely transferrable to users' intention to protect

for privacy, which is triggered by the persuasive privacy prompt. That is, the self-reported intention toward privacy protection might be given for vulnerable narcissistic persons (as observed by Ahn, Kwolek, & Bowman, 2015) but this reported intention might not be sufficient in triggering actual privacy behavior. By contrast, the privacy prompt intervention might trigger the respective fears of vulnerable narcissistic persons and in turn initiate protective intentions resulting in withdrawing any given information about the self after being exposed to a privacy intervention. From a methodological perspective, the opposing results regarding the influence of vulnerable narcissism can also be attributable to operationalization of the dependent variables number of changes and number of empty fields. Since there was a positive relation between the number of changes and vulnerable narcissism, this indicates that users with strong vulnerable narcissism provided a particular amount of information that they deleted after receiving a privacy prompt. Thus, the finding that vulnerable narcissistic persons had fewer empty fields in the end than persons with a lower extent of vulnerable narcissism is still in contradiction to the stated hypothesis but actually fits to results of Hypothesis 3. Only if users disclose a certain amount of information (and consequently have fewer empty fields in the end, as was shown for vulnerable narcissistic persons in *H4*) do they have the possibility of making a lot of changes, resulting in a positive relationship between vulnerable narcissism as found in Hypothesis 3.

Second, in line with the stated hypothesis, users' need for popularity was significantly negatively related to the number of empty fields (for $N = 187$), indicating the need for popularity to be a strong predictor of online disclosure behavior (e.g., Christofides, Muise, & Desmarais, 2009; Hofstra, Corten, & van Tubergen, 2016; Utz, Tanis, & Vermeulen, 2012). People with a high need for popularity want to be visible to get as much feedback as possible (e.g., Utz, Tanis, & Vermeulen, 2012). A small number of empty fields in the current study would allow for more feedback and recognition by other users because people are able to see and appreciate disclosed information. However, there was no significant effect of users' need for popularity on the number of changes (for $n = 150$) and no interaction effect with the predictor prompting in the suggested moderation model ($N = 187$). Thus, the need for popularity influences disclosure behavior in general instead of affecting the impact of a persuasive prompt. However, this seems to be quite logical because need for popularity was suggested to have an influence on

disclosure behavior so that the person has more space for self-presentation. Being influenced by a recommendation represented through the number of changes of inputs are no result of being in need for popularity but might rather be attributable to other characteristics such as privacy concerns or anxiety, warranting future investigation.

In line with prior findings, results indicate that personality can indeed influence privacy behavior (e.g., Christofides, Muise, & Desmarais, 2009; Hofstra, Corten, & van Tubergen, 2016; Utz, Tanis, & Vermeulen, 2012). However, users' personality characteristics were not significant moderators for the relation between prompting and the decision to not disclose personal information (i.e. the number of empty fields). Contrary to our expectations, this indicates that the effect of prompting on behavior in our experiment was neither strengthened nor weakened by users' manifestation of personality.

Analyses with regard to the last hypothesis (*H5*) demonstrate that psychological privacy-related concerns can significantly predict psychological privacy-related behavior. Specifically, the number of changes in psychological privacy-related fields (i.e. religion & politics and about you) can be predicted by psychological privacy concerns by approximately 5%. This indicates that people with psychological privacy-related concerns are likely to withdraw very intimate information like political or religious beliefs after seeing a psychological privacy-related privacy prompt. Thus, if a user is generally concerned regarding specific privacy risks, privacy support dealing with this kind of concern might be especially helpful. Since regression analyses were calculated instead of moderation analyses, it cannot be concluded but only suggested that the effect of a prompt concerning a specific dimension of privacy is strengthened by respective concerns. However, data indicate that psychological privacy-related concerns are an important factor for specific privacy behaviors, which demonstrates that it is important to consider privacy concerns in a sophisticated manner (informational-, social-, and psychological-related privacy concerns) when investigating the impact of technical privacy support. In addition, system-based privacy support measures can gain efficiency if users' concerns are specifically addressed.

12.7 Limitations and Future Work

Despite this study contributes to the research field of technical privacy protection, it also has some limitations as well. For instance, the presentation of the stimulus material (i.e. persuasive privacy prompts) was not the same for all participants of one experimental group. This is due to the fact that, for reasons of credibility and consistency, participants were only prompted if they disclosed information (through an input field, checkbox, or radio button). Since the amount of disclosed information (i.e. how many fields and boxes the user would click on) was unknown beforehand, it was not foreseeable how many prompts the participants would see on average. Participants who decided to reveal only very little information did not get many privacy prompts in comparison with those who disclosed a lot. However, those who already reveal sparse information may not need privacy prompts. Most participants in this study were female. Future studies should have a more balanced distribution of male and female participants. However, it was controlled for effects of the variable sex in the analyses, whereby the effect of privacy prompts was not found to be different between female and male users. Furthermore, the low value of reliability for examining people's susceptibility to persuasion for the style authority can be regarded as a limitation. Future studies should consider more sophisticated scales for measuring users' susceptibility to particular persuasive strategies if they aim at adapting the persuasive style of a prompt to its user. Furthermore, the low value for interrater reliability with regard to explorative qualitative analyses of participants' free text inputs ($\kappa = 0.3$) constitutes a strong limitation. This might be due to the challenge of defining sensitive information and qualitatively distinguishing it from non-sensitive information. However, this limitation solely affects explorative analyses of the individually formulated statements regarding the self. The main dependent variables in this study (i.e. number of changes and empty fields) are based on predefined sensitive categories allowing for less individual variation. Concerning calculative power of the current results, it should be admitted that most effect sizes are rather small to medium so that, for generalizability, future studies with bigger samples are needed. Moreover, future research should focus even more carefully on how a privacy prompt is visualized and formulated, and how often it is presented (i.e. "timing" by Acquisti et al., 2017). In addition, the social dimension of privacy should be covered more explicitly for investigation, for instance through a setting regarding the visibility of provided information for other users or the possibility to define

communication circles or friend lists. Since a dummy network was used in this study, the privacy prompts were not fully adapted but randomly occurred for predefined situations. In future work the full adaptation to the information and the user should be realized by means of an instructional awareness system that is grounded on a database including privacy as well as user information (e.g., Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016). However, in this work it was concentrated on the effect of a prompt and its persuasive style and its impact on subsequent behavior. Since explorative analyses revealed significant positive correlations between the number of changes and users' evaluations of persuasive privacy prompts as well as the intention to use a system that would provide this kind of privacy support, the mediating role of the evaluation of privacy prompts needs to be examined more carefully in future studies.

12.8 Conclusion

It was revealed that it makes a difference in privacy behavior whether a user receives a privacy prompt or not. Raising the question of whether people want to publish particular pieces of information can indeed result in less (sensitive) information disclosure. The effect of a prompt was influenced more strongly by its appearance and the amount of information provided in the prompt than by users' specific personality traits. Users' vulnerable narcissism, their need for popularity, and the need for privacy are important predictors of general privacy behavior but these characteristics did not alter the impact of persuasive privacy prompts on actual privacy behavior in the present study. Psychological privacy-related concerns predicted the number of changes in psychological privacy-related fields, indicating that users' manifestation of specific concerns relating to specific dimensions of privacy is an important factor to consider for adapted privacy support. In sum, it was revealed that the effects of persuasive privacy prompts depend not only on one variable but rather on the multifaceted interplay of its formulation, the provided information, users' specific privacy concerns as well as their evaluation and acceptance of provided privacy support. These insights should be integrated in the elicitation of requirements for technical privacy support in order to help users in maintain their privacy. This study contributes to the field of human-computer interaction in terms of providing into system-based possibilities to support users in online privacy protection.

Summary Study 3

A lack of privacy awareness with respect to information disclosure on online social networking sites (SNSs) can result in privacy risks for users. As presented in Chapter 7.5, there are different approaches for reducing privacy risks, for example, raising awareness through nudging and prompting. In order to better understand user-oriented variables that influence the effectiveness of persuasive privacy prompts in human–media interactions, Study 3 examined users’ behavior after being exposed to persuasive privacy prompts on an SNS. Users’ characteristics were considered as influencing factors. Persuasive styles (authority vs. consensus) and the presence of reasoning (no reasoning vs. reasoning) within the prompts were varied and the responses to the prompts by people of a control group receiving no prompts were observed as well. Data demonstrated that participants receiving privacy prompts disclosed less information than those who did not receive privacy prompts. It was pointed out that a prompt without additional information and in a consensual style led to lowest extent of self-disclosure. In contrast to the stated hypotheses, participants’ personality traits and their susceptibility to the presented persuasive styles were not significant moderators of the effect of privacy prompts.

Based on the results and the limitations of Study 3, the last study in the scope of this dissertation was designed. It was decided to focus further on the consensual style of communication for transmitting privacy-related information. Further, the scope for protective interventions was widened so that not only text-based interventions but also visual cues, indicating the current level of privacy, were considered. Moreover, one limitation of Study 3 was addressed, namely, the difficulty of deciding when and how often to provide a privacy intervention. The privacy interventions in Study 4 were present during the whole interaction with the registration form of the social network (which was basically the same as the one used in Study 3, with some exceptions that will be addressed in Chapter 13.6) but the color changed depending on the amount of disclosed information. This was done to indicate the current privacy state more carefully and in accordance with the well-known color concept of traffic lights. Furthermore, Study 4 will tackle an additional issue, namely, concrete decision-making processes with regard to the question of whether to disclose a posting or not by investigating the privacy calculus in more depth than was done in prior research using self-reports of users. Study 4 will concentrate more

strongly on risk-communication and decision-making processes in the realm of online privacy.

13 Study 4: The Influence of Persuasive Privacy Support on the Dynamics of Self-Disclosure, Self-Withdrawal, and Calculating Privacy

The goal of the final study in this dissertation is to further reflect on findings from Study 3 with regard to the effectiveness of persuasive privacy interventions. Therefore, the basic SNS environment that was developed for Study 3, was used again for investigations. Study 4 extends analyses from Study 3 via testing additional variations in the design and functionality of system-based privacy interventions. Based on reported findings with regard to the persuasive self-monitoring features and findings from Study 1, which indicate that users want to have a concrete indicator of potential privacy risks such as a privacy-meter, and the findings from Study 3, revealing that a consensual style of communication might be promising for communicating current privacy risks, this study provides three different kinds of privacy interventions. The system-based interventions in Study 4 were a privacy traffic light and an information box (both dynamically adapting the color), and an information without visual assistance. Additionally, Study 4 aims at further elaborating on the role of risks for privacy decision-making by drawing on the privacy calculus (Culnan & Armstrong, 1999).

13.1 Introduction

As already outlined in Study 3, a promising measure to support social media users in privacy-aware behavior is to provide risk-related interventions referring to potential negative outcomes of the disclosure of sensitive information by means of system-based support measures such as privacy prompts or warning messages in social media environments (see also Acquisti et al., 2017).

Users' perception of online privacy conditions is an important factor influencing their disclosure behavior (Dienlin & Metzger, 2016). The perception of a present online privacy state might affect the individual's cognitive processing and coping with potential privacy threats. Based on the privacy calculus (Culnan & Armstrong, 1999) and a model

for decision-making (Schiebener & Brand, 2015), the individual processes of assessing privacy risks and weighing the threats against the benefits of disclosing and withdrawing information are addressed in the following chapters. Research on online privacy protection and empowerment of users based on supportive systems raises the question of how to adequately communicate potential privacy risks in a crucial situation of endangerment, without causing reactions such as reactance or frustration (e.g., Acquisti et al., 2017; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016). Following the privacy calculus (Culnan & Armstrong, 1999; see Chapter 5.2) and the protection motivation theory (Rogers, 1975, see Chapter 5.4), concerns and perceived risks are relevant drivers for people's behavior and decision-making. In the context of online privacy, decisions pertain to disclosing or withdrawing personal information or implementing privacy settings, for instance (Metzger & Dienlin, 2016).

Study 4 aims to provide insights about the impact of system-based risk-communication on users' privacy behavior. Moreover, the current study's goal is to reveal knowledge about users' decision-making processes related to privacy risks. Therefore, users' disclosure and withdrawal behavior in a realistic social network environment is investigated after current privacy states are provided by means of system-based persuasive privacy interventions. Furthermore, users' decision-making processes are analyzed by means of a choice-based conjoint (CBC) analysis. This method allows for the examination of the relative importance of a particular attribute and its levels for making a decision without asking participants directly but rather indirectly about their preferences with regard to a decision (Luce, 1979). The underlying principle of this measure will be explained in more detail in the method section of this study. As far as can be derived from the literature, to date there is no study in the online privacy realm examining self-disclosure decision processes on SNSs by means of a CBC analysis. However, the oftentimes experienced difficulties of examining users' online privacy behavior by means of self-reports of individuals (e.g., biased responses) emphasize the need for more sophisticated measures in order to better understand users' online privacy decisions and to derive insights for efficacious support measures for reducing privacy risks.

Given that people's personal characteristics can influence their online privacy behavior (see Chapter 6.2), users' expression of personality traits that are related to

privacy behavior (see Chapter 6.2) as well as their privacy awareness, concerns, and perceived privacy norms (see Chapter 6.3) are also exposed. In particular, it was analyzed whether specific personality traits of users moderate the impact of the privacy interventions on their behavior after being exposed to that intervention. In the following, the specialties of online privacy behavior, privacy-aware decision-making, and the roles of persuasion and personality in the realm of online privacy protection are outlined.

13.2 Calculating Online Privacy

Research on online privacy behavior repeatedly revealed a lack of users' privacy awareness and knowledge regarding privacy protective actions. As already introduced, the privacy paradox describes the missing link between users' privacy concerns and attitudes, and their risky privacy behavior, representing an attitude–behavior gap (Barnes, 2006). More recent approaches point out the methodological shortcomings of the privacy paradox, for instance, the incomplete considerations of influencing factors such as behavioral intentions (e.g., Dienlin & Trepte, 2015) and the complexity of risk evaluation processes. Approach that tackle these shortcomings are for instance the privacy process model by Dienlin (PPM; 2014) and the privacy calculus (Culnan & Armstrong, 1999). The PPM claims that an individual engages in privacy regulation if, depending on the privacy context, privacy perception, and current privacy behavior, the present privacy status is not equivalent to the desired status of privacy (Dienlin, 2014). The process of regulating privacy also depends on the controllability that the individual perceives (Dienlin, 2014). However, if users are not aware of a situation being threatening to their privacy, the process of privacy regulation does not take place. External cues indicating potential privacy invasions might help to trigger such regulation processes (as suggested by Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016; see Chapter 8.1). As outlined in Chapter 5.4, the privacy calculus (Culnan & Armstrong, 1999) states that individuals evaluate risks and benefits of self-disclosure rationally based on privacy concerns, anticipated benefits, and trust beliefs, (Dienlin & Metzger, 2016; Krasnova, Veltri, & Günther, 2012). However, human beings are not able to act exclusively rationally, making it impossible for them to evaluate risks and benefits of information disclosure comprehensively under varying situational conditions (Rogers, 1983), calling for awareness-raising tools. Depending on individual characteristics (e.g., cognitive

flexibility or the need for cognition; Schiebener & Brand, 2015; Kehr, Kowatsch, Wentzel, Fleisch 2015) and the consulted route of information processing (e.g., central vs. peripheral or impulsive vs. reflective; Petty & Cacioppo, 1986; Schiebener & Brand, 2015, see also Chapter 3.1), the perception of privacy-relevant situations might differ among individuals, influencing the perceived privacy control and the willingness to change behaviors. As also explained in relation to Study 2, perceived risks and privacy concerns have been revealed to be negatively related to online self-disclosure, whereas benefits have been shown to be positively related to self-disclosure (e.g., Dielin & Metzger, 2016; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Krasnova, Kolesnikova, & Guenther, 2009). Though, Dienlin and Metzger (2016) found no relation between Facebook benefits and withdrawal of information but a positive relation between privacy concerns and withdrawal of information. However, so far, the weighing process of the privacy calculus seems to be a black box because only little is known about the individual relative relevance of the benefits and consequences for users. It is important to consider anticipated negative (i.e. severity and likelihood of negative consequences) as well as positive outcomes (i.e. rewards) regarding self-disclosure in order to investigate this complex process in a more sophisticated way. In addition to the impact of evaluation processes regarding anticipated risks and benefits of self-disclosure, online privacy behavior is also shaped by users' personality characteristics (see Chapter 6.2). This indicates that the processes of evaluating current and desired states of privacy, the evaluation of privacy risks, and subsequent disclosure behavior occur depending on the individual's personal (as well as situational) characteristics. In the following sections, first, the influence of decision-making styles and, second, the impact of personality on (online) privacy behavior are outlined in more detail.

13.3 Processing of Privacy-Relevant Information and Privacy-Aware

Decision-Making

As outlined in Chapter 3.1, a situation can trigger different processes of information evaluation and subsequent decision-making (impulsive or reflective, Bechara, 2005; Schiebener & Brand, 2016). Making (privacy) decisions brings risks of uncertainty regarding the outcomes of the decision (Schiebener & Brand, 2015; Yates & Stone, 1992), which can be for instance the loss of privacy due to disclosing personal

information (Malhotra et al., 2004). Since users' perceived privacy risks were demonstrated to be positively related to their privacy concerns (e.g., Dinev & Hart, 2004; Xu & Chen, 2013), Study 4 aims at investigating the role of perceived risks in terms of negative consequences occurring and the likelihood to which they occur. Owing the importance of perceived risks in users' evaluation of their current privacy situation and potential behavioral changes, this work utilizes the evaluation of a given privacy-relevant situation by means of a sophisticated measure of decision-making research that is a CBC analysis. In addition, users will interact with a registration form of an SNS (as participants in Study 3 did) and their privacy behavior will be examined. However, before explaining specific functionalities of the SNS, which have been modified after Study 3, further variables that are considered in this work, will be summarized.

13.4 Persuasion and Personality

Persuasive strategies offer the potential of increasing the effectiveness of system-based privacy support interventions. Persuasive nudges can call for users' attention in a privacy-relevant situation (Acquisti et al, 2017; Wang et al, 2013). Since the processes of persuasion do not solely depend on the characteristics of a persuasive message but also on users' personal characteristics (Haugtvedt & Petty, 1982), Study 4 considers users' personality, as was also done in Study 3. Personal traits that are considered in this work are vulnerable narcissism, self-control, need for cognition, and the need for privacy. For a detailed overview of the aforementioned characteristics, please refer to Chapter 6. In addition, the influence of perceived privacy norms, users' privacy concerns, and their situational affect are considered in the analysis.

Prevalent social norms can seduce people to respond in a way they think that the society or peers believe it would be appropriate to respond (e.g., Asch, 1951; Park & Smith, 2007). With regard to SNSs, it has been shown that perceived social norms referring to appropriate privacy behavior can positively influence the usage of restrictive privacy settings (Utz & Krämer, 2009). Further, Utz and Krämer (2009) suggested that privacy-protective recommendations might be especially influential if they are communicated by peers instead of authorities. This study considers perceived privacy norms (distinguishable into peer, societal, and media norms) as a potential

factor shaping users' privacy behavior when responding to system-based persuasive privacy support.

Privacy concerns refer to the potential loss of privacy as a negative consequence of disclosing personal information (Xu et al., 2008). In the context of SNSs, privacy concerns were shown to predict users' online self-disclosure and self-withdrawal behavior (Dienlin & Metzger, 2016). Therefore, when analyzing privacy decisions, it is important to consider users' anticipated negative consequences of self-disclosure.

Early research on emotions and cognitions demonstrates the impact of both, emotion and cognition, on people's behavior (e.g., Lazarus & Folkman, 1984). Li, Zhang, and Sarathy (2018) investigated the mediating role of emotions in the relation between online privacy concerns and privacy management strategies. It was demonstrated that the impact of users' privacy concerns on their usage of preventative privacy management strategies was entirely mediated by negative emotions, namely, frustration and regret. In addition, it was observed that the influence of privacy concerns on users' self-censoring behavior was mediated by regrets. This is congruent with earlier findings by Wang and colleagues (2011), who suggested users' regrets of online self-disclosure to be a critical factor shaping future online behavior of users. Given the importance of users' emotions concerning their privacy protection behavior, Study 4 argues that users' positive and negative affect might play an important role with regard to the evaluation of privacy protection tools as well.

In sum, persuasive privacy interventions can increase users' attention in a privacy-relevant situation (Acquisti et al, 2017; Wang et al, 2011). If recognized, those support measures can either trigger the impulsive or the reflective route of information processing (Schiebener & Brand, 2015). Both can hypothetically lead to more secure privacy behavior. The reflective system might influence the behavior in a more long-termed manner, whereas the impulsive system would lead users to take or avoid benefits or risks on a short-term basis. Users' evaluation of privacy risks and potential consequences of self-disclosure (i.e. privacy calculus) can, on the one hand result in online self-disclosure (if benefits are more salient than risks) or, on the other hand, in self-withdrawal (if risks are more salient than benefits; Metzger & Dienlin, 2016). In the following, the hypotheses and research questions of Study 4 are presented.

13.5 Hypotheses

This study focuses on the impact of persuasive privacy interventions (information vs. information box vs. traffic lights; see method section) on disclosure behavior and corresponding risk evaluation processes of individuals. Since it has been shown that persuasive elements and warning messages referring to online privacy can help to change users' behavior (e.g., Acquisti et al., 2017; LaRose & Rifon, 2007; see Chapters 8.4 and 8.5; see also Study 3), the presence of privacy interventions is assumed in resulting in less self-disclosure compared with the usage of SNS without privacy interventions (*H1a–H1c*):

Hypothesis 1a (H1a): Users will disclose less information (i.e. higher number of empty fields) when being exposed to privacy interventions than when not being exposed to privacy interventions.

Hypothesis 1b (H1b): Users' disclosures are less sensitive (i.e. related to the self or not) when being exposed to privacy interventions than when not being exposed to privacy interventions.

Hypothesis 1c (H1c): Users' disclosures are less diverse (i.e. the number of different categories of self-related information) when being exposed to privacy interventions than when not being exposed to privacy interventions.

Since the impact of persuasive measures can differ regarding particular factors and users' individual susceptibility to persuasion (e.g., Kaptein, De Ruyter, Markopolulos, & Aarts, 2012; see Study 3), it was aimed to find out which privacy intervention would be the most effective for supporting users in reducing sensitive disclosures:

Research Question 1 (RQ1): Which kind of privacy intervention (traffic light, prompt, information) is the most effective for inducing privacy-aware behavior (i.e. the number of empty fields)?

A common concern with regard to privacy intervention measures is users being annoyed resulting in reactance reactions. Therefore, it was aimed to find out whether the

experience with the SNS would be evaluated worse if privacy interventions are present than if no interventions occur. In addition, it was investigated whether users' current affect is positively or negatively influenced by the presence of privacy intervention measures:

Research Question 2 (RQ2): Will the evaluation of the experience with the SNS differ based on whether there was a privacy intervention or based on the different intervention types?

Research Question 3 (RQ3): Will users' positive and negative affect be influenced by the exposure to privacy interventions?

Given that users' personality traits, concerns and perceived norms have been shown to be related to privacy behavior and the intention to disclose or withdraw information (see Chapters 5.2, 6.1, 6.2) personal characteristics were suggested to moderate the impact of privacy interventions on disclosure behavior:

Hypothesis 2 (H2): The impact of the privacy interventions on participants' privacy behavior is (a) enhanced by users' need for privacy and vulnerable narcissism, and (b) mitigated by users' self-control

Hypothesis 3 (H3): The impact of the privacy interventions on participants' privacy behavior is enhanced by users' privacy concerns.

Hypothesis 4 (H4): The impact of the privacy interventions on participants' privacy behavior is enhanced by users' perceived privacy norms.

Based on findings related to privacy decision-making and the relevance of negative experiences for privacy behavior (Wang et al., 2011) as well as the negative influence of perceived risks and concerns on online self-disclosure (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Krasnova, Kolesnikova, & Guenther, 2009), the severity of anticipated negative consequences of information disclosure was hypothesized to be perceived as more relevant for the decision to reveal or not reveal personal information compared with the importance of anticipated benefits. Furthermore,

given that the need for cognition has been shown to play a significant role in decision-making and is related to effortful elaboration of information (Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Schiebener & Brand, 2015), it was assumed that the need for cognition is positively related to the relative importance of negative consequences that might follow sensitive information disclosure, and negatively related to anticipated benefits that are more closely related to subjective and emotional thinking processes (Bechara, 2005, see also Chapter 6.2.5).

Hypothesis 5 (H5): Users base their decisions regarding disclosures more strongly on the anticipated severity of consequences of self-disclosure than on anticipated benefits or the likelihood that a consequence occurs.

Hypothesis 6 (H6): Users' need for cognition has an influence on their privacy-related decision-making, that is, users with a high need for cognition evaluate risks and negative consequences (central, objectively) as more important than benefits (peripheral, emotional)

13.6 Method

The current study investigates the effectiveness of three different types of privacy interventions on users' actual behavior within a social network environment by means of a 3×1 between-subjects experimental setting. A control group who got no privacy intervention was considered as well. In order to analyze actual behavior, a self-developed nonartificial environment, namely, an interactive online registration form of an SNS is used for the current study. Participants were asked to register for the social network. The social network provided space for basic information such as name or birthdate (informational privacy), for information regarding religious and political views (psychological privacy), allowed for individual self-disclosures regarding the self, and provided different settings for regulating the visibility of the created profile (social privacy). The dimensions of privacy are explained in Chapter 2.1. Depending on the experimental condition, the registration form provided either privacy-related information in the welcoming text or a privacy-related persuasive prompt (in both cases saying "Everybody agrees: To protect your privacy you should be aware of the kind and amount of information you disclose"), or a privacy-risk-related visual cue (traffic light; see Figure

11). The prompt did not appear or disappear depending on the information provided (as was the case in Study 3) but changed its color depending on the amount of information provided by the individual.

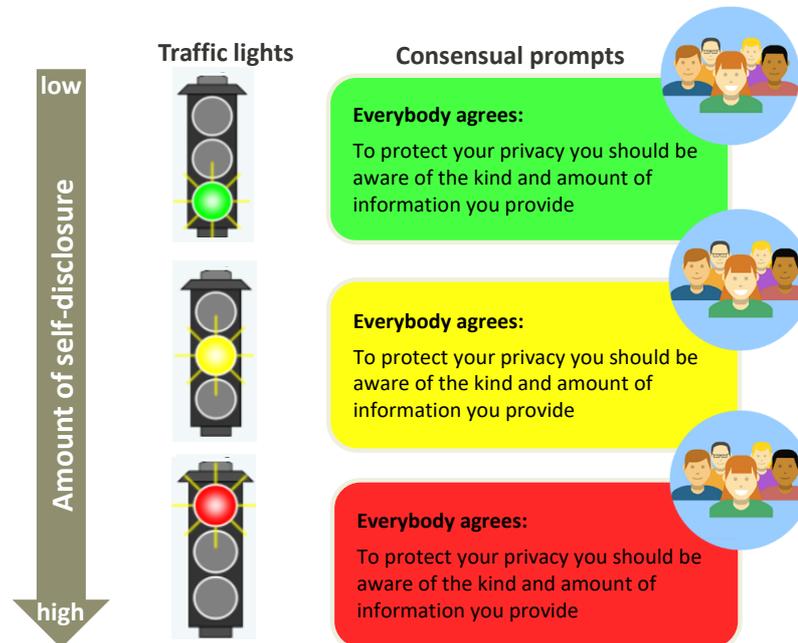


Figure 11: Persuasive privacy interventions (Study 4).

CBC. The CBC task is a method for implicitly assessing users' preferences with regard to a specific decision. Originally, this method was used for economics and purchasing decisions (McFadden, 1974, 1980; Theil, 1970) about products based on the product's attributes and the quality of the attributes (e.g., for a car the attribute *price* with different price categories, e.g., cheap, moderate, expensive; Hondori, Javanshir, & Rabani, 2013). By considering the CBC it is possible to infer which attribute is most important for the person's decision and additionally, which quality of the attribute is most attractive for the person. The calculation of the relative importance of the attributes and qualities is based on hierarchical Bayesian analyses (see Johnson & Orme, 2003). Analyses reveal estimations for the overall sample (i.e. one can detect which attribute is the most important and which quality of this attribute is the most decisive for the full sample). In addition, it is possible to consider values for the relative importance of each attribute and the quality of each participant, which makes it possible to relate users' importance ratings to manifestations of personality. In this study, the CBC was used to estimate the likelihood of users publishing a specific posting related to anticipated

benefits (low rewarding, moderately rewarding, highly rewarding), the severity of a negative consequence (not severe, moderately severe, highly severe), and the likelihood that the consequence occurs (not likely, moderately likely, highly likely). In order to make the hypothetical situation of deciding whether to publish a posting or not with regard to possible outcomes more realistic, the users were confronted with a concrete example and detailed explanations of all attributes and levels. The CBC consisted of three different attributes, namely, reward, consequence, and likelihood that the consequence occurs with each three levels ranging from low to high (see Table 30 and Figure 12).

Table 30
Attributes and levels in the choice-based conjoint task (Study 4)

Attribute	Level
Reward	Low rewarding
	Moderately rewarding
	Highly rewarding
Consequence	Low severe
	Moderately severe
	Highly severe
Likelihood that the consequence occurs	Not likely
	Moderately likely
	Highly likely

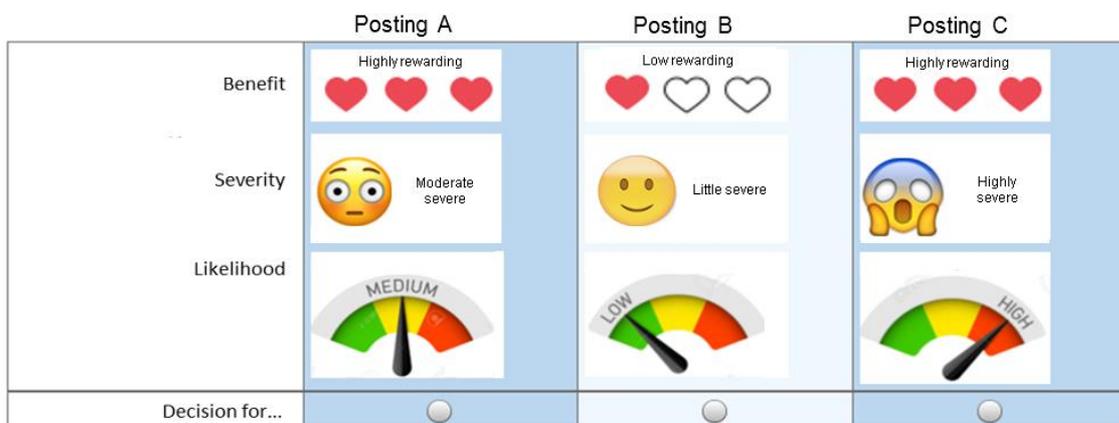


Figure 12: Attributes and levels of the CBC scenario (Study 4).

13.6.1 Measures

Self-control

Self-control was measured on a 5-point Likert scale by Bertrams & Dickhäuser, 2009, consisting of 13 items. Participants were asked to indicate their self-assessments regarding self-control on an integral ranging from 1 = *completely inaccurate* to 5 = *completely accurate* (e.g., “It is hard for me to discard bad habits”). The test of reliability yielded a satisfactory value of $\alpha = .824$.

Narcissism

Participants’ manifestation of vulnerable narcissism was measured by a scale by Hendin and Cheek (1997). On a 5-point Likert scale ranging from 1 = *I don’t agree at all* to 5 = *I totally agree*, participants were asked regarding their self-evaluations (e.g., “I often take comments of others personally”). Reliability did not reach a particularly good value ($\alpha = .688$). However, because excluding single items did not significantly increase reliability, all items were considered for calculations.

Need for cognition

Need for cognition was measured by considering the Scale by Keller, Böhner, and Erb (2000). Fourteen items asked for users’ need for cognition (e.g., “I do not find it particularly exciting to learn new ways of thinking”) on a 7-point Likert Scale ranging from 1 = *completely inaccurate* to 7 = *completely accurate*. Reliability was satisfying ($\alpha = .880$).

PANAS

The positive and negative affect scale from Krohne, Egloff, Kohlmann, and Tausch (1996) who provided a German version of original scale by Watson, Clark, and Tellegen (1988), was considered to get insights regarding users’ emotional mood before and after interacting with the social network. By means of 20 items, participants were asked to indicate their current mood (e.g., *enthusiastic* for positive affect and *upset* for negative affect) on a Likert Scale ranging from 1 = *not at all* to 5 = *extremely*. Users were asked to rate their mood two times. Reliability was $\alpha = .838$ for PANAS_{t1} and $\alpha = .861$ for PANAS_{t2}.

User experience

Users' experience with the website was measured with seven items adapted from Schrepp, Hinderks, and Thomaschewski (2017). Participants were asked to rate their experience with the website on a 5-point Likert scale ranging from 1 = *confusing* to 5 = *clear* or 1 = *inefficient* to 5 = *efficient*, for instance. Reliability was satisfactory ($\alpha = .839$).

Privacy concerns

By means of nine items, participants were asked about their privacy concerns. The items are oriented toward the items assessing privacy intentions, attitudes, and behaviors by Dienlin and Trepte (2015). There were three items each referring to informational, social, and psychological privacy. Participants were asked, for example: "How concerned are you about disclosing identifying data about yourself on your social network?" (informational privacy, $\alpha = .778$), "How concerned are you when you are not restricting access to your profile?" (social privacy, $\alpha = .789$) or "How concerned are you to communicate personal things to your community?" (psychological privacy, $\alpha = .727$). Reliability overall was $\alpha = .874$.

Social norms

Social norms were investigated via three subscales, peer norms (e.g., "Most people who are important to me think that I should care about my privacy on Facebook", $\alpha = .753$), societal norms (e.g., "Society suggests to care about online privacy", $\alpha = .839$), and media norms (e.g., "The media in Germany are clearly in favor of people paying attention to their privacy on the Internet", $\alpha = .803$). Items were adapted to measures by Park and Smith (2007) and assessed on a 5-point Likert scale ranging from 1 = *I don't agree at all* to 5 = *I totally agree*.

Awareness

Privacy awareness was measured by means of three different items (e.g., "I am aware of the privacy and data protection issues and privacy practices of our society", $\alpha = .821$). Participants rated the items on a 7-point Likert scale ranging from 1 = *I don't agree at all* to 7 = *I totally agree*.

Need for privacy

The need for privacy was evaluated by means of a Scale by Trepte and Masur (2017) consisting of three subscales relating to informational (e.g., “I prefer if only little is known about my person”, $\alpha = .781$), interactional (e.g., “There are many things about me that I would rather not talk about with other people”, $\alpha = .695$), and physical privacy (e.g., “In the tram or on the bus I don’t like to sit next to a stranger”, $\alpha = .750$). All items were rated on a 5-point Likert scale ranging from 1 = *I don’t agree at all* to 5 = *I totally agree*.

Privacy behavior

In this study, privacy behavior was operationalized through three variables. First, the number of empty fields was considered as an indicator of privacy behavior. Privacy behavior can be considered to be more pronounced, the more fields a user leaves blank during the registration process. Second, since users had the chance to introduce themselves by means of a self-formulated text, the sensitivity of disclosure was considered as a further privacy behavior variable. Third, users’ self-formulated disclosures related to different categories of content. The more different categories were addressed by users, the more diverse and sensitive their disclosures were. Thus, the number of categories of disclosed information was used as a third dependent variable indicating users’ privacy behavior.

13.6.2 Sample

Overall, 412 people participated in this study. Owing to technical problems leading to missing data and outliers with regard to age, we had to exclude 32 cases. In the end, a total sample size of $N = 380$ participants was considered for investigations. Participants were aged between 18 and 59 years ($M = 26.35$, $SD = 7.40$). Two-hundred-thirty-six persons were female (62.1%) and 144 were male (37.9%). Three persons were pupils (0.8%), 248 were students (65.3%), 93 persons were employees (24.5%), 12 were self-employed (3.2%), eight were seeking for a job (2.1%) and 16 people chose the option “other” (4.2%). As can be seen in Figure 13, almost all participants were social media users, whereof most of them used Facebook ($n = 367$), Whatsapp ($n = 351$) and Instagram ($n = 228$).

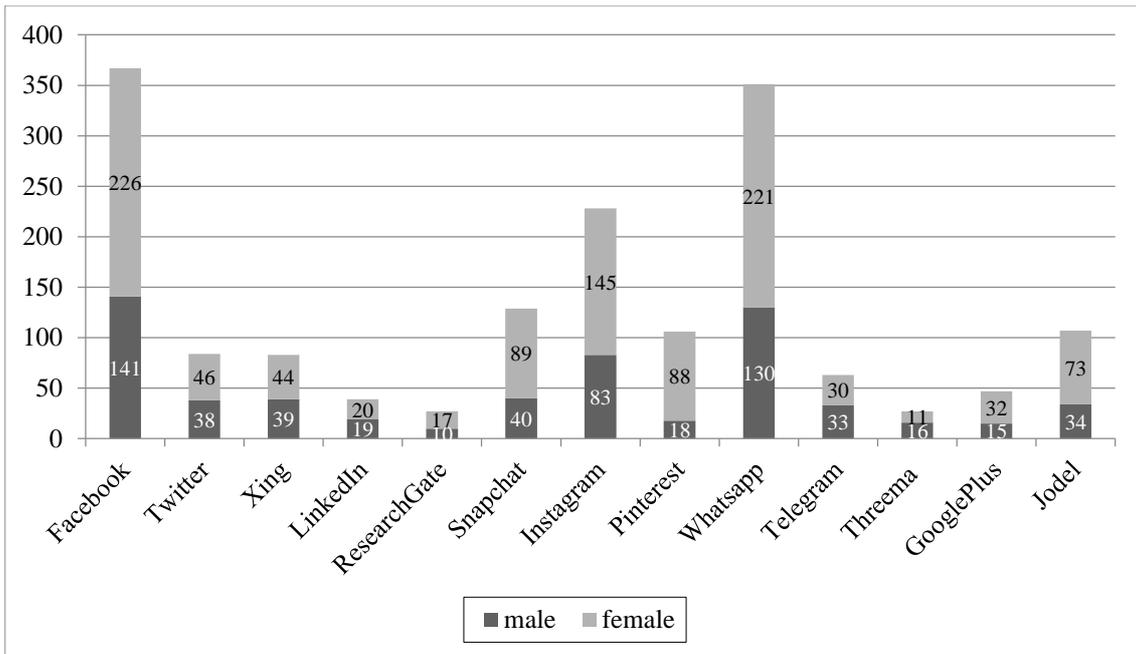


Figure 13: SNS usage of participants (Study 4).

Participants were asked whether they would like to keep the profiles they created in the course of the study after finishing the survey (see Figure 14). Most participants decided to delete the profile ($n = 333$), whereas 47 participants wanted to keep the profile for future interactions. There was no significant effect of the experimental manipulations concerning the decision to keep or delete the profile, $\chi^2(1) = .295, p = .587$.

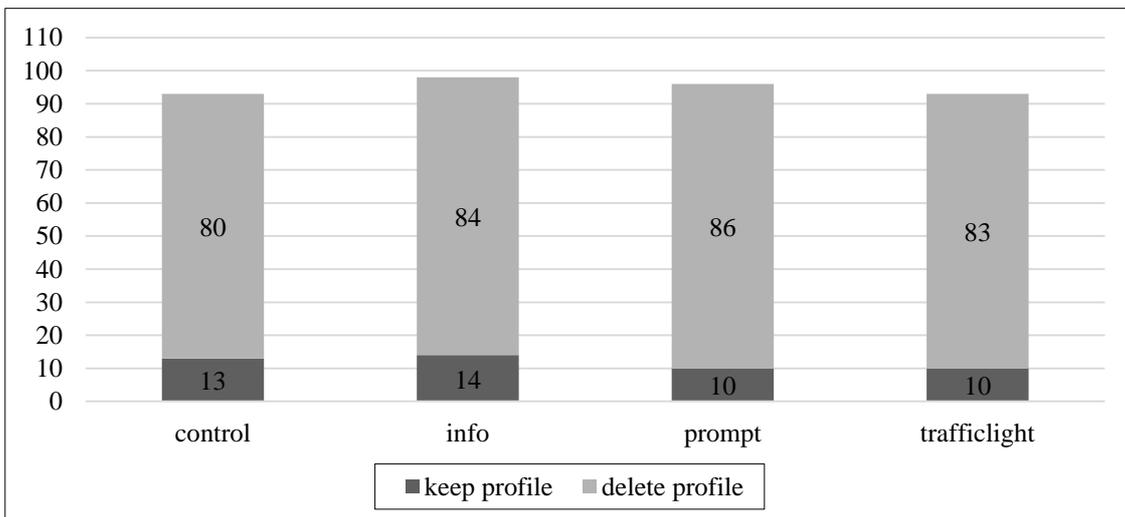


Figure 14: Total numbers of participants deciding to keep or to delete the profile after the survey (Study 4).

13.7 Hypotheses Testing

Hypothesis 1 (H1)

H1a suggested that users who were exposed to privacy interventions (traffic light, prompt, information) will disclose less information (higher number of empty fields) than those who were not exposed to privacy interventions. In order to investigate this assumption, a hierarchical analysis of regression was conducted with the independent variable *intervention versus no intervention* and the dependent variable *empty fields*. Sex was considered as a control variable. The suggested model significantly explained 4% of variance in the number of empty fields, $R^2 = .040$, $F(2, 377) = 7.82$, $p < .01$. Beta values indicate a significant positive effect for the control variable sex ($\beta = .172$, $p < .01$) and a significant positive influence of the variable intervention versus no intervention ($\beta = .101$, $p < .05$) on the number of empty fields. Furthermore, beta values indicate female participants showing more empty fields than male participants. In sum, beyond the influence of the control variable sex, the independent variable intervention versus no intervention significantly influenced the average number of empty fields in the registration form ($M_{\text{intervention}} = 4.21$, $SD_{\text{intervention}} = 3.44$, $M_{\text{no_intervention}} = 3.41$, $SD_{\text{no_intervention}} = 3.35$). Corresponding values are summarized in Table 31. In sum, Hypothesis 1a can be accepted.

Table 31
Hierarchical analysis of regression including intervention vs. no intervention as independent variable, sex (-1 = male, 1 = female) as control variable and the number of empty fields as dependent variable (Study 4)

		Number of empty fields					
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2
Step 1							.030
	Sex	.61	.18	.17	3.40	.001	$F(1,378) = 11.56, p = .001$
Step 2							.010
	Sex	.61	.18	.17	3.42	.001	$F(2,377) = 7.82, p = .000$
	Intervention vs. no intervention	.81	.40	.10	2.00	.046	
Final							.040
R^2							

Note. Bold values indicate significant effects.

H1b predicted that disclosures of users who were exposed to privacy interventions were less sensitive (i.e. not related to the self) than disclosures of users who were not exposed to privacy interventions. A hierarchical analysis of regression was conducted

with the independent variable intervention versus no intervention and the dependent variable disclosure sensitivity, controlling for sex. Disclosures related to the self such as “I am a daddy of two children, am currently at home on parental leave and my partner is currently working” or “Hey :) My name is [name], 19 years old, and I am a law student in Jena. Originally I come from the Ruhr area in NRW, where I usually spend most of my time. I love to travel, do stuff, go out for a walk, films, and series... The usual stuff.” were identified as sensitive, whereas disclosures that were not related to the self, for example, “If you want to know something, ask” or “Hello, I am introducing myself here”, were identified as being not sensitive. However, there was no significant influence of the privacy interventions on sensitivity of disclosures (see Table 32), which is why *H1b* has to be rejected.

Table 32
Hierarchical analysis of regression including “intervention vs. no intervention as independent variable, sex (-1 = male, 1 = female) as control variable, and the sensitivity of disclosure (0 = no disclosure, 1 = disclosure not related to the self, 2 = disclosure related to the self) as dependent variable (Study 4)

		disclosure sensitivity					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.003	$F(1,378) = 1.22, p = .217$
	Sex	-.05	.05	-.06	-1.10	.217		
Step 2							.001	$F(2,377) = .80, p = .450$
	Sex	-.05	.05	-.06	-1.10	.270		
	Intervention vs. no intervention	-.07	.11	-.03	-.62	.534		
Final							.004	
	R^2							

H1c assumed users’ disclosures were less comprehensive (i.e. diversity of self-related information) if they were confronted with privacy interventions (traffic light, prompt, information) than if they were not confronted with a privacy intervention. To investigate the influence of the privacy interventions on the comprehensiveness of participants’ self-disclosures, a hierarchical analysis of regression was conducted with the independent variable intervention versus no intervention and the dependent variable disclosure comprehensiveness, again controlling for sex. The more different categories were addressed in self-disclosures, the more comprehensive the disclosure was considered to be. Categories of self-disclosures that were identified were related to personal characteristics, sexual orientation, hobbies, family, job, university, aims (with regard to the SNS), age, name, place of residence, and hometown. There were no

significant effects of the intervention on the comprehensiveness of the disclosures (see Table 33), which is why *H1b* is rejected. Descriptively, most people revealed information regarding the self in one to four categories (Figure 15).

Table 33

Hierarchical analysis of regression including intervention vs. no intervention as independent variable, sex (-1 = male, 1 = female) as control variable, and the comprehensiveness of disclosure as dependent variable (Study 4)

		disclosure comprehensiveness						
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>	ΔR^2	
Step 1	Sex	-.00	.09	-.00	-.02	.983	.000	$F(1,378) = .00, p = .983$
Step 2	Sex	-.00	.09	-.00	-.02	.982	.001	$F(2,377) = .16, p = .851$
	Intervention vs. no intervention	-.12	.21	-.03	-.60	.570		
Final	R^2						.001	

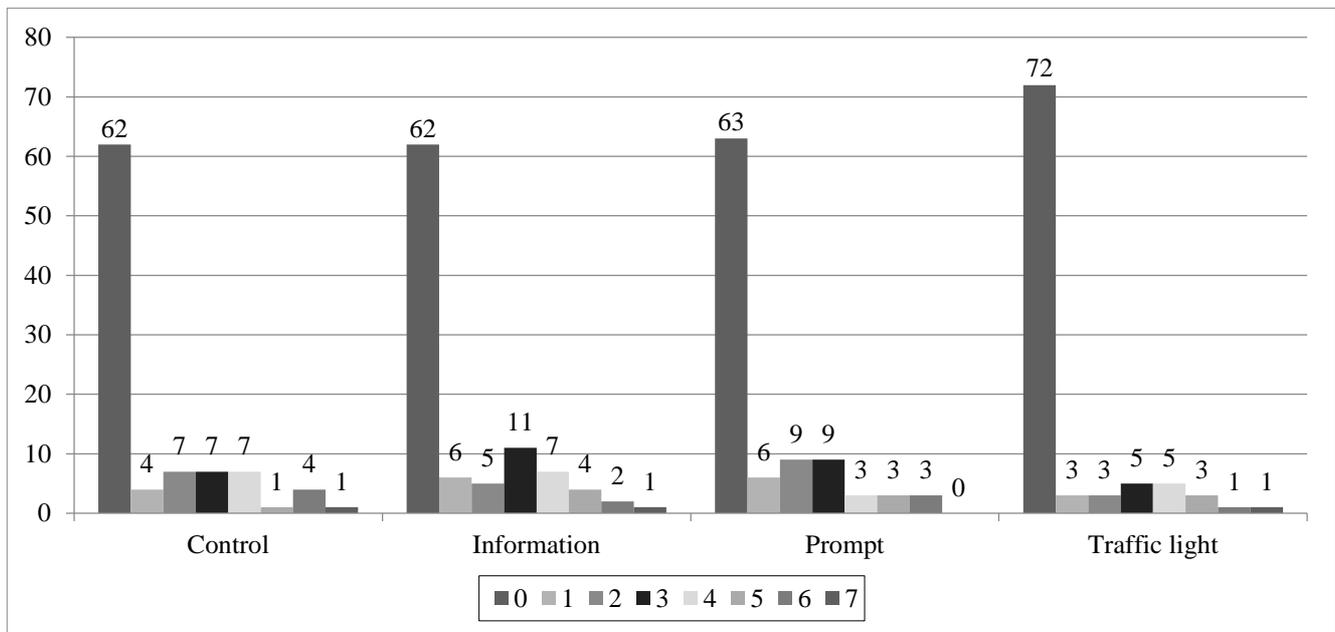


Figure 15: Number of disclosed self-disclosure categories (Study 4).

Research Question 1 (RQ1)

RQ1 asked which kind of privacy intervention (traffic light, prompt, information) would be the most effective for inducing privacy aware behavior (i.e. the number of empty fields). Therefore, a hierarchical analysis of regression with dummy-coded variables representing the experimental manipulations (no intervention vs. traffic lights,

no intervention vs. prompt, no intervention vs. information) was conducted. In the regression analysis, sex was considered as control variable and entered in the first block. In the second block, all dummy-coded variables were commonly entered. The first block controlling for sex explained about 3% of the variance in the number of empty fields, $R^2 = .030$, $F(1, 378) = 11.56$, $p < .01$. When including the dummy variables in the second step, the explained variance increased to 5%, $R^2 = .045$, $F(4, 375) = 4.41$, $p < .01$. Coefficients reveal that the dummy variable prompt had a significantly positive contribution to the explanation of variance in the number of empty fields ($\beta = .133$, $p < .05$). In addition, the dummy variable information explains the variance of empty fields marginally significantly ($\beta = .120$, $p = .054$). The traffic light did not contribute to explaining the variance in the dependent variable ($\beta = .051$, $p = .415$). For a summary over all values please refer to Table 34. In sum, the prompt intervention had the greatest impact on users' privacy behavior. Specifically, the prompt intervention resulted in a higher number of empty fields, indicating more cautious privacy behavior.

Table 34
Hierarchical multiple regression analysis including the dummy-coded privacy interventions as independent variable, sex (-1 = male, 1 = female) as control variable and the number of empty fields as dependent variable (Study 4)

		Number of empty fields					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.030	$F(1,380) = 11.37, p = .001$
	Sex	.61	.18	.17	3.40	.001		
Step 2							.015	$F(4,377) = 4.47, p = .002$
	Sex	.62	.18	.18	3.46	.001		
	No intervention vs. traffic light	.40	.50	.05	.82	.415		
	No intervention vs. prompt	1.05	.49	.13	2.15	.033		
	No intervention vs. info	.94	.49	.12	1.93	.054		
Final							.045	
	R^2							

Note. Bold values indicate significant effects.

Research Question 2 (RQ2)

RQ2 asked whether the experience with the SNS would be evaluated differently based on whether there was a privacy intervention or not and based on the different types of privacy interventions. Therefore, an analysis of variance with the experimental

condition as factor and the user experience as dependent variable (controlling for sex) was conducted. Analysis did not reveal significant but only marginally significant differences between the groups regarding users' evaluation of the experience with the website, $F(3, 372) = 2.45, p = .059$. However, the descriptive values demonstrate that the experience was evaluated in a fairly balanced way among all experimental conditions (see Table 35).

Table 35
Descriptive statistics regarding user experience for all experimental groups (Study 4)

Group	<i>n</i>	User experience <i>M (SD)</i>	Minimum	Maximum
Control	93	3.04 (.66)	1.00	4.57
Information	98	3.05 (.74)	1.57	5.00
Prompt	96	2.99 (.65)	1.29	4.57
Traffic light	93	2.83 (.66)	1.00	4.29

The third *RQ* asked whether users' positive and negative affect would be influenced by the exposure to privacy interventions. In order to address this question, two repeated measures ANOVAs with participants' positive and negative affect, were conducted. Participants were asked to indicate their current affect before and after the registration process for the SNS. Since it was aimed to find out whether the privacy interventions have an influence on the participants' mood, analyses were conducted with $n = 189$ participants (traffic light, prompt). Both analyses revealed significant results, indicating that participants' positive, $F(1, 188) = 18.49, p < .001, \eta_p^2 = .090$, as well as their negative affect, $F(1, 188) = 5.84, p < .05, \eta_p^2 = .030$, differed between measurement_{t1} and measurement_{t2}. Mean values for the positive affect significantly decreased from measurement_{t1} ($M = 2.64, SD = .66$) to measurement_{t2} ($M = 2.51, SD = .75$). The mean values for the negative affect significantly decreased from measurement_{t1} ($M = 1.46, SD = .62$) to measurement_{t2} ($M = 1.38, SD = .60$), too (see Figure 16). Results indicate that participants' positive as well as negative affect decreased after the interaction with the SNS.

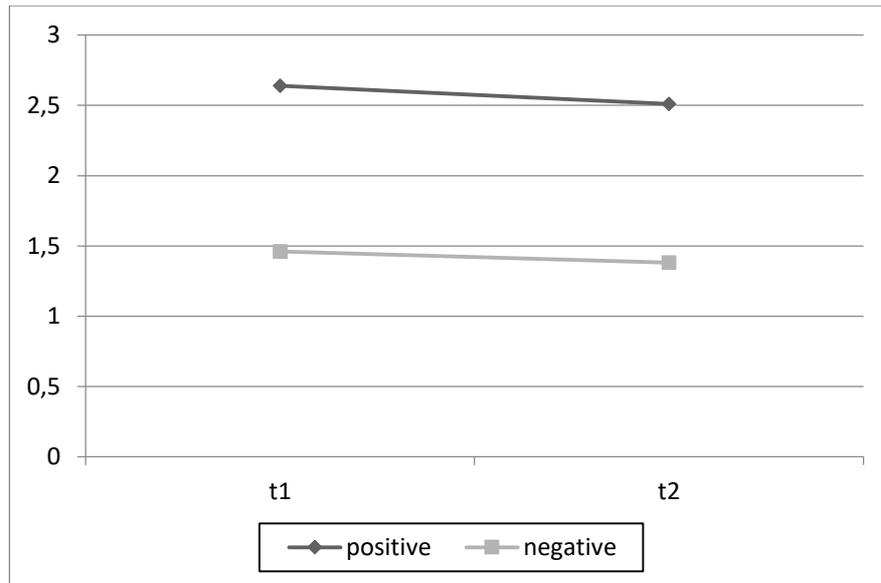


Figure 16: Participants' positive and negative emotional affect at measurement *t1* and *t2* (Study 4).

Hypothesis 2 (H2)

H2 predicted the impact of the privacy interventions on participants' privacy behavior to be moderated by the expression of those individual characteristics that generally have an influence on privacy behavior and privacy protection intentions (need for privacy, vulnerable narcissism, self-control). To test *H2*, several hierarchical regression analyses, one for each dummy-coded privacy intervention and each trait, were conducted. In each analysis, sex was considered as control variable in the first step, followed by dummy-coded variables representing the experimental condition (no intervention vs. traffic light, no intervention vs. prompt, no intervention vs. information) in the second step. In the third step, mean-centered traits (need for privacy, vulnerable narcissism, self-control) were entered, followed by each of the interaction terms (e.g., no intervention vs. traffic light \times vulnerable narcissism) in the fourth step of the hierarchical regression. The analysis revealed that the control variable sex had a significant influence on the disclosure behavior of participants in each model. Furthermore, examining the relation between the prompt intervention and participants' disclosure behavior dependent on their general self-control revealed a significant positive effect of participants' self-control on the number of empty fields in the third step ($\beta = .102, p < .05$). However, the assumed interaction effect between the prompt intervention and the users' expression of self-control was not found to be significant ($\beta = .009, p = .885$). Considering the impact

of the variable no intervention vs. information, a marginal effect of self-control on the number of empty fields was observed ($\beta = .094, p = .065$) but again, there was no interaction effect between the intervention and self-control ($\beta = .044, p = .454$). Furthermore, analyses regarding the variable no intervention versus information revealed a marginally significant interaction between the intervention and users' physical need for privacy ($\beta = -.111, p = .056$). In sum, *H2* has to be rejected.

Hypothesis 3 (H3)

H3 assumed privacy concerns to be a moderator in the relation between the privacy interventions and disclosure behavior that is, users' who are generally concerned about their privacy might be more prone to the privacy interventions than those who are less concerned. Again, several hierarchical analyses of regression were conducted for examining the assumed moderating effect of privacy concerns. Analyses were performed for all dummy-coded intervention variables and with each informational, social, and psychological privacy concerns. Again, the control variable sex had a significant influence on participants' disclosure behavior. However, analyses revealed that privacy concerns did not moderate the influence of a privacy intervention on participants' behavior. Consequently, *H3* has to be rejected.

Hypothesis 4 (H4)

In *H4* it was predicted that perceived privacy norms positively influence the impact of the privacy interventions on users' disclosure behavior. Hierarchical analyses of regression were conducted with each dummy-coded intervention and each type of social norm, controlling for sex. Again, the control variable sex had a significant influence on the observed number of empty fields. Examining the impact of the traffic light intervention revealed a significant main effect of societal norms on the number of empty fields in the third ($\beta = -.144, p < .05$) as well as in the fourth ($\beta = -.148, p < .05$) step. An interaction effect was not observed. Beta-values indicate a negative relation between perceived societal norms and the number of empty fields. Examining the influence of media norms on the relation between the traffic light intervention and the number of empty fields further revealed a significant negative main effect of media norms on privacy behavior in the third step of regression analysis ($\beta = -.109, p < .05$), whereas there was

no interaction effect in the final step of regression analysis. Analyses with the prompt intervention as independent variable revealed a significant main effect of societal norms in the third ($\beta = -.144, p < .01$) and fourth ($\beta = -.177, p < .01$) step. Here also, no interaction effect was found. Furthermore, a significant main effect for media norms in the third ($\beta = -.106, p < .05$) and fourth step ($\beta = -.124, p < .05$) was found when investigating the relations between the prompt intervention, media norms, and privacy behavior. Investigations regarding the last intervention, namely, the information provided in the welcoming text, and privacy norms demonstrated a significant main effect of societal norms in the third ($\beta = -.143, p < .01$) step as well as a marginally significant effect in the fourth step ($\beta = -.113, p = .053$). No interaction with media norms was observed. Moreover, there was a significant main effect of media norms in the third ($\beta = -.111, p < .05$) and fourth ($\beta = -.128, p < .05$) steps of the hierarchical regression analysis. However, again, no interaction was indicated by the data. In sum, perceived privacy norms indeed influence privacy behavior, although they do not moderate the impact of the persuasive privacy interventions. The relations between perceived privacy norms and privacy behavior were shown to be negative, indicating high norms are related to a lower number of empty fields (i.e. less secure privacy behavior). In sum, *H4* cannot be supported by the data. For an overview of all corresponding values please refer to Table 36, which summarizes the values of partial correlation analyses (corrected for sex) between the considered variables and all types of participants' privacy behavior.

Table 36

Partial correlations between the personal variables of participants and the dependent behavioral variables empty fields, sensitivity of self-disclosure, and number of disclosed categories of self-disclosure, controlled for sex (Study 4)

	Empty fields <i>N</i> = 380	Empty fields <i>n</i> = 93	Self- disclosure sensitivity <i>N</i> = 380	Self- disclosure sensitivity <i>n</i> = 93	Self-disclosure number of categories <i>N</i> = 380	Self-disclosure number of categories <i>n</i> = 93
Narcissism	-.066	-.080	.019	.030	.034	.031
Self-control	.098		-.003	-.025	-.018	-.034
Need for cognition	.075	.05	-.026	-.032	-.026	-.007
User experience	-.179***	-.128*	.093	.105	.065	.042
Perceived privacy control	-.035	-.068	-.016	.010	.026	.054
Privacy concerns	.037	.019	.006	.005	.020	-.005
Peer norms	-.026	-.032	-.079	-.019	-.038	-.010
Societal norms	-.145**	-.133*	-.054	-.014	-.016	.008
Media norms	-.111*	-.078	.020	.064	.037	.070
Awareness	.004	.018	.018	-.009	.028	.020
Need for privacy inf.	.005	-.005	-.112*	-.130*	-.097	-.131*
Need for privacy phy.	-.069	-.097	-.059	-.043	-.032	-.024
Need for privacy inter.	-.045	-.089	.017	.044	.038	.053
Concerns inf.	-.30	-.057	-.045	-.026	-.018	-.032
Concerns soc.	.081	.079	.016	-.002	.026	.001
Concerns psy.	0.65	.056	.024	.035	.038	.025
CBC: reward	-.048	-.053	.067	.076	.004	.005
CBC: severity	-.004	.006	.056	.034	.088	.067
CBC: likelihood	.051	.040	-.128*	-.108	-.110*	-.083

* $p \leq .05$, ** $p \leq .01$, *** $p \leq .001$, bold without asterix indicates marginal significant effect

Hypothesis 5 (H5)

In *H5* it was predicted that users base their decisions regarding disclosures more strongly on the anticipated severity of the consequences of publishing a posting than on the anticipated benefits or the likelihood that a consequence occurs. Therefore, a CBC analysis was conducted. Table 37 summarizes the average utility and importance values for all attributes in the decision task.

Table 37

Average utility and importances with standard deviations for every attribute and its corresponding levels of the CBC task for the full sample N = 380 (Study 4)

		Average Utility	SD	Average Importances	SD
Reward	Low	-27.05	20.12	20.21	10.42
	Moderate	3.61	13.69		
	High	23.44	17.14		
Severity	Low	82.56	25.67	54.01	13.51
	Moderate	-7.31	15.45		
	High	-75.24	26.72		
Likelihood	Low	37.53	18.00	25.78	9.31
	Moderate	0.07	10.54		
	High	-37.60	19.20		

For the decision to disclose, the severity of consequences was the most decisive attribute, followed by the likelihood that a consequence occurs. The lowest importance values were recognized for the anticipated rewards. Considering the level-values reveals interesting insights as well. For the attribute reward, the most relevant indicator for disclosure was *high reward*, followed by *moderate* and finally by *low*. The most important levels for the attributes severity and likelihood were *low*, followed each by *moderate* and finally by *high*. Thus, if the most relevant attribute for the decision to disclose a posting was reward, the participant most often chose the posting related to high rewards for publishing. If the most important attribute was severity or likelihood, the most decisive level was *low*, indicating that the postings most likely to be disclosed are those that implicate the lowest severity and likelihood regarding the occurrence of negative consequences. This pattern was observed in all experimental groups.

H5 suggested that users base their decisions regarding disclosures most strongly on the anticipated severity of negative consequences of publishing a posting and less on the anticipated benefits or the likelihood that a consequence occurs. This assumption was tested via a CBC analysis. As explained earlier, users were asked to indicate which of three different postings they would most likely publish, depending on three different attributes (rewards, severity of consequences, and likelihood of consequences), each specified by three levels (low, moderate, high). A repeated-measures ANOVA was calculated to assess whether one attribute was more important for making the decision to publish the posting than the others. The repeated-measures design was chosen because every user decided several times between the options. Furthermore, the manifestations of

the dependent variable, namely, the relative importance values of the attributes, are not independent of each other since every decision for one attribute is a decision against the two other attributes at the same time. In sum, the relative importance values of the three attributes reveal 100%. Therefore, the results need to be considered carefully. Given that the Mauchly test revealed a violation of sphericity, and the Greenhouse–Geisser ϵ was greater than .75 ($\epsilon = .892$), the Huynh–Feldt correction was considered to correct for violations (see Field, 2009; Girden, 1992). Results with Huynh–Feldt correction showed that the mean values of the three factors reward, severity, and likelihood are significantly different from each other, $F(1.80, 678.74) = 721.93, p < .001$. Huynh–Feldt-adjusted post hoc analysis revealed a significant difference in the mean values between the factor rewards and severity of consequences ($-34.35, 95\% \text{ CI } [-36.84, -31.87], p < .001$), severity of consequences and likelihood of occurrence ($27.78, 95\% \text{ CI } [25.27, 30.30], p < .001$), as well as rewards and likelihood of occurrence ($-6.57, 95\% \text{ CI } [-8.43, -4.71], p < .001$). Analyses indicate that attributes referring to the severity of consequences were more relevant for participants' decisions to publish a posting than those referring to anticipated rewards (see Figure 17). Descriptive values further indicate that the decision-makings were balanced among the experimental conditions. Descriptive values further indicate that the decision-makings were balanced among the experimental conditions (see Figure 17) Analyses of regression, considering the experimental conditions as independent and each attribute of the CBC analysis as dependent variable supported the descriptive observations in terms of revealing no significant predicting effects.

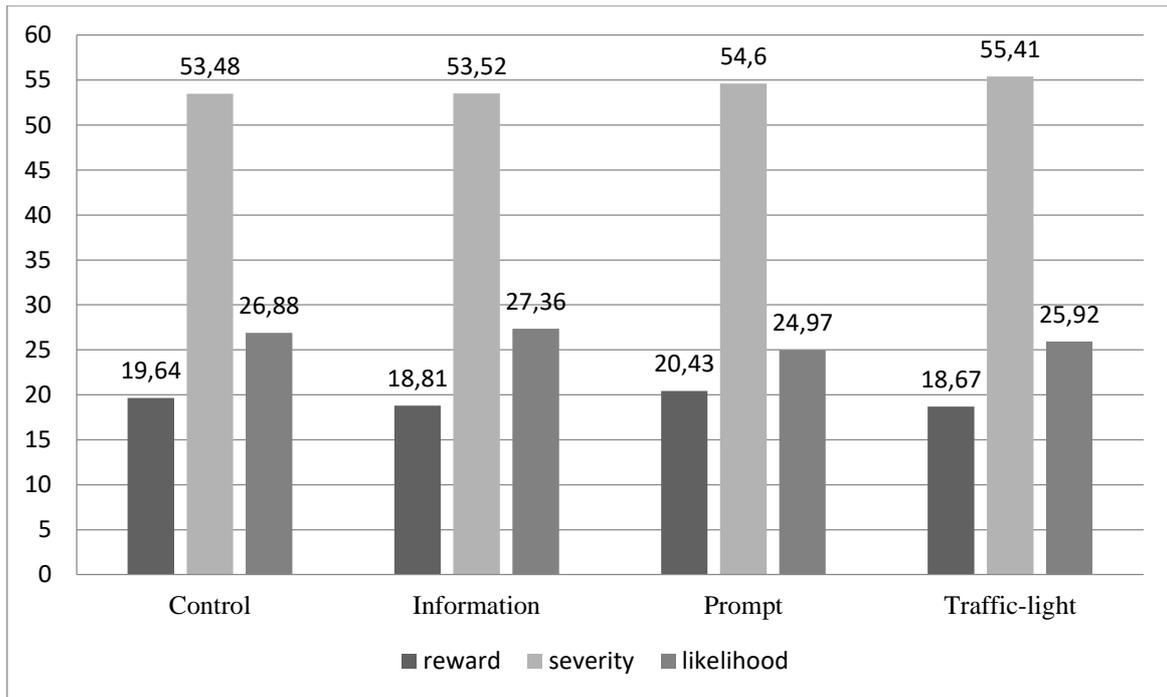


Figure 17: Relative importance values of CBC decisions (Study 4).

Hypothesis 6 (H6)

In *H6* it was hypothesized that participants' need for cognition influences their choices in the CBC task. That is, users' need for cognition was assumed to have a positive influence on the relative importance of risk-related attributes (severity and likelihood of consequence) and to have a negative influence on the relative importance of anticipated rewards when making the decision to disclose or not disclose a posting related to the mentioned attributes. Therefore, three analyses of regression with need for cognition as independent variable and the attributes rewards, severity of consequences, or likelihood of consequences as dependent variables were conducted. In all regressions, sex was considered as control variable in the first step. Analyses revealed a significant positive influence of need for cognition on the assessed importance of the severity of potential consequences, $R^2 = .023$, $F(2, 377) = 4.41$, $p < .05$, $\beta = .130$. There was no significant effect for the control variable sex. Furthermore, analyses revealed a significant negative influence of need for cognition on the dependent variable rewards, $R^2 = .040$, $F(2, 377) = 7.95$, $p < .01$, $\beta = -.165$. A significant main effect for the control variable sex was observed, indicating that male participants more often chose the attribute rewards as being most relevant. The third analysis of regression with the likelihood that negative

consequences might occur as a dependent variable revealed no significant influence of users' need for cognition on the decision in the CBC task. In sum, *H6* can be supported by the data. All corresponding values are summarized in Table 38 and Table 39.

Table 38
Hierarchical analysis of regression including need for cognition as predictor, sex (-1 = male, 1 = female) as control variable, and CBC severity of consequences as dependent variable (Study 4)

		Decision for severity of consequences					ΔR^2	
		<i>b</i>	<i>SE</i>	β	<i>t</i>	<i>P</i>		
Step 1							.006	$F(1, 378) = 2.26, p = .134$
	Sex	.97	.65	.08	1.50	.134		
Step 2							.017	$F(2,377) = 4.41, p = .013$
	Sex	.94	.64	.08	1.47	.143		
	Need for cognition	1.63	.64	.13	2.56	.011		
Final							.023	
R^2								

Note. Bold values indicate significant effects.

Table 39
Hierarchical analysis of regression including need for cognition as predictor, sex (-1 = male, 1 = female) as control variable (Study 4)

		Decision for reward					ΔR^2	
		<i>B</i>	<i>SE</i>	β	<i>t</i>	<i>p</i>		
Step 1							.013	$F(1,378) = 5.04, p = .025$
	Sex	-1.12	.50	-.12	-2.25	.025		
Step 2							.027	$F(2,377) = 7.95, p = .000$
	Sex	-1.09	.49	-.11	-2.22	.027		
	Need for cognition	-1.60	.49	-.17	-3.27	.001		
Final							.040	
R^2								

Note. Bold values indicate significant effects.

13.8 Discussion

The aim of the current study was to investigate the impact of different privacy interventions on users' disclosure behavior, the moderating roles of users' personal characteristics, and to expand the privacy calculus by providing insights into the black box of users' risk-benefit evaluation. In contrast to many other investigations, this study assessed participants' actual behavior through an experimental online study in which users interacted with a registration page of an SNS, and concrete decision-making processes by means of a choice-based-conjoint analysis allowing relevant (privacy-) decision factors to be made more tangible.

Analyses regarding *H1* demonstrate that privacy interventions that are presented during a registration process for an SNS, are related to a lower amount of information disclosure by users. In the present study, this was represented through users having more empty fields in the end of the registration process if they saw a privacy intervention during the registration process. In line with Study 3 and findings by Acquisti and colleagues (2017), and Wang and colleagues (2013) who suggested privacy prompts are effective in increasing users' privacy behavior, the privacy intervention called for users' attention to privacy issues resulting in a more cautious behavior. With a view to application, the result implies that privacy interventions indicating the current level of privacy threat seem to be an adequate method to support users in converting an unaware state of information disclosure in an aware and more cautious state. With reference to processes of evaluating information in behavioral decision-making this means that an ambiguous risk situation, namely, a situation in which potential negative outcomes are unknown, was changed to a situation under approximately objective risk-conditions (see Schiebener & Brand, 2015) in which the user is informed about negative consequences that might happen as a result of sensitive information disclosure. By raising users' awareness via privacy interventions as they were presented in the current study, users still have the freedom to decide on their own whether to act in accordance with the suggestion or to continue disclosure as before. In doing this, users would not be deprived of their autonomy which is highly important in the realm of persuasive support measures (Fogg, 2009), and especially relevant in the case of privacy protection in which autonomy plays a decisive role for users' well-being (Westin, 1967).

By contrast, analyses regarding *H1b* and *H1c* did not show significant effects. The sensitivity and diversity of self-formulated texts introducing the self to other users were not influenced by the presence of a privacy intervention. Results indicate that self-disclosure on SNSs is a complex process comprising different factors that are decisive for disclosing or not disclosing personal information. Privacy interventions seem to be more helpful for reducing the amount of personal information being disclosed (*H1a*) than for reducing the level of sensitivity within particular disclosures. It seems that once the decision to reveal personal information has been made, the sensitivity of the provided content is no longer influenced by privacy interventions. The decision of what to disclose in particular seems to be more complex and dependent on other individual factors than

the amount of provided information in a registration form. Here, further research is needed in order to uncover the underlying processes and to provide adequate protective measures.

Analyses revealed that the prompt intervention was the most effective in terms of resulting in a high number of empty fields (*RQ1*). The prompt informed about potential negative outcomes of self-disclosure in a consensual style (which was found to be effective in a prior study investigating the effect of different persuasive styles of communication, see also Study 3). Utz and Krämer (2009) also suggested privacy protection recommendations to be especially influential if they are transmitted from a peer instead of an authority person, which shows a relation to the results of the current and the prior study, namely, that persuasive privacy interventions in a consensual style of communication were related to a low extent of disclosed information. Surprisingly, the traffic light intervention did not contribute to the explanation of variance in the number of empty fields. It was assumed that a traffic light indicating the severity of the current privacy situation might be effective due to the simplicity and familiarity of this symbol, which is also used to inform about information in other realms such as nutrition information. However, in line with prior findings (Schäwel, 2017), this might indicate that users wish for some information explaining the communicated level of a privacy threat. The traffic light, in contrast to the prompt intervention, did not provide written information but solely indicated the risk level by changing the color depending on the amount of information provided. The prompt, by contrast, provided information and changed the color adapted to the colors of a traffic light on top (green indicating no risk, orange indicating medium risk, and red indicating high risk).

The second *RQ* explored, whether the experience with the SNS was evaluated differently based on the presence of privacy interventions. Results do not indicate a significant effect of the presence of privacy interventions on the experience users had with the network. Participants evaluated the experience with the social network in a quite balanced way as being medium among all experimental conditions. With a view to application, this result is to be regarded as positive because it indicates that interventions, as presented in the current study, do not negatively affect users' joy of use.

The results regarding the third *RQ*, exploring the impact of the provided interventions on users' positive and negative affect, were quite striking. It was shown that

users' positive affect was significantly more pronounced before the interaction with the network than after the interaction. However, users' negative affect also decreased from measurement_{t1} to measurement_{t2}, indicating that users felt less positive after interacting with the SNS but also less negative at the same time. It might be the case that users became languid in the course of the study so that their emotional affect in general was less intense at measurement_{t2}. Future studies might consider items that are related more directly to the privacy interventions instead of asking for general mood.

In *H2* it was assumed that the impact of privacy interventions would be moderated through users' personality traits, namely, the need for privacy (see Dienlin, 2017), vulnerable narcissism (see Ahn, Kwolek & Bowman, 2015) and self-control (see Taddei & Contena, 2013). Analyses did not reveal significant interaction effects. Thus, beyond the influence of sex (which had a significant influence on disclosure behavior independently from the privacy intervention, with females disclosing less than males; see also Special & Li-Barber, 2012; Saeri, Ogilvie, Macchia, Smith, & Louis, 2014) and the intervention itself, personality seems to have no additional influence on the impact of a privacy intervention on actual behavior. There might be further situational cues influencing the effectiveness of the intervention that might be more decisive than users' stable traits. The examined traits might have an influence on the intention to engage in privacy protection in general but not on the impact of situational interventions on actual behavior (see also *H3*). However, the data revealed a significant positive main effect of users' self-control on the number of empty fields. This indicated that people with general high self-control might also show more cautious privacy behavior. As was discussed earlier, pronounced self-control can help people to resist temptations (Ent, Baumeister, & Tice, 2015) and users with low self-control are more likely to become a victim of Internet scam (Chen, Beaudoin, & Hong, 2017). Applied to our data this indicates that users with pronounced self-control were able to resist the temptation to disclose personal information that would usually be related to positive outcomes such as presenting the self in a positive light and getting positive feedback from other users, or allowing other people to contact oneself based on similar characteristics or attitudes (see Christofides et al., 2009; Taddicken, 2011). Furthermore, people who are generally able to control themselves seem to also be able to control their disclosures on an SNS. In line with the theory of planned behavior (Ajzen, 1991), the results demonstrate that perceived self-

control is highly relevant for actual behavior. Increasing users' perceived self-control seems to be a promising factor for increasing privacy-aware behavior.

H3 assumed users' privacy concerns were a further moderator in the relation between the privacy intervention and actual disclosure behavior. Again, no interaction was revealed by the data. Based on research reporting on the influencing role of privacy concerns on privacy behavior (e.g., Li, Luo, Zhang, & Xu, 2017, Xu et al., 2008), the idea behind this assumption was that users who are highly concerned might also be more sensitive toward privacy interventions and follow the privacy recommendation given. However, this was not the case. As reported earlier, privacy concerns are not the only indicator of privacy protection behavior, but they induce information withdrawal if anticipated benefits are not as salient as anticipated negative outcomes (Dienlin & Metzger, 2016). It is conceivable that concerns did not have a significant effect on the impact of privacy intervention because the perceived situational benefits might have been more pronounced for users. This seems to contradict the findings of the CBC analysis, which indicates that users weigh the anticipated severity and likelihood of the occurrence of privacy threats more strongly than they do with anticipated benefits (*H5*). However, the findings from *H3* relate to situational and immediate concealing behavior, whereas the decisions in the CBC task were based on (several rounds of) explicit evaluations of risks and benefits under objective conditions for decision-making (see Schiebener & Brand, 2015). An objective condition in this case means having concrete indicators for the occurrences of benefits, negative consequences, and their severity. Users were able to think about a situation in which they would disclose or not disclose a specific posting by being aware of the negative as well as the positive consequences of their action at the same time. Moreover, risks and benefits were explicitly visualized through icons indicating each level of risks and benefits (see Figure 12). In this case, the perceived severity outweighs the anticipation of risks (see *H5*). These results underline the assumption that situational disclosure and concealing behavior differ from long-term and more cautious privacy behavior (see Masur, 2018). It needs to be considered that in the discussion regarding *H1* it was also argued that the privacy interventions can change an ambiguous privacy decision situation into a more objective one, which might be one reason for the interventions being effective. Nevertheless, when comparing the existence of a privacy intervention (which can transform a completely unaware privacy situation in

a more objective one) with the even more comprehensive and concrete privacy indicators in the CBC task, it reveals that these concrete indices can increase the persuasive effect even more. With regard to practical implications, this means that persuasive privacy interventions can be further enhanced by additionally providing visual cues for the anticipated benefits *and* the potential risks. This might facilitate the privacy calculating process (see Culnan & Armstrong, 1999) and allow for more objective risk–benefit evaluations.

The last hypothesis referring to the SNS (*H4*) stating that perceived privacy norms (distinguished into peer, societal and media norms) have a positive influence on the effectiveness of privacy interventions (based on Park & Smith, 2007, and Utz & Krämer, 2009) did not show significant interaction effects. However, significant main effects of perceived norms on actual privacy behavior were found. Strikingly, and against our hypotheses, the relations revealed to be negative, indicating that high perceived privacy norms lead to more disclosure behavior. That is, analyses regarding the impact of the traffic light intervention on the disclosure behavior revealed a significant negative main effect of societal norms on the number of empty fields. This contradicts the assumptions because users perceiving that society suggests caring about privacy actually seem to care less about their online privacy (because they had fewer empty fields). Furthermore, perceived media norms were negatively related to the number of empty fields as well, indicating that people who think the media is reporting about privacy protection have fewer empty fields. This might be based on the measurement of privacy behavior, which was not a self-report but real behavioral data. It might be the case that in self-reports, users would have indicated caring more about their privacy the more pronounced they perceive the social norms regarding privacy to be. It might be also conceivable that users want to defy perceived norms and behave in contrast to transmitted norms. However, this result needs to be considered carefully because perceived norms have been shown to be related to actual behavior (e.g. restricting access to one's profile on an SNS) in several studies (e.g., Utz & Krämer, 2009). Nevertheless, restricting the profile relates to social privacy behavior (see Burgoon, 1982), whereas disclosing or not disclosing information during a registration process for an SNS (e.g., name, interests, personal characteristics) instead refers to the informational and psychological dimensions of privacy (see Burgoon, 1982). It might be the case, that perceived social norms do not influence privacy behavior

with regard to all dimensions of privacy but potentially only to a specific part of privacy behavior. This result once again supports the complexity and multidimensionality of human privacy (see Westin, 1967; Burgoon, 1982; Petronio, 2002).

In line with Krasnova, Spiekermann, Koroleva, and Hildebrand (2010) and Krasnova, Kolesnikova and Guenther (2009), results of the current study indicate that for the decision to self-disclose, the anticipation of a negative consequence is of high relevance (*H5*). Although research indicated that rewards in terms of social support can foster information disclosure and lower users' inhibitions, or overwrite privacy concerns, concretely communicated risks seem to be even more relevant for users' decisions to disclose information. In the current study, a CBC scenario was used to examine users' privacy decision-making. Three different attributes, referring to either positive (i.e. rewards) or negative (i.e. likelihood and severity of consequences) outcomes of sensitive information disclosure, each varying depending on characteristics of the attributes (from low to highly rewarding / likely / severe) were investigated concerning their relative importance in a privacy decision. The advantage of this method is that it is possible to derive people's most likely behavior based on their decisions with regard to specific choice options by overcoming the problem of biased responses when relying on explicit self-reports. The attributes within the CBC analysis mirror the early assumptions of the protection motivation theory (Rogers, 1975) in the sense that the most important factors for processing a given threat are the severity, the vulnerability (here, likelihood that the threat is actually occurring) and anticipated rewards of the action of interest (here, sensitive self-disclosure). Following the protection motivation theory, the interaction of these three variables can validly predict a person's motivation to engage in protective behavior. In the current study, the threat appraisal and consequently one element of the protection motivation theory was indicated through the intention to disclose a posting, associated to positive and negative consequences, or not. More precisely, participants chose (several times in a row) one posting (out of three) which they would most likely publish, depending on varying levels of rewards related to disclosure, as well as severity, and likelihood related to negative consequences of disclosure. Thereby, the current study extends the assumption of the protection motivation theory, which states that severity, vulnerability, and rewards are decisive factors for the threat appraisal (i.e. the evaluation of maladaptive response) in terms of demonstrating the relative importance of the

mentioned variables. More precisely, for the intention to disclose a sensitive posting or not (i.e. protection motivation in this case), the most decisive factor was the severity of anticipated negative consequences, whereas anticipated rewards were least important for participants in this study.

With a view to application, this work provides valuable insights. Providers of privacy interventions and support measures should focus on communicating possible consequences of self-disclosure to users of SNSs (referring to results regarding *H3*, even negative and positive consequences in combination so that an objective and reasoned decision can be taken by the users). If anticipated risks become perceptible by being clearly and visually transmitted, users strongly refer to them and intend not to disclose sensitive content referring to the self (here, a posting related to one's own job). The likelihood that a consequence would generally occur was the second important variable after the severity. The least important variable was the anticipated rewards, indicating interesting implications for risk communication in terms of privacy support. Since users assess the severity of a consequence and the likelihood that a consequence occurs as more relevant than potential rewards, privacy interventions should focus on communicating explicit risk information if a very severe threat is posed, potentially in combination with concrete examples of severe privacy invasions. This is also in line with the protection motivation theory (Rogers, 1983) stating that fear appraisals are effective in inducing protection motivation and implementing protective behavior. Furthermore, results by Wang and colleagues (2011, 2013) also indicate that negative online experiences resulting in regrets might shape future behavior.

As hypothesized (referring to Kehr, Kowatsch, Wentzel, & Fleisch, 2015), users' need for cognition positively predicted the relative importance of considering the severity of the consequences of publishing a posting, whereas it negatively influenced the consideration of anticipated rewards (*H6*). This indicates that users with a high need for cognition seem to evaluate possible risks of their behavior in a more reasoned way (through the reflective route, conceivably driven by the prefrontal cortex; Bechara, 2005; Schiebener & Brand, 2015) than users with a low need for cognition who seem to be more influenced by the benefits of information disclosure (through the impulsive route; Bechara, 2005; Schiebener & Brand, 2015). Users with a high need for cognition tend to think and elaborate more carefully and consider different outcomes of particular

situations more cautiously. In contrast to effortful elaborations of potential privacy risks, anticipated rewards might be considered less objectively and instead driven by emotions which is not typical for users with a high need for cognition (Cacioppo & Petty, 1982, Schiebener & Brand, 2015). Since the attributes for decisions in this study depended on each other, the reported results need to be considered carefully. In particular, the relative importance values of all three attributes reveal a value of 100 altogether. Therefore, the result depends on the given attributes. Nevertheless, attributes were chosen based on prior research on the privacy calculus and decision-making under different conditions revealing that negative consequences on the one hand and positive consequence on the other hand influence decisions. Future research might differentiate between anticipated rewards of information disclosure more carefully, for instance, with regard to rewards in terms of online feedback in contrast to positive feedback in the offline world or concerning feedback in terms of likes versus feedback in terms of appreciating written comments. However, since it was shown that communicated risks of information disclosure influence users' behavioral intention more strongly than rewards – even independently of users' need for cognition – privacy risk-related communication should be focused on fostering users' online privacy in a situation of concrete threat. When solely aiming at informing about the situational privacy state, a balanced presentation of potential negative and positive consequences might be more reasonable (see *H3*).

13.9 Limitations

Besides the valuable insights of this study, some limitations were revealed as well. In order to not prime participants, the functions of the privacy interventions were not explicitly addressed. However, explanations (e.g., green means *low privacy risk*) might have been helpful for users to understand the intention of the interventions. Future studies should provide legends and examples for the visual privacy interventions as it was also done for the icons within the CBC task. Results with regard to participants' current affect need to be considered carefully, depending on the wealth of questions they responded to, it cannot be guaranteed, that the affect by users is contributable to the persuasive privacy intervention only. Moreover, most reported effects were small. There seem to be further factors contributing to actual behavior, which should be reflected on in future research. Furthermore, the fact that there were no moderating effects of users' personal traits might

be attributable to the short-term interaction with the SNS. The influence of personal traits might be more relevant for behavioral changes in long-term privacy behavior. For learning about moderating effects of personality traits on the impact of privacy interventions on privacy behavior, long-term studies might be more appropriate.

13.10 Conclusion

By means of an experimental online investigation, the current study examined the impact of three different privacy interventions on subsequent actual privacy. This study demonstrated that the presence of a privacy intervention can help to shape users' privacy behavior on a registration page of an SNS. The most effective intervention was a persuasive privacy prompt in a consensual style of communication, indicating the importance of online privacy protection. Furthermore, sex was identified as a relevant variable for privacy behavior. In line with prior research, female participants showed more pronounced privacy behavior than male participants. Participants' self-control positively influences their privacy behavior, although it does not moderate the effect of a privacy intervention on the amount of disclosed information. Following the results of a CBC analysis, the severity of negative consequences related to self-disclosure is most relevant in the weighing process concerning disclosure or withdrawal of information. Furthermore, the need for cognition plays a major role in privacy decision-making. With the results gathered by behavioral data and actual decision-making, current findings regarding online privacy protection were expanded. Moreover, relative importance values concerning anticipated risks and benefits of information disclosure reveal insights into the black box of users' evaluation of positive and negative consequences of disclosing or concealing self-related information in the privacy calculus. Theoretically, this work stresses the complexity of privacy and disclosure behavior and indicates that more research should be done on the differences between planned and situational privacy behavior as well as regarding different types of self-disclosure (i.e. revealing information to input fields of a registration form or providing individually formulated self-reports). Practically, this work indicates that communicating concrete risks, especially with regard to their severity, seems to be the most promising kind of privacy intervention if a real threat is posed. If the user would rather generally be informed regarding the current

privacy state, the presentation of possible risks and benefits might be the most feasible solution.

In sum, valuable insights into the realm of privacy research in terms of increasing knowledge concerning actual privacy behavior and privacy decision-making have been provided.

VI GENERAL DISCUSSION

This chapter summarizes and discusses the main findings of the present dissertation. The contribution to the field of online privacy protection is outlined from an interdisciplinary point of view and limitations of prior research as well as arising research demands from current investigations are discussed. Furthermore, theoretical implications with an outlook to future research as well as practical implications with respect to application are provided. Given that online privacy protection is a highly sensitive topic, ethical implications and potential hazards of misusing the derived knowledge from the presented studies are addressed as well. This dissertation concludes with outlining the relevance of research on online privacy for further advances in raising users' awareness of online privacy protection.

From a psychological perspective, the studies in this work addressed the subject of privacy behavior by analyzing users' individual reflection upon privacy on the one hand, and their self-reported attitudes and behavioral intentions toward the usage of privacy protection measures on the other hand; accordingly, users' requirements toward a system-based privacy protection were explored in Study 1. Secondly, a quantitative examination assessed users' behavioral intention to use an opting-out measure (super-logoff) in Study 2. Additionally, actual privacy behavior after being exposed to a privacy intervention were investigated in Study 3 and Study 4. Concrete processes of privacy decision-making were considered in Study 4. From a software engineering's perspective, privacy protection has been considered as a system-based process, going through different stages of monitoring users' behavior, analyzing the extent of information sensitivity, planning whether and which feedback to provide, and finally providing feedback to the user in terms of a warning regarding sensitive self-disclosure (Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016).

14 Synopsis of the Underlying Research Model and Empirical

Results

The aim of this dissertation was to examine the field of online privacy protection systematically and to reflect on methods for privacy support of SNS users from an interdisciplinary point of view. More precisely, it was aimed to investigate the relations

between psychological user-centered variables and the effectiveness of system-based privacy support measures.

The practical implication of this work is the identification of specific types of privacy support that might be most effective for assisting users in reducing situational sensitive self-disclosure, and consequently, diminishing the likelihood of the occurrence of privacy harms. In addition to that, considerations regarding the application of this knowledge in real life is outlined. In order to provide feasible implications, these aims were addressed from both, a psychological and a software engineering's perspective. These perspectives were considered to integrate users' behavioral and psychological needs with technical requirements towards a potential system-based supportive measure for maintaining online privacy.

The theoretical implication of this work is firstly given through a theoretical model (see Figure 19), which summarizes the relevant factors involved in users' actual online privacy behavior and their intention and motivation to rely on system-based privacy support measures. This was done by combining the key elements of the theory of planned behavior (Ajzen, 1991), the protection motivation theory (Rogers, 1975) and the privacy calculus (Culnan & Armstrong, 1999). Secondly, this work particularly contributes to the theoretical framework of the privacy calculus (Culnan & Armstrong, 1999) in terms of giving insights to the black box of decision-making processes regarding disclosing or withdrawing sensitive information under the consideration of anticipated rewards and negative consequences. Thirdly, this work provides an understanding of balancing a system's usability and its users' privacy needs (see Chapter 8).

15 Summary of the Main Findings

Besides analyzing solely self-reported behavior, the studies of this dissertation also examined actual privacy behavior of social media users (i.e. withdrawal and modification of information, and opting-out). Additionally, and in contrast to many prior approaches which often mainly cover the informational dimension of privacy, the current thesis considers aspects beyond data security (i.e. informational privacy) by examining the social and psychological dimensions of privacy as well (see Burgoon, 1982; Chapter 2.1). From a methodological perspective, this was done by investigating disclosed information relating to different dimensions of privacy (see Studies 3 and 4). From a

theoretical perspective, this was done by reflecting on the value of privacy for the individual and its pivotal functions and facets (see Chapter 2.1).

The first study qualitatively addressed users' needs for privacy support measures and allows for deriving *transparency*, *autonomy*, *fit* (to the situation and the user), and *usability* (low effort, pleasant usage) as pivotal characteristics of a system-based privacy support measure. Furthermore, a recurrent theme during conducted interviews was the concern that a system-based support measure needs to monitor and analyze users' online activities very accurately in order to provide adapted feedback (i.e. one of the desired characteristics of the support measure). This contradiction between the desire for protection and the skepticism toward monitoring and analyzing activities of the support measure is referred to as *protection paradox* in this work. As can be seen in Figure 20, representing a synthesis of behavioral theories that underlie the current work, the *protection paradox* pertains to the technical part that would be necessary in order to provide desired protection functions.

Study 2 analyzed motives for opting-out from a social network (SLO; see Chapter 7.2) by considering users' privacy concerns, literacy, attitudes, intentions, and impression management motivation. Analyses yield *protection against personal attacks*, *avoidance of distraction*, and *avoidance of pressure* as main motives for opting-out. *Avoidance of distraction* and *protection against personal attacks* were shown to be the strongest predictors for users' intention to actually opt-out from the network Facebook in the future. Users' amount of self-disclosure was positively related to the intention to opt-out from Facebook. Further, this relation was mediated by situational impression management motivation, indicating the influence of general self-disclosure activity on the intention to opt-out can fully be explained by situational impression management behavior. Users' privacy attitudes and intentions were both positive predictors for the intention to opt-out from the network, whereby privacy literacy was not related to the intention to opt-out. Under consideration of the theory of planned behavior (Ajzen, 1991), the positive impact of the privacy attitudes and privacy intentions on the intention to use a privacy protection strategy (here, the super-logoff) can be explained by the predictable power of attitudes and intentions on according behavioral intention. However, data do not allow for conclusions regarding actual behavior since findings base on users' self-reports regarding behavioral intentions.

Most relevant findings with a view to practical implication arise from Study 3 and Study 4. These studies demonstrate that system-based support measures, derived from the previous qualitative investigation on users' needs and expectations towards privacy support measures (Study 1) and prior research on persuasion (see Chapter 8.5) can influence users' privacy behavior in the sense that they reveal fewer information to a SNS. Furthermore, Studies 3 and 4 support prior findings suggesting that specific personality traits and individual motivations of the users have an influence on their online privacy behavior and their privacy protection intention (see Chapter 6). To be more precise, users' vulnerable narcissism, need for privacy, need for popularity (Studies 3 and 4), need for cognition, and self-control (Study 4) were revealed to influence participants' actual privacy behavior within experimental investigations. Interestingly, the influences of personality traits revealed different directions depending on the operationalization of privacy behavior which was either the extent of undisclosed information (i.e. the number of empty fields in the registration form in Studies 3 and 4), or the amount of modifications of disclosures (i.e. the number of changes after being prompted in Study 3; see Figure 7). In contrast to stated hypotheses, users' characteristics did not significantly strengthen or weaken the persuasive effect of situational privacy interventions on participants' behavior (see Studies 3 and 4). However, these results are no evidence that there is no impact of personal characteristics on the effectiveness of privacy support measures, and, accordingly, no need for specific interventions for specific groups of users. Theoretical considerations still allow for assuming that particular privacy-related characteristics can shape the impact of privacy support measures (see also Egelman & Peer, 2015). It remained open to question whether this impact would have occurred in long-term investigations in which personality traits would have had a stronger influence on more stable long-term behavior. Conceivably, the single interaction with a social network and persuasive privacy prompts in each, Study 3 and Study 4, might be more influenced by situational cues (see also Masur, 2018) than by stable personality traits.

In Study 4, investigations regarding users' weighing processes of risks and benefits concerning online self-disclosure were addressed via a CBC scenario in which users took decisions to publish one of three postings related to different outcomes. From data it is apparent that the most relevant attribute for the decision to publish a posting was the *severity* of a potential consequence of disclosing, indicating that concrete risk-

communication (in line with the protection motivation theory by Rogers, 1975) can contribute to raise users' privacy awareness.

Taken together, this dissertation provides findings regarding users' individual attributes (*intrapersonal* factors), characteristics of user-centered and system-based privacy support measures (*environmental* factors), and the impact of users' as well as a system's characteristics on protection motivation and actual online privacy behavior (*appraisal* and *coping*, see PMT, Chapter 5.4). These factors will be addressed in the following two chapters (14.3.1 *Intrapersonal factors* and 14.3.2 *environmental factors*). Related behavior (appraisal and coping) is addressed continuously within both sections. The factors will be evaluated under the consideration of each study in which the variables of interest were examined. The overarching research question underlying all studies asked for methods that help raising users' awareness of online privacy protection. By stating this, it was not solely referred to general awareness (which revealed to be present for most users) but rather situational awareness of according privacy threats and potential intervening actions in a state of high risks (which revealed to be not present for most users).

16 The Influence of Intrapersonal and Environmental Factors on Users' Online Privacy Behavior

In the following, the results from four empirical studies will be discussed on the basis of the main elements of the research model presented in Chapter 9 (Figure 2), which summarized the hypothesized relationships between the investigated variables, revealing relations among intrapersonal and environmental factors. The main assumption of this work, that a persuasive privacy intervention can influence users' actual privacy behavior, was supported by data. The assumed moderating effects were not supported. Particular findings will be discussed in the following.

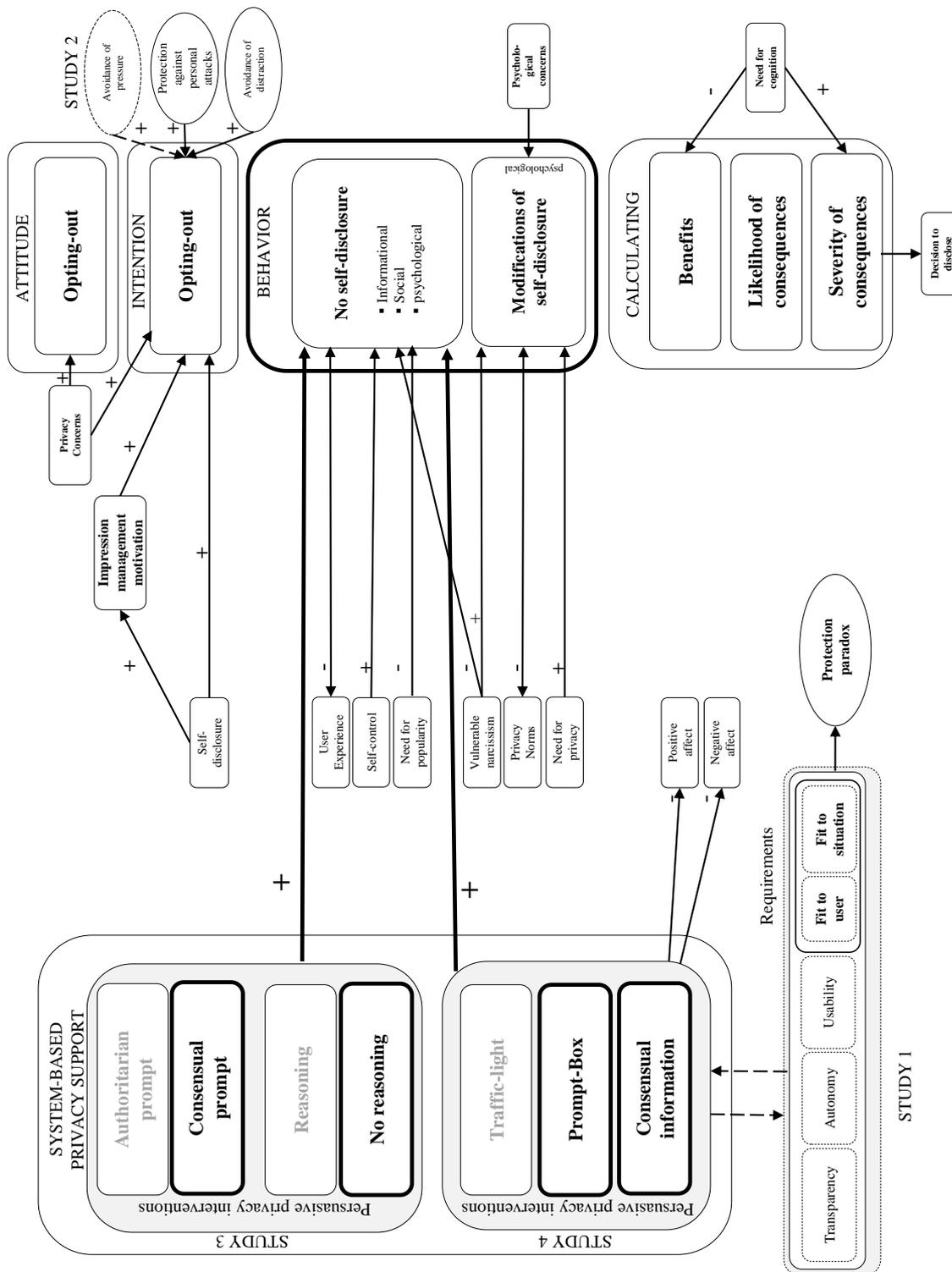


Figure 18: Modified research model based on empirical investigations.

16.1.1 Intrapersonal Factors

Intrapersonal factors comprise personality variables, prior experiences (see PMT; Floyd, Prentice-Dunn, & Rogers, 2000), perceived norms (whereas actual transmitted norms from peers, media, or society can also be assigned to the environmental factors), attitudes, intentions, perceived behavioral control (see TPB, Ajzen, 1991), and perceived (or desired) states of privacy (see PPM, Dienlin, 2014; here also: the actual privacy state might be assignable to the environmental factors, but the individual perception of one's own privacy is considered as intrapersonal factor in this work).

Current and desired states of privacy

In the scope of this dissertation, the users' desired and actual states of privacy have mainly been addressed in Study 1. Therefore, the following paragraph will summarize and discuss insights from the first study and partly refer to the results of Study 4, in which perceived privacy norms have been investigated, as well.

Study 1 qualitatively addressed users' perceived privacy states, their desire for privacy protection and their anticipated intentions to utilize system-based privacy protecting measures in the future. In line with this, the multidimensionality of privacy, the relevance of individual needs, and users' (during the interviews revealing) skepticism towards privacy protection tools (i.e. the *protection paradox*, see Chapter 10.6; *RQ4*) were addressed. While there is a wealth of knowledge about motives of why users are disclosing personal information online (see Chapter 4.1), it is still not clear how to empower users sufficiently in protecting their privacy, how to deal with users' dissatisfaction with available privacy settings, how to deal with users' skepticism toward providers of privacy supporting tools (see Chapter 10.6; *RQ4*), and how to reduce threats based on situational and impulsive disclosures on the Internet. Against the background of the theory of planned behavior (Ajzen, 1991), Study 1 addressed the question of how to increase users' intentions (i.e. important drivers for actual behavior) to reflect on risky online actions and engage in protective behavior. Following the theory, users' intention to improve privacy behavior would be an essential factor for installing an application that provides system-based privacy support and for its impact on users' actual

behavior. As was explained in Chapter 5, human behavior is quite reliably predictable through assessing people's attitudes and intentions (TPB; Ajzen, 1991). However, in the scope of this dissertation, it revealed that this predictive power is less accurate when examining situational short-term privacy behavior. Stable attitudes and intentions seem to be overridden by situational triggers and anticipated short-term rewards. The findings from Study 1 indicate that users wish for external support concerning privacy protection, which might be contributable to users' stable privacy attitudes and protection intentions. The fact that they *need* support might be attributable to the situational mitigation of stable privacy attitudes through anticipated short-term rewards. The desire for privacy support might also be based on the perceived contradiction between users' desired (i.e. no privacy risk is given) and actual (i.e. privacy is threatened) privacy states. The regulation of a current privacy state requires people's capability and ability to control the situation (see Dienlin, 2014). To the disadvantage of most users of SNSs, the required level of situational control is not continuously retrievable. In a situation in which users' control is lacking, external privacy support can provide the required controllability and help the users to achieve their desired privacy state. It needs to be considered that once, a desired privacy state is reached, this will not be constantly present but rather, due to the dynamic nature of privacy (see Chapter 2.1), de- and increase from time to time. Therefore, users would need to repeatedly engage in (online) privacy regulation, which might be perceived as costly and effortful by them. User-centered and adapted systems that are able to adapt to a given situation, to evaluate privacy states as well as potential harms and, based on this evaluation, provide recommendations for privacy-enhancing actions, can disencumber the users of SNSs.

In line with prior research, Study 1 revealed perceived norms to be a relevant predictor for people's self-reported behavioral intentions as well as for reported and desired states of privacy (see also Chapter 4.1 and Chapter 5.1). Nevertheless, in-depth investigations in the scope of Study 1 demonstrated that interviewees' actual behavior is not comprehensively in accordance with the reported social norms. Strikingly, Study 4 even revealed users' actual privacy behavior to be contrary to perceived privacy norms, which is referred to in the next section. Interviewees of

Study 1 stated that they know about the relevance of privacy protection and the potential harms of disclosing sensitive information, for instance, transmitted by family, peers, or the media (which was quantitatively investigated in Study 4; see Chapter 13). Participants were sure about the fact that online privacy is something one has to care about (see Chapter 13.6.2). However, when asking for concrete intervening and protecting measures that were translated into action, low privacy engagement on a regular basis was reported. Despite some self-concealing activities (e.g., deleting postings) and the reported tendency to avoid publishing personal content *in general*, participants nevertheless stated that they sporadically publish personal content (see Chapter 13.6.2). This might be due to a lack of situational awareness and the anticipation of benefits outperforming privacy concerns and perceived risks. This fits to the findings by Dienlin and Metzger (2016) demonstrating that the anticipated benefits of disclosing the self diminish users' privacy concerns (see also privacy calculus; Chapter 5.2).

In contrast to the results of Study 1 that are based on qualitative self-reports the results of Study 4 mirror actual privacy behavior in terms of disclosing or withdrawing personal information on an SNS. Interestingly, and contradicting to the stated hypotheses which referred to Park and Smith (2007) and Utz and Krämer (2009), social norms did not positively, but instead negatively influence users' privacy behavior in Study 4. More precisely, perceived privacy norms (i.e. the perception that society and media suggest to take care about privacy) was related to less cautious privacy behavior (i.e. more personal disclosure by users with strong perceived privacy norms). This implies that users, who think that media and society suggest caring about privacy, protect their privacy less, at least in terms of their disclosure behavior in a registration form of an SNS. The discrepancies between results of prior studies regarding the influence of perceived norms on behavior and findings in this study might be based on the measurement of the privacy behavior which was not a self-report in this study but real behavioral data. It might be the case that in self-reports, users would have indicated to care more about their privacy when they perceive the social norms regarding privacy more strongly. It is also conceivable that users want to defy perceived norms and therefore behave contrary to transmitted rules. However, this result should be considered with caution,

because in line with the mentioned literature regarding the examined hypothesis, perceived (privacy) norms have been shown to be related to people's behavior, for instance, in terms of restricting the access to one's profile on an SNS (e.g., Utz & Krämer, 2009). Nevertheless, restricting the profile relates to social privacy behavior (see Burgoon, 1982), whereas disclosing or not disclosing information (e.g., name, interests, personal characteristics) during a registration process for an SNS rather refers to the informational and psychological dimensions of privacy (see Burgoon, 1982). It might be the case, that perceived social norms do not influence privacy behavior regarding all dimensions of privacy, but only some of them. With this result, the complexity and multidimensionality of human privacy behavior has been revealed once more (see Burgoon, 1982; Petronio, 2002; Westin, 1967), stressing the importance of meticulously considering the psychological and social value of privacy protection and factors that influence protective behaviors. Furthermore, restricting the access of the own profile is a long-term method for privacy protection whereas concealing or withdrawing particular information can be considered as situational privacy behavior.

In sum, the potential of real-time privacy support was underlined by the finding of Study 1 suggesting that users' *general privacy awareness* is present but *situational privacy awareness* is missing.

The diverse roles of online privacy concerns

Findings of Study 1 demonstrated privacy concerns to be a continuous attendant in the back of participants' heads, being the reason for a negative basic feeling regarding online privacy (and also, one reason for the general desire for privacy support). However, according to findings of Study 1, these constant concerns are not sufficient to prevent users from privacy-threatening actions (e.g., disclosing sensitive content to unknown audiences). One reason for that might be that human beings tend to focus their attention on selected cues or factors related to making decisions in order to avoid an information overload (i.e. an individual's state in which he or she is not able to process all incoming inputs leading to breakdown; Rogers & Agarwala-Rogers, 1975). If users' attention is not fully given to situational online privacy protection but instead disturbed by other incoming

stimuli, privacy-relevant disclosure decisions are likely to be driven by the peripheral or emotional processing of situational cues (see Chapter 3.1). This leads to disadvantageous privacy decisions (e.g., sensitive disclosure based on the anticipation of benefits instead of withdrawing information due to potential risks). In situations in which users are lacking awareness and cognitive capacities to either apply privacy literacy (if it is present) and regulate the privacy state by using privacy settings or other regulative measures, or to act in accordance with perceived privacy norms, external privacy support can be a promising solution for users who want to protect themselves.

The first study further revealed that privacy concerns are related to the horizontal (e.g., other users) rather than to the vertical dimension of privacy (e.g., network providers; see Chapter 2.2; Bartsch & Dienlin, 2016). This is not due to the fact that users feel secure concerning practices of network providers and companies but instead it might be a kind of acceptance regarding the fact that personal data cannot be fully protected in the current digitalized world (as participants said). This result also refers to the *privacy cynicism* which was revealed to be present for users perceiving to have no chance to protect data in a study by Hofmann and colleagues (2016; see Chapter 8.3). From a psychological perspective, this perception represents a dramatic development since the feeling of powerlessness diminishes users' autonomy, which is an important factor with regard to privacy and users' well-being (Masur, 2018; Westin, 1967). The perception of not having any chance to avoid observation, or the constant fear of potential data theft and privacy violations might have severe consequences. In line with this, the question of how to empower users in their privacy decisions becomes even more relevant and is not only an issue for psychologists and software engineers, but also for politicians. First steps in this regard were taken with the new GDPR in the EU, aiming at providing more transparency and fairness with regard to data processes. The new law, for instance, claims that data processing systems and responsible actors are obliged to provide system designs in line with the legal guidelines as well and clarifying the rights of the users. The GDPR further ensures that all EU-member states follow the same rules, aiming at providing comparable conditions for all involved actors. As summarized by Barlag (2017), there are three

overarching goals of the GDPR, covering the EU-wide standardization of the data protection law, the harmonization in terms of competition, and the modernization of the data protection law.

Although users indicated to feel powerless regarding vertical privacy issues and highly concerned regarding horizontal privacy-related consequences (e.g., becoming victims of firestorms), a third-person effect was recorded as well, implying that users perceive themselves to be less endangered than other users are (children and teenagers were perceived to be especially endangered). Among others, this might be attributable to the fact that no interviewee already experienced a very harmful privacy threat. It has been revealed, that making negative experiences is one of the motivations to engage subsequently in privacy protection (see Chapter 3.3; Wang et al., 2011). However, as outlined in Chapter 3.1, people are also able to act based on the pure idea of being exposed to a privacy threat if a privacy-related decision (e.g., disclosing sensitive information or not) was made under objective risk conditions, meaning that risks are known to the user (e.g., through being communicated through support measures) and cognitive capacities are available (see also Schiebener & Brand, 2015). In line with this, the potential of situational system-based privacy support reveals itself again. Even if people did not experience negative outcomes of sensitive self-disclosure by themselves, an external cue occurring in real-time, persuasively hinting to potential threats, can release the user from his or her unaware state and trigger more reasoned privacy action. Using the persuasive power of triggers in crucial situations was also suggested by Fogg (2009). This situational solution would be beneficial for both user groups, with and without privacy literacy. Users having privacy literacy would be reminded of their knowledge in a privacy-relevant situation in which they might lack awareness and attention, and users with insufficient literacy can rely on the suggested recommendation by the system-based privacy protection measure. For sure, this requires accurate and transparent transmission of information by the system (see Chapter 10.6; *RQ4*). In order to guarantee privacy support measures adhering to privacy requirements as well, software developers of technical privacy interventions should adhere to the mentioned patterns for designing privacy-enhancing technologies (see Chapter 8.3). As outlined by Meis and Heisel (2017),

such patterns comprise security issues such as data integrity, anonymity or unlinkability as well as user experience forces. Since participants stated to be concerned that the system that provides privacy support could be a privacy invasion in itself, it is highly relevant to adhere to these patterns and to transparently communicate how the privacy support system works, in what sense data is stored, for which reasons it is used, and whether or when it is deleted. This concern with regard to potential privacy harms, based on the privacy intervention measure itself, was named *protection paradox* within the scope of this work (see Chapter 10.6). Participants of Study 1 communicated the desire for having external privacy support from a system. However, the fact that the support system would need to parse the users' online actions very carefully, and consequently gain detailed knowledge of the participants, scared the users and might even decrease their intention to use such a privacy preserving measure. This pattern was also examined in a quantitative online investigation concerning Internet users' desire for protection and their intention and attitude toward using a privacy protecting tool for a specific website (Meier & Schäwel, 2018). With regard to the desire for protection, it was found that perceived privacy risks were positively related to the users' desire for protection and the desire for protection was positively related to users' willingness to use an introduced privacy protecting tool (Meier & Schäwel, 2018). Most importantly, this study revealed that users' desire for privacy protection was only related to the behavioral intention to utilize this tool if it was introduced as not recording and collecting personal user data. This finding is in line with reported mistrust by users towards a privacy protection system that gathers their data, although it should be in their interest in privacy protection.

With respect to the diversity and multidimensionality of privacy concerns, concerns are not the only indicator for privacy protection behavior, but they rather induce information withdrawal if anticipated benefits are not as salient as anticipated negative outcomes (Dienlin & Metzger, 2016). This was also revealed by the investigations of Study 2, in which positive relations between users' privacy concerns and each of their attitudes and intentions to opt-out from a social network were found. It is conceivable that concerns did not have a significant effect on the impact of privacy intervention in Study 4 because perceived situational benefits

might have been more salient to users (which would be in line with findings by Dienlin & Metzger, 2016). This seems to contradict the findings of the CBC analysis, also in Study 4, which demonstrated the severity and likelihood of the occurrence of a privacy threats to be more crucial for users' decisions about posting or concealing content than anticipated benefits. However, the non-significant impact of privacy concerns on the effectiveness of the privacy intervention relate to situational and immediate concealing behavior, whereas the decisions within the CBC task were based on (several rounds of) explicit evaluations of risks and benefits under objective conditions for decision-making. Objective condition in this case means having concrete indicators for the occurrences of benefits, negative consequences, and its severity (see Schiebener & Brand, 2015). In addition to that, and in contrast to the function of the privacy traffic light in the registration process (see limitation outlined in Chapter 13.9), the conditions for the privacy decision in the CBC task have been extensively explained. This might implicate that participants were strongly sensitized to the relevance of risks and benefits of self-disclosure on the Internet. In line with this, privacy-decisions were taken in a more aware state compared to the situations without clear indicators and explanations regarding potential outcomes of particular privacy-related actions. The fact that in the decision-task, the perceived severity of a consequence of self-disclosing outweighed the perceived importance of the likelihood of the occurrence of the risk, supports the assumption that situational disclosure and concealing behavior differ from cautious long-term privacy behavior (see Masur, 2018). In the discussion of Study 4 it was argued that the privacy interventions can change an ambiguous privacy decision situation into a more objective one, which might be one reason why the interventions were effective. However, when comparing the impact of a privacy intervention in a current disclosure situation (which can transform a complete unaware privacy situation to a more objective one) with a decision-situation with even more concrete privacy indicators as it was the case in the CBC task, it reveals that concrete indices can boost the persuasive effect of privacy protection measures. This result is a relevant insight with regard to practice because it demonstrates the power of concrete and informative icons indicating privacy risks and suggestions for alternative actions.

The diverse influence of users' personality traits

As it was outlined in the Chapters 5.1, 6.1, and 6.2, a considerable number of variables that influence privacy intentions and behaviors have been examined by several researchers so far (e.g., privacy concerns, see Dienlin & Trepte, 2015; Hoy & Milne, 2010; privacy literacy, see Bartsch & Dienlin; 2016; Trepte et al., 2015; traits like narcissism, need for popularity, or need for privacy, see Ahn, Kwolek, & Bowman, 2015; Hofstra, Corten, & van Tubergen, 2016; Zlatolas, Wezler, Heričko, & Hölbl, 2015). Nevertheless, knowledge regarding the potential influence of users' personality characteristics on the impact of specific privacy support measures on actual behavior (by means of an experimental setting) has not been examined comprehensively until now. Therefore, Studies 2, 3, and 4 of the present dissertation investigated users' personal traits with regard to behavioral privacy intentions and actual privacy behavior, as well as the influence of personality traits on the relation between privacy interventions on subsequent behavior.

In Study 2, participants' extent of self-disclosure was found to be positively related to the intention to use the opting-out measure presented, mediated through situational impression management motivation. However, the influence of *impression managing* activities on privacy behavior needs to be reflected critically. One might pose the question under what conditions impression management is solely driven by the intent to present oneself in a positive light and under what circumstances the managing of one's impression is meant as a privacy protective action (as it was proposed by Vitak, 2012). On a meta-level, shaping one's impression online can be understood as privacy protection measure because damageable presentations of the self might provide space for other users to attack or embarrass the user, which poses a risk for horizontal privacy. Therefore, impression management motivation in this work is considered as a variable shaping users' privacy behavior.

In general, people with a strong *impression management motivation* want to be visible for other people (see Chapter 6.2.3). Accordingly, they also might seek to guard their profiles that are presenting positive impressions of them, in order to counteract other users adding negative comments on their profiles. The mediating effect of impression management motivation on the positive relation between users' extent of online self-disclosure and the intention to opt-out from the network in Study 2 might be explained

by the fact that users who are strongly concerned about being represented in a negative light by other users perceive opting-out from the network as an adequate solution for controlling their impression and counteract (horizontal) privacy violations. Interestingly, personality characteristics associated with self-expressive behavior (e.g., impression management, need for popularity, grandiose narcissism) had no moderating role in the relation between a privacy intervention and subsequent privacy behavior in Study 3 and Study 4. This apparent contradiction might be explained by the fact that the constructs measured in Study 2 were investigated with regard to behavioral intentions instead of actual behavior (as it was done in Studies 3 and 4). It can be assumed that users with strong impression management motivation tend to avoid situations, in which other users could harm their positive image that they created on an SNS (e.g., through other users posting negative content on the users), leading to the reported intention to make use of the opting-out method. However, it cannot be concluded, that these users actually would engage in using the super-logout in reality. Behavioral intentions are valid predictors for actual behavior in general (Ajzen, 1991), and also with regard to online privacy behavior (Dienlin & Trepte, 2015). Still, it cannot be excluded that users with pronounced impression management motivation would omit opting-out in reality, possibly because they cannot withstand the situation of not being online and engage in impression management or guiding their profile. The reported behavioral intentions might be weakened by anticipated benefits (coming along with different cognitive processes of privacy-related decision-making) or situational cues that disturb elaborated weighing of risks and benefits regarding presenting oneself driven by impression managing motivations. Study 2 of this dissertation investigated the situational motivation to engage in concrete impression managing activities with direct regard to users' online presence. In contrast to the measurements in Study 2, the Studies 3 and 4 measured actual observable behavior of participants. In Study 3, personality characteristics that are related to self-promoting activities (need for popularity, grandiose narcissism, and impression management) were considered as potential influencing factors on participants' privacy behavior. Here, privacy behavior was analyzed by means of two different variables measuring actual behavior, namely, modifying behavior (i.e. the number of changes within input fields in a registration form for an SNS after receiving a persuasive privacy

prompt) or self-withdrawal (i.e. the number of empty fields at the end of a registration process).

Need for popularity for instance, was assumed to negatively influence the effect of the persuasive privacy prompt (which was suggesting to disclose less information) on users' withdrawal behavior. The assumed effect was not supported by the data. However, a significant negative main effect of need for popularity on withdrawing behavior was found, indicating that users with a high need for popularity tend to withdraw less information than users with a low need for popularity. This result, as well as the findings of Study 2, reveals personal characteristics (e.g., need for popularity) and situational motivations (e.g., managing one's impression) related to self-expressing activities, to be important drivers for actual and intended online behavior and also for online privacy behavior. However, the negative relation between need for popularity and self-withdrawal (Study 3), and the positive relation between impression managing motivations and the intention to opt-out from the network (Study 2) seem to be contradicting and might be contributable to two factors. First, users with pronounced situational impression management motivation are able to disclose self-related information to their network and temporally withdraw from the network without suppressing the need for self-disclosing and the desire for getting positive feedback. The advantage for them would be that in situations in which they are not online and able to control potential impression damaging activities on their profiles, the possibility that disadvantageous and defamatory activities can happen is very low. It might have come to another result if – instead of assessing the temporally opting out option – the intention or the actual behavior of disclosing less information was examined. This idea was actually implemented in Study 3 in which users' withdrawal behavior was examined. Users were not asked whether they would temporally deactivate their SNS accounts due to privacy reasons, but their actual withdrawal behavior in a situation in which they in fact had the chance to create a positive impression of them by providing advantageous self-related information, was examined. Here, the negative influence of the need for popularity on the extent of information withdrawal was in line with theoretical assumptions, stating that a high need for popularity would lead to less self-withdrawal. Conceivably, high need for impression management would have led to a similar result in Study 3, when observing behavioral patterns allowing for creating a positive impression in contrast to temporally protecting

the SNS profile from attacks. Interestingly, a relation between need for popularity on privacy behavior, in terms of changing self-related information after being reminded on privacy protection, was not revealed (i.e. number of changes, see Chapter 12.5). A behavioral change as a response to a single situational cue might be based more strongly on immediate situational circumstances and characteristics of the privacy intervention, whereas the cumulated behavior at the end of the registration process in terms of the total number of empty fields as a response to privacy measures might be influenced more by personal characteristics. It is also conceivable that users realized the relevance of communicated privacy-related information within the prompts only after seeing it several times and then, with increased awareness and several experiences with the prompts in the course of that interaction with the social network, for instance, their general need for popularity did actually influence current behavior.

Study 3 demonstrated a positive influence of participants' *need for privacy* on the quantity of edits of disclosed information (i.e. number of changes) of people who received a privacy prompt, indicating that the users' need for privacy might indeed influence the impact of privacy interventions, even though there were no moderation effect revealed by data. Since the need for privacy is a relevant variable in privacy research and pivotal for people's privacy behavior (e.g., Dienlin 2017; Trepte & Masur, 2017), results of this study should not be interpreted as proof that privacy-related personality traits do not matter with regard to external privacy interventions. Instead, these results should spark further research investigating the impact of users' need for privacy on intervening measures. Furthermore, as was also revealed with regard to the influence of privacy attitudes on privacy behavior (see Chapter 6) by Dienlin and Trepte (2015), it is not sufficient to consider only two variables, that are hypothesized to be related to each other, but instead consider the variable of interest embedded in interferences with other variables. Taking this into account, it is conceivable that the influence of the users' need for privacy on the relation between an intervention and subsequent privacy behavior might depend on other variables such as people's need for cognition (if the privacy intervening message provides much information), privacy concerns, or experiences, as well. The need for privacy was also investigated in Study 4, but no no significant moderating effects revealed. This mirrors the findings of Study 3. However, significant negative correlations between the users' need for informational privacy and the extent of

introducing the self (i.e. sensitivity and diversity of self-disclosure) were found. Thus, users with a high need for informational privacy provided less sensitive and less diverse personal information. This is in line with Błachnio and colleagues (2016) who found that individuals with a strong need for privacy are less likely to engage in online social networking activities. However, both Study 3 and Study 4, demonstrate that the need for privacy is a decisive variable for users' online privacy behavior in terms of withdrawing the self, stressing the importance of considering this need in privacy research in order to (a) better understand users' online actions and non-actions and (b) to provide more efficacious protection measures, which account for the human need for privacy.

Strikingly, people's need for privacy is challenged by nowadays' social media. In the ubiquitous online environments, humans' general desire for being in control of self-related data, in terms of controlling who has access to personal data, whether it is forwarded to others, or (mis-)used by strangers, cannot be satisfied due to blurred boundaries and mixed communication circles consisting of heterogeneous audiences (see Chapter 2.2). In line with this, social media users' autonomy and opportunities for experiencing solitude, intimacy, autonomy, and reserve (i.e. the states of privacy as defined by Westin, 1967) are threatened in the digitalized world, which might bring severe consequences for users' well-being and emotional release. Therefore, it is of high relevance to provide users with the possibility to diminish the threat of privacy and to foster more research examining the construct of users' need for privacy in the scope of privacy protective attempts.

People's *vulnerable narcissism* was also shown to influence withdrawal behavior (i.e. number of empty fields) in Study 3. Strikingly, and in contrast to the assumed positive influence of vulnerable narcissism on withdrawing the self (based on findings by Ahn, Kwolek, & Bowman, 2015), a negative relation between the variables was observed, here. As already indicated in Chapter 12.5, an explanation for the contradicting results might be the different operationalization of privacy behavior. While Ahn, Kwolek, and Bowman (2015) argued that vulnerable narcissistic persons engage more in restricting privacy settings on SNS, the present study investigated users' behavior in terms of withdrawing and concealing particular information during a registration process. Furthermore, Ahn, Kwolek, and Bowman (2015) considered behavioral intentions, based on self-reports, instead of analyzing actual behavior. Once more, the current study

demonstrates that people's actual behaviors might differ from self-reported attitudes and intentions (see also results regarding the impression management motivation). Based on their characteristics (e.g., general fear and suspect, see Wink, 1991), vulnerable narcissistic users might actually intend to protect their profile more strongly. However, with respect to real behavior, people's desire for recognition and special treatment might override their concerns and the willingness to control online privacy, indicating that the weighing process of risks and benefits related to disclosing or not disclosing the self (i.e. the privacy calculus), might result in different privacy decisions depending on situational versus long-term decisions. Additionally, this result stresses the difference between various kinds of protection behaviors, suggesting that the intention for withdrawing and concealing personal information might be driven by other factors than the intention to generally restrict the profile, once more. Interestingly in contrast to this negative influence of vulnerable narcissism on the number of empty fields, vulnerable narcissism was a positive predictor for the number of changes in input fields. As was observed by Ahn, Kwolek, and Bowman (2015), vulnerable narcissistic persons intend to protect their online privacy. However, this reported general intention regarding the usage of privacy settings, which might be more transferrable to long-term behavior than to situational disclosure or withdrawal intentions, might not be sufficient in triggering situational privacy behavior. In contrast, the privacy prompts in Study 3 might have triggered fears of vulnerable narcissistic persons, recalling protective intentions resulting in withdrawing disclosed self-related information after being prompted by the privacy intervention. From a methodological perspective, the opposing results regarding the influence of vulnerable narcissism can be also attributable to the operationalization of the dependent variables (a) modifying disclosures (i.e. number of changes) and (b) self-withdrawing (i.e. the number of empty fields). The positive relation between modifying disclosures as a response to a privacy intervention and vulnerable narcissism necessarily implies that vulnerable narcissistic users at first provided a specific amount of information that they were then able to modify after receiving a prompt. Thus, the finding that vulnerable narcissistic persons had fewer empty fields in the end than persons with a lower extent of vulnerable narcissism still contradicts the stated hypothesis concerning the withdrawing behavior, but actually supports results concerning the hypothesis referring to the number of changes as dependent variable. Only if users disclose a certain amount of information, they had

the possibility to make many changes (possibly resulting in fewer empty fields in the end, e.g., if information was deleted), resulting in a positive relationship between vulnerable narcissism and the number of changes. It needs to be considered that the changes not only included the change from a filled field to an empty field but also modifications in the expression or regarding the amount of provided information.

A further important individual characteristic in the scope of this work was the individual *need for cognition*. As hypothesized (referring to Kehr, Kowatsch, Wentzel, & Fleisch, 2015), analyses in Study 4 indicated users' need for cognition to be positively related to the perceived severity of negative consequences of online self-disclosure. In contrast, users' need for cognition negatively influenced the perceived importance of anticipated rewards. This indicates that users with a high need for cognition evaluate potential risks more reasoned (through the reflective route) than users with a low need for cognition who seem to be more influenced by the benefits of information disclosure (through the impulsive route, see Chapter 3.1). Basically, users with a high need for cognition tend to think and elaborate more carefully and consider different outcomes of particular situations more cautiously. In contrast to effortful elaborations of potential privacy risks, anticipated rewards might be considered less objectively but instead driven by emotions, which is not typical for users with a high need for cognition (Cacioppo & Petty, 1982; Schiebener & Brand, 2015).

Study 4 revealed a significant positive main effect of participants' *self-control* on withdrawing behavior, indicating that people with high self-control show more cautious privacy behavior. As was discussed in Chapter 6.2.6, people's self-control can help them to resist temptations (Ent, Baumeister, & Tice, 2015). Referring to results of Study 4, this indicates that users with pronounced self-control were able to resist the temptation to disclose personal information, which originally would have been related to tempting outcomes (e.g., getting positive feedback and appreciation, e.g., Christofides et al., 2009; Taddicken, 2011). Derived from data, it can be concluded that people who generally have high self-control seem to be able to control their disclosures on an SNS, as well. In line with the theory of planned behavior (Ajzen, 1991), results demonstrate that perceived self-control is highly relevant for actual behavior. Increasing users' perceived self-control seems to be a promising factor for increasing privacy awareness and might also come

along with increased well-being since the capability of handling a situation is associated with a positive association of the self.

In sum, it revealed that personality traits indeed have an influence on particular online privacy behaviors of users. In addition to that, and in contrast to previous research which did not measure actual behaviors or distinguish between different types of privacy behavior as it was done here, it was demonstrated that users' personality traits have different influences on the different kinds of privacy behavior. This reveals considerable insights for privacy research because it indicates that, depending on the operationalization of privacy behavior, the influence of personality traits on users' privacy behavior is as manifold as users' personality and the construct privacy itself.

Besides users' personal characteristics, their perceptions of privacy risks and potential consequences were revealed to be decisive for disclosure and withdrawal behavior. The relevance of perceived and communicated risks will be discussed in the following.

Perceived risks and consequences for privacy-protection approaches

In the scope of this dissertation, users' perceived risks of online self-disclosure and corresponding weighing processes were investigated in order to shed more light on the privacy calculus (see Culnan & Armstrong, 1999). As outlined in Chapter 5.2, the privacy calculus describes people's evaluation of potential positive and negative outcomes of disclosing the self and subsequent decisions with regard to privacy behavior. In this work it was assumed that the weighing of risks and benefits of online-self-disclosure is actually embedded in even more complex relations between users' intrapersonal characteristics, prior experiences, behavioral motivations (see Rogers, 1983), behavioral intentions, anchored standards, norms, and attitudes (see Ajzen, 1991), and does not take place rationally without personal and environmental factors playing a role.

The privacy calculus was explicitly addressed in Study 4. It was aimed to get further insights into the black box of online privacy decision-making by examining the relevance of each, positive and negative outcomes of disclosing the self. Following the protection motivation theory (Rogers, 1975), negative outcomes comprise of both, the severity of consequences (of not protecting the self) and the vulnerability (Floyd,

Prentice-Dunn & Rogers, 2000). In order to also address the complexity of negative outcomes of online self-disclosure and to make potential risks more tangible for users, Study 4 differentiated between the severity of a negative consequence and the likelihood that the consequence will occur, representing the level of vulnerability. The intention behind operationalizing the privacy calculus was to find out whether anticipated positive or negative outcomes of disclosing the self are more relevant for users' decision to actually disclose in a more indirect way than through self-reports. Therefore, a choice-based conjoint scenario was used for examining users' privacy decision-makings. Three different attributes, referring to either positive (rewards) or negative (likelihood and severity of consequences) outcomes of sensitive information disclosure, each varying depending on characteristics of the attributes (from low to high rewarding / likely / severe) have been investigated concerning their relative importance in a privacy decision. In line with Krasnova and colleagues (2010), and Krasnova, Kolesnikova, and Guenther (2009), Study 4 indicated that for the decision to self-disclose, the severity of consequences is decisive. Although prior research indicated that rewards (e.g., social support) can foster information disclosure and outperform users' privacy concerns (e.g., Dienlin & Metzger, 2016), concretely communicated risks, indicating explicit levels of severity, seem to be even more relevant for users' decisions to disclose. Data revealed that, if anticipated risks become perceptible through being clearly and visually communicated; users strongly refer to it and tend to decide to not disclose sensitive content referring to the self (if the severity of a risk was high). This pattern was also derived from interviews in Study 1, in which interviewees wished for concrete and easy to understand information about potential risks in order to make more aware privacy decisions. Study 4 revealed that the likelihood that a consequence would generally occur was the second most important variable after the severity. The least decisive variable in the decision to publish a posting was the anticipation of rewards, indicating interesting implications for risk-communication in terms of privacy support. This is also in line with the protection motivation theory (Rogers, 1983) stating that fear-appraisals are effective in inducing protection motivation and implementing protective behavior. In line with this theory, a privacy intervention triggers threat appraisal processes, evaluating the maladaptive response to the severity of communicated risks, inducing protection motivation and finally influencing the actual coping mode and subsequent behavior.

As the protection motivation theory claims, intrapersonal factors such as personal characteristics and experiences also have an influence on people's evaluation of threats and subsequent protection motivation. Hence, Study 4 examined the influence of a decisive variable for human decision-making – the need for cognition – on the calculus regarding positive and negative outcomes of self-disclosure. The fact that individuals' need for cognition positively influenced the relevance of the severity of a consequence related to disclosing the self and negatively impacted the importance of anticipated rewards, gives new insights to the privacy calculus as well. This result might be associated to findings regarding the influence of users' privacy literacy on privacy behavior. More precisely, high levels of privacy literacy correlate with more secure privacy behavior in terms of the usage of more restrictive and regulative measures (e.g., Bartsch & Dienlin, 2016). Likewise, users with high privacy literacy might be able to assess risks of online actions more accurately. Given that people with a high need for cognition enjoy problem solving, thinking, and processing information (Cacioppo & Petty, 1982) they might also be more inclined to learn about privacy conditions and acquire privacy literacy. Thus, the assessments of privacy risks and benefits within the privacy calculus might also depend on users' levels of privacy literacy. However, the concrete influence of privacy literacy on the privacy calculus needs to be investigated further, as Dinev and Hart (2004) found internet literacy to be negatively related to privacy concerns and positively related to the intention to conduct online transactions, for instance. This indicates that high literacy might come along with less privacy concerns, since users with high literacy know how to counteract potential harms through making use of privacy regulative measures and settings. This is in line with findings by Bartsch and Dienlin (2016), demonstrating that users with high privacy literacy feel safer than users with lower levels of privacy literacy. Still, even if people with high literacy were less concerned and feel more protected based on their skills, their decision to disclose might nevertheless depend on the anticipated severity of consequences. However, in contrast to users with low literacy, users with high literacy might know how to cope with the threats. Thus, it is important to re-elaborate the role of privacy concerns. On the one hand, privacy concerns can be related to privacy cynicism, repressing privacy risks, or a biased assignment of privacy risks for people with low privacy literacy (subsequently even increasing privacy risks). On the other hand, privacy concerns – accompanied by high privacy literacy or a high need for cognition –

might foster privacy-aware and protective behavior by assessing negative consequences as being important and similarly knowing how to deal with them.

However, given that current data indicated that communicated risks of information disclosure influence the outcome of the privacy calculus more strongly than rewards – even independently from users’ need for cognition – it should be focused on communicating concrete privacy threats in privacy risk-related communication when aiming at fostering users’ online privacy in a situation of concrete threat. When solely aiming at informing about the situational privacy state, a balanced presentation of potential negative and positive consequences might be more reasonable.

Susceptibility to persuasive privacy interventions

This work also considered the impact of the susceptibility to a persuasive style of communication of a persuasive intervention. This construct played the biggest role in Study 3, which assumed that the persuasive style of communication might influence users’ behavior in the sense that one persuasive style (either authority or consensus) would potentially be more persuasive than the other one. Data from Study 3 revealed an interaction effect between the persuasive style of the prompts and the extent of provided information within the prompts. Mean values indicated that users who received a consensual privacy prompt without reasoning concealed more personal data than those who received a consensual prompt with reasoning. In contrast, a persuasive prompt in an authoritarian style was more effective (i.e. users provided less data) with additional information than without (see Chapter 12.5). Overall, the strongest privacy behavior (i.e. most empty fields) was found for participants receiving a persuasive prompt in a consensual style without information. However, users’ susceptibility to the persuasive styles authority and consensus did not influence the persuasive effect of the provided prompts in terms of inducing a higher amount of changes. The idea to consider the susceptibility to persuasive styles of communication originated from a study by Kaptein and colleagues (2012) who found that users’ susceptibility to persuasive communication has an influence on the effect of a long-term intervention aiming at a behavioral change. In contrast, the persuasive prompts in the current study were only presented in one single experiment. It is open to question whether a long-term exposure to the persuasive prompts

would have revealed an influence of the susceptibility to persuasive styles of provided interventions on their actual effectiveness.

Despite the fact that there was no moderating effect of users' susceptibility to the considered persuasive styles, Study 3 revealed a significant positive main effect of participants' susceptibility to the persuasive style consensus on their privacy behavior as a response to the prompts (see Chapter 12.5). This indicates that people who are in general sensitive towards a consensual style of communication did more changes in their input fields after receiving a persuasive privacy prompt. Interestingly, users who were more susceptible to the style consensus did also more changes after a prompt in a consensual (instead of authoritarian) style occurred. However, the data showed that beyond the main effect of the susceptibility to the consensual style of communication, there was no significant interaction effect between the provided style and the susceptibility towards it. From a statistical perspective, this might be an issue of limited power due to a low number of participants. For the persuasive style authority, there was no main effect. However, data allow at least for cautious assumptions in the direction that a consensual style might be more effective than an authoritarian prompt, mirroring conclusions by Utz and Krämer (2009), and supporting findings from Study 1, which indicate that users want to have (a) feedback that is suited (indicating that susceptibility indeed might be an issue), and (b) not paternalistic but benevolent instead (indicating a preference for a consensual instead of an authoritarian style). In line with this, in Study 4, in which three different persuasive privacy interventions were tested, those privacy interventions that were formulated in a consensual style (adapted to consensual prompts in Study 3) revealed to be more effective than the intervention that was not presented in a consensual style.

Needs with regard to system-based privacy support

The findings of Study 1 are a valuable basis for developing system-based privacy support measures for users of SNSs. In line with them, system-based privacy support measures should provide transparent and gentle feedback referring to potential privacy risks. Participants' requirements in fact mirror the core elements of PETs as they were explained in Chapter 8.3, referring to Meis and Heisel (2017). It became clear that users wish for comprehensive information about data processing activities and for the unlinkability of their data. In addition to that,

they do not want their data to be forwarded to third parties and they want to experience a benefit of using the protective measure (compared to self-disclosing personal information for which the benefits are more present to the users). The desire for knowing about the benefits of using a privacy protecting tool might be grounded in the fact that the privacy measure might actually diminish the perceived gratifications which users usually gather through using SNSs, such as positive responses to their personal disclosures. With respect to application, this implies that privacy support measures can be even more efficacious when the benefits of following the suggested privacy recommendation are outlined. This can be implemented by textual positive enhancement or by using visual cues (as proposed in Study 4), indicating the current state of privacy (e.g., through a privacy-meter or a privacy traffic light) and clearly showing an improvement of the privacy state by changing the color from red to orange, or green, for instance. However, Study 4 provided ambiguous insights concerning this idea. On the one hand, visual cues indicating the extent of privacy threat and anticipated rewards within a concrete decision scenario (i.e. disclosing content depending on visually indicated risks and benefits) made risks more salient. More precisely, risks were evaluated as being more important for the decision to disclose than anticipated rewards, which actually contradicts the findings by Dienlin and Metzger (2016), who found that for the decision to self-disclose on SNSs, perceived benefits are more important than privacy concerns (however, with regard to self-withdrawal, concerns had a more influencing role than perceived benefits). On the other hand, a visual cue (traffic light), indicating the privacy level during actual self-disclosure, did not contribute to less self-disclosure than without the cue. This might be attributable to the methodological limitation that users were not clearly informed about the functionality of the privacy traffic light but instead had to find out by themselves what the visual cue is indicating. A practical implication of that result is that – even for seemingly self-explanatory measures – clear guidelines and explanations (in this case, an indicator for red means a high threat, orange means a moderate threat, green means no threat) can impact users' risk-evaluation and actual privacy behavior.

16.1.2 Environmental Factors

Appearance of system-based privacy support measures and provided risk-related information

This work also provides valuable insights with regard to the usability of a potential privacy support system. Derived from Study 1, users should not feel disturbed or overwhelmed by the intervention, since this would probably lead to the opposite behavior than intended (i.e. reactance reaction; see Chapter 5.4). Moreover, continuous feedback regarding the actual state of privacy might be a suitable method to enhance privacy behavior even more. As it was already discussed in Chapter 8.5, persuasive elements indicating the current state of progress or endangerment, respectively (e.g., Bang, Torstensson, & Katzeff, 2006), might be auspicious for indicating the current privacy state and concomitantly enhancing privacy awareness of SNS users. Moreover, Dienlin (2014) stated in his privacy process model that people constantly try to regulate discrepancies between current and anticipated privacy states. This can be easier to implement for users of SNSs if they had concrete and continuous measures indicating the present privacy states. From Study 1, the idea of a privacy-meter, giving an indication regarding the level of sensitiveness of the disclosed information or the level of current privacy risk, arose. This design idea was implemented in Study 4, which investigated the impact of persuasive privacy support interventions that changed their appearances with regard to the current state of privacy risk. This state was symbolized through a change of color of the system-based privacy intervention from green (i.e. no privacy risk), over orange (i.e. medium privacy risk), to red (i.e. high privacy risk). This was on the one hand done by means of a privacy traffic light (see Figure 11, Chapter 13.6) and on the other hand by means of a colored information-box which persuasively informed about the importance of privacy protection by changing its color in accordance to the privacy traffic light. Talukder, Ouzzari, Elmagarmid, Elmleegy, and Yakout (2010) suggested a similar approach. As indicated in Chapter 8.4, Talukder and colleagues (2010) suggested indicating the amount of information leakage caused by the users' friends within the online network and the concomitant security risks for the users. However, the authors did not consider the users and their personal traits, and in what sense these traits might influence the effect of their *privometer* and users' subsequent privacy protection behavior. Furthermore, they did not outline potential limitations or ethical considerations of

utilizing users' data, even though they suggest extending their approach in the future by using private information such as the number of messages being exchanged between persons or mutual friendships in order to denote weak and strong ties for providing more accurate inferences (see Talukder et al., 2010). In contrast, the present thesis outlines advantages and disadvantages of using adapted and personalized privacy protection, and also discusses ethical implications (see Chapter 19). The considered persuasive style of communication and the amount of provided information in the persuasive privacy information box was based on findings of Study 3, revealing that a consensual style of communication, transmitting concise and not too extensive privacy-relevant information, comes along with pronounced privacy behavior (see Chapter 12.8). The functionality of the changing color was intended to enhance the process of persuasion in terms of providing a self-monitoring feature (see Chapter 8.5). As discussed, self-monitoring features that confront users with personal risks might also be helpful in order to diminish the third-person effect, which often reveals when asking users regarding their privacy perception and their perceived individual risk. It was argued that through visualized *personal* risks relating to a current privacy state, the individual's intention to reduce sensitive self-disclosure might be strengthened, and thus, in line with the theory of planned behavior (Ajzen, 1991), users may modify their online behavior more likely. Furthermore, the protection motivation theory (Rogers, 1975) states that subjective (adapted to the individual) threat appraisals are more decisive for the motivation to engage in privacy protecting behavior than universal risks without a fit to the user and the situation (see Chapter 5.4). This was considered through using persuasive privacy boxes that provided risk-related information, depending on the individual extent of self-disclosure by participants. Further, a privacy-meter, indicating the likelihood of a risk to occur, emoticons, indicating the severity of a risk, and icons, indicating the anticipated benefits of disclosing content, were implemented in a CBC task.

Besides continuous feedback regarding the current privacy state, information justifying the given recommendation were identified as relevant factors for participants (Study 1). An often-stated issue was that it would feel like paternalism if there would be a request for action without giving a reason or an explanation, or at least an indicator for why a particular behavior is recommended. This demand (which might be even more pronounced for people with a high need for cognition) was addressed by testing

persuasive privacy prompts that differed with respect to the presence of reasoning for a recommendation versus no reasoning in Study 3 (besides varying the persuasive communication style of the privacy intervention). However, in contrast to the stated hypotheses, the provided information did not increase the persuasive power of system-based privacy support measures. As already discussed in Chapter 12.7, this might have been the case because users were overloaded by information provided by the persuasive privacy prompts in Study 3. Given that the prompts occurred several times, users had to process several pieces of information. Results concerning the perception of system-based privacy interventions that was examined in Study 4, revealed, that the experience with the registration pages of the SNS did not differ with regard to the presence of a privacy intervention.

It was argued that the presentation of risks and potential negative outcomes of online behavior might be beneficial for persuading users to disclose less information. Indeed, Study 4 revealed that users assess the severity of a consequence and the likelihood that a consequence occurs as more relevant than potential rewards. Therefore, privacy interventions should focus on communicating explicit risk information if a very severe threat was given, potentially in combination with concrete examples of severe privacy invasions. When comparing the impact of a privacy intervention in a disclosure situation (which can transform a complete unaware privacy situation in a more objective one) with even more concrete privacy indicators within the CBC task, it revealed that concrete indices can increase the persuasive effect even more. With regard to practical implications, this means that persuasive privacy interventions can be further enhanced through additionally providing visual cues for each, anticipated benefits *and* potential risks. This might facilitate the privacy calculating process (see Culnan & Armstrong, 1999) and allow for more objective risk-benefit-evaluations.

Experience with an SNS providing system-based privacy support

Study 4 explicitly explored users' reported experience with the SNS depending on the presence of privacy interventions. Results did not indicate a significant effect of the presence of privacy interventions on the experience users had with the network. With a view to application, this result can be regarded positively because it indicates that interventions, as presented in the current study, do not negatively affect users' joy of use.

However, it also did not positively affect users' experience. Considering long-term interactions, it should be deliberated whether and which elements increase positive affect with regard to the interaction with a protecting intervention. One possibility would be to implement features providing positive feedback if privacy recommendations were implemented into action (as it is also suggested by persuasive research; e.g., Thaler, 2008; Fogg, 2009). However, one needs to keep in mind that rewarding elements bear also the danger that intrinsic motivation is converted into extrinsic motivation, which becomes a problem if an enhancing measure is only used temporally. More precisely, rewards can enhance behavior (see Deterding, 2011) and increase (in this case) protection motivation. However, if the protecting tool would not be used anymore after a time, the motivation is threatened to be even lower than before using the intervention (see also self-determination theory). Future research should focus on examining users' motivation and emotion with regard to the interaction of privacy intervention measures in more detail. Ambiguous findings with regard to users' affect in Study 4 support this track of research. Privacy interventions providing rewards and positive feedback can be one step in that direction.

17 Theoretical Implications

One goal of the present dissertation was to emphasize the importance of considering the complexity, multidimensionality, and diversity of people's online privacy behavior. With this work, it was attempted to provide theoretical and conceptual insights in the complex interplay between intrapersonal factors influencing the motivation and intention to protect one's online privacy, environmental factors transmitting actual privacy states and privacy risks, and behavior resulting from internal and external influences.

The theory of planned behavior (Ajzen, 1991) was successfully considered for explaining privacy behavior of SNS users in prior research (e.g., Dienlin & Trepte, 2015). For instance, analyses by Dienlin and Trepte (2015) revealed that users who think that it is important to regulate the access to one's profile on an SNS, show an increased intention to restrict the profile, leading to the fact that they more likely engage in restricting the access to their profiles. These relations are validly explainable through the theory of planned behavior (Ajzen, 1991), which states that attitudes and behavioral intentions are relevant predictors for actual behavior. However, these behavioral patterns are based on

self-reports of SNS users, implicating that they might be biased. Accordingly, reported behaviors, intentions, and attitudes give insights about general disclosure tendencies and privacy behavior. It is not clear, whether actual observable behavior would be as validly predictable through reported intentions and actions as the reported behavioral patterns. A meta-review of studies investigating the theory of planned behavior (Armitage & Conner, 2001), for instance, demonstrated that the elements of the theory of planned behavior were more reliable predictors for self-reported behavior than for observed behavior. Given that the theory of planned behavior – as already indicated by its denomination – mainly addresses reasoned and planned actions, the explanation of situational behavior in terms of a response to an external cue calls for the consideration of further factors that influence behavior. Such factors are, for instance, external conditions for making decisions with regard to a risk (e.g., ambiguous or objective conditions), the type of processing and evaluating external cues (risk-benefit evaluation, central or peripheral processing of information), intrapersonal characteristics and traits related to privacy protection behavior (e.g., need for privacy or popularity), and decision-making processes or risk-assessments (e.g., need for cognition). Therefore, the current work integrates elements of existing approaches that have been considered to explain privacy behavior into one model, serving as an overview of decisive factors for privacy-relevant decision-making as well as privacy behavior. This model combines the theory of planned behavior (Ajzen, 1991), the protection motivation theory (Rogers, 1975) and the privacy calculus (Culnan & Armstrong, 1999), consisting of intrapersonal and external factors with regard to the formation of stable as well as situational privacy behavior. The protection motivation theory (Rogers, 1975), in contrast to the theory of planned behavior (Ajzen, 1991), explicitly addresses the motivation to cope with a communicated risk based on intrapersonal factors (e.g., personal characteristics and experiences) and the characteristics of the risk-transmitting message (e.g., fear-arousing). It further addresses the individuals' evaluation of adaptive and maladaptive responses (i.e. threat and coping appraisal) and the chosen strategies for coping with the risk (i.e. adaptive and maladaptive coping modes). This theory is valuable for the present dissertation because of three reasons. First, it explicitly addresses how a communicated risk can influence appraisal, coping, and subsequent behavior. Second, it considers the characteristics of an individual who is exposed to a risk-communicating message. Third, it distinguishes between the

influence of positive (rewards) and negative (severity and vulnerability) outcomes of maladaptive (i.e. non-protective) behavior, allowing for theoretically connecting the threat appraisal (which evaluates the maladaptive coping behavior) with the privacy calculus. The privacy calculus (Culnan & Armstrong, 1999) describes individuals' weighing processes of risks and benefits associated with self-disclosure, which is the basis for the decision to disclose or withdraw personal information. The privacy calculus assumes that perceived benefit of disclosing the self might increase the likelihood that a person discloses personal information (i.e. the maladaptive coping within the PMT), whereas perceived risks might diminish a person's intention to disclose (i.e. adaptive coping within the PMT). Rohrmann (2008) and Krasnova and colleagues (2009) argued that self-disclosure risks can be subdivided into severity / perceived damage of negative consequences and the likelihood that consequences might occur. This distinction is also detectable in the protection motivation theory (Rogers, 1975), which distinguishes between severity and vulnerability related to non-protective behavior.

Accordingly, Figure 19 provides an integration of these three approaches in order to contribute to the understanding of users' privacy behavior after they were exposed to risk-related communication informing about the current state of privacy and indicating potential threats. This integration of the different approaches can help to better understand the interaction between stable traits and situational assessments of privacy threats, leading to, for instance, either protective (adaptive coping, self-withdrawal because of risks) or un-protective (maladaptive coping, self-disclosure despite risks) behavior.

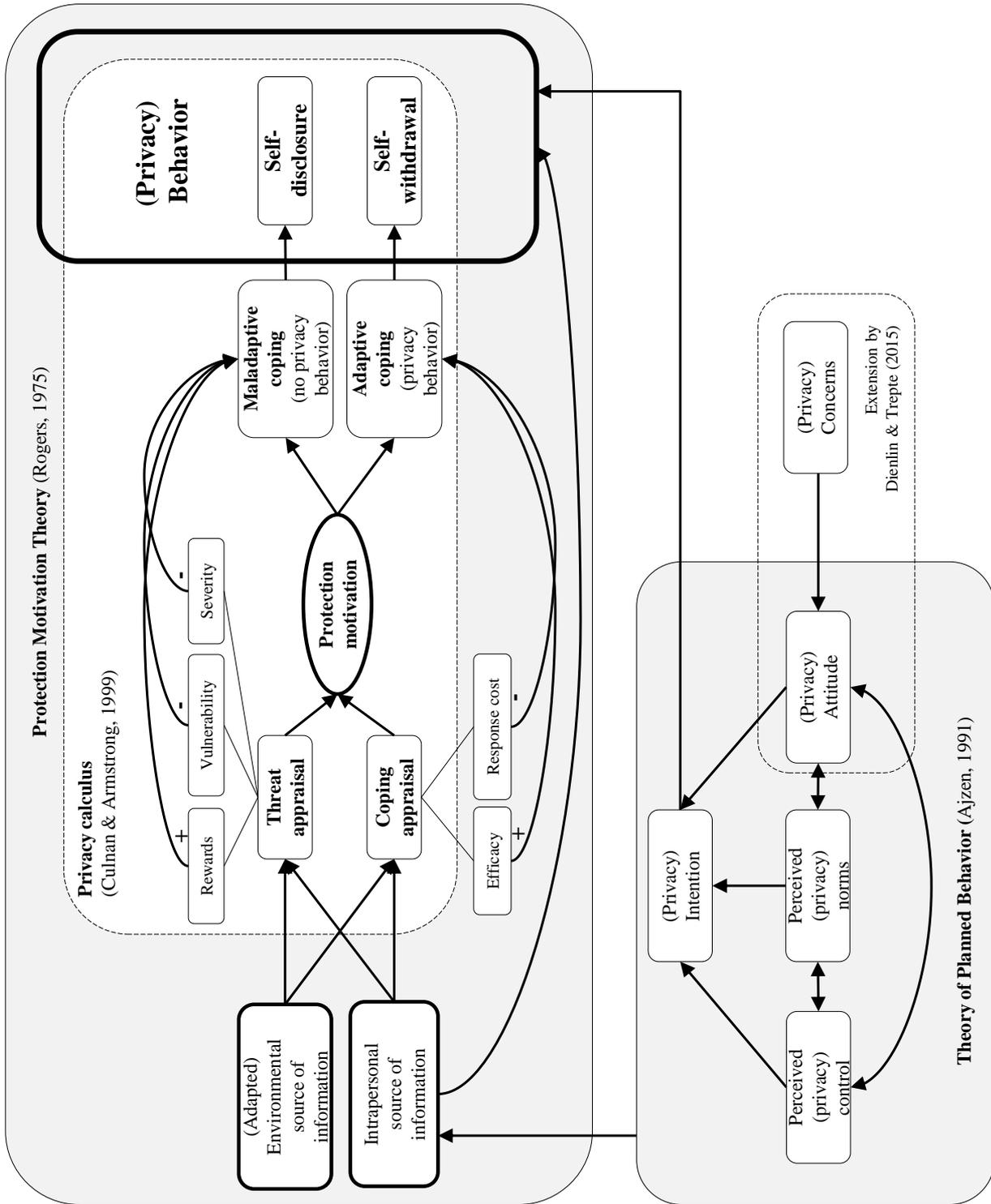


Figure 19: Integration of the protection motivation theory, the theory of planned behavior, and the privacy calculus

18 Practical Implications

The practical relevance of this work is provided through a collection of user requirements toward system-based privacy support measures and through findings of experimental investigations about the impact of particular privacy interventions on actual user behavior. These implications are advantageous for future attempts to protect and increase online privacy. Besides that, it needs to be considered that the derived implications involve new challenges as well.

Theoretical investigations with regard to systems' functionalities (Díaz Ferreyra & Schäwel, 2016; Díaz Ferreyra, Schäwel, Heisel, & Meske, 2016) as well as the results from qualitative and quantitative investigations (Studies 1 – 4) reveal a number of factors that can be considered by software-engineers and system-designers who are aiming at developing privacy protecting tools and systems. Likewise, these practical implications might also be of interest for teachers (see also Egelman et al., 2016) or politicians who might translate user requirements towards privacy protective systems into supportive guidelines or standards for privacy-aware online behavior.

In the following, the practical implications regarding (a) the functionality of privacy support and (b) the appropriate appearance of privacy support are outlined.

Functionality of privacy support

Depending on the level of adaptation of user-centered privacy support measures, features that allow for monitoring users' activities are required. In order to meet users' desire for adapted and reasonable privacy recommendations, the privacy measure has to monitor and analyze users' online actions and disclosures in order to provide adequate recommendations for action in real-time, if a privacy threat was identified (protection paradox; see Figure 20). This paradox concerning the desire to be protected and the fear of being observed by a system calls for further research. It is indispensable to relieve users from these concerns because otherwise, a privacy support system would probably not be accepted by them. As can be seen in Figure 20, the relations in the model, which is combining the underlying theories of this work (see also Figure 19), are affected by the protection paradox as well. The figure shows that users' current privacy behavior (either self-disclosure or self-withdrawal) is monitored by the system, which is going to provide adapted privacy feedback. All behaviors that have been monitored by the system need to

be analyzed against the background of data-bases, privacy rules, and algorithms (see Chapter 8), in order to assess whether the disclosed information poses a risk or not. If a risk is given and negative consequences are likely to occur, the system needs to plan the risk-related feedback which in turn can be translated into a warning message or any other risk-communicating system-based privacy recommendation, representing the environmental source of information within the protection motivation theory (see Figure 20). The generated risk-related warning will then affect users' threat appraisal, subsequent protection motivation and result in either maladaptive coping (not following the communicated warning), for instance self-disclosure, or adaptive coping (following the warning), for instance self-withdrawal. Then, the loop of monitoring, analyzing, planning, and executing will start again.

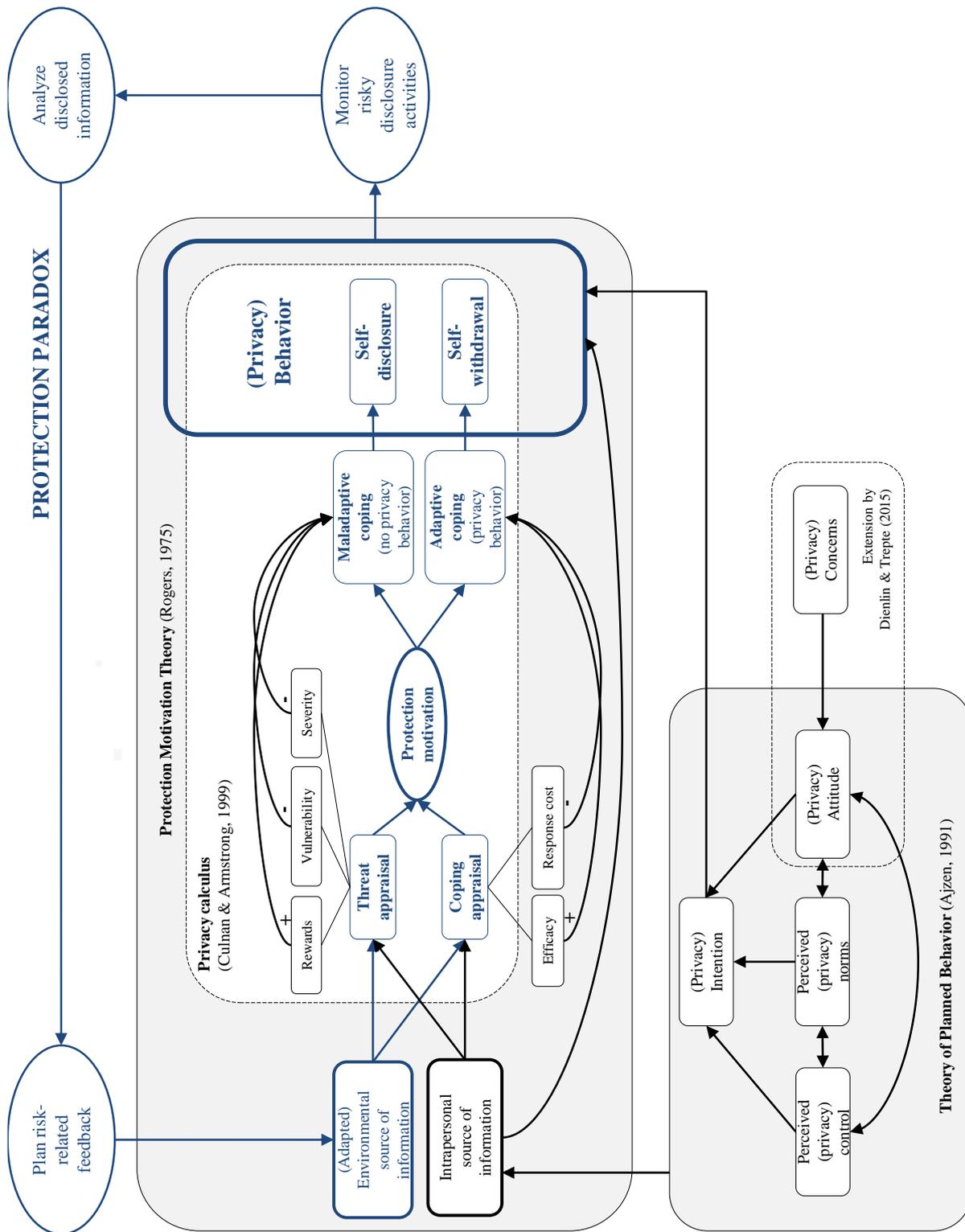


Figure 20: Integration of the protection motivation theory, the theory of planned behavior, the privacy calculus, and the protection paradox

This functionality brings ethical concerns and needs to be considered with extreme caution. In line with users' desire for transparency during an interaction with a privacy support system, users must be able to decide autonomously whether they want to utilize such a measure or not. This can be realized through providing applications with functions of monitoring and analyzing, and respective privacy support features that can be installed by the users themselves (e.g., as an ad-on for social media services). Users have to be informed about all functionalities and conditions so that they can make a reasoned and self-determined decision to utilize the protective measure, driven by the internal desire for more privacy. This functionality addresses the users' desire for making autonomous decisions, and maintaining an individual's autonomy i.e. a core element of people's privacy, see Westin, 1967). Analyzing users' behavior without permission would not meet ethical standards, even if the monitoring was to the advantage of users' privacy.

Appearance of privacy support

Besides ensuring transparency, autonomy, and adaptation, a further relevant aspect is to provide a feasible usability (e.g., through accurate functionality, appealing design, clear layout, clear affordance, reliable performance, and low effort). With regard to the style of privacy interventions, this work provided the following insights that occur to be most promising:

- (a) A consensual style of communication (see Study 3 and 4).
- (b) Visual cues that attract attention (see prompts in Study 4).
- (c) Not too extensive textual information (see Study 3).
- (d) Concrete indicators of the current privacy state (see CBC in Study 4).
- (e) Concrete explanations about the meanings of particular indicators (e.g. risk-related icons).

Visual cues are decisive for self-monitoring processes (see Chapter 8.5) that are needed in order to assess one's individual state of privacy and to modify it, if necessary (see PPM; Dienlin, 2014). It might be helpful if the current state of privacy would not only be indicated through three distinct levels (low, moderate, high risk) as it was done in Study 4, but through a continuous and more fine-grained visualization in which improvements or deteriorations are more directly visible. Concerning the content of a

system-based privacy intervention it seems feasible to concentrate on risk-communication with regard to potential outcomes affecting the horizontal dimension of privacy (in line with identified motives for opting-out from an SNS, namely, protection against personal attacks, avoidance of distraction, and avoidance of pressure) and to specify and communicate short-term as well as long-term consequences. Further investigations should also consider providing positive feedback to users if a privacy recommendation was accepted and implemented into action (although, as already mentioned, the increase in the privacy level visualized through green color already displays a positive enhancement). In sum, the current work provides several practical implications and calls for further research at the same time.

19 Ethical implications

Providing system-based privacy interventions implies that users' behavior is guided by an external entity. This becomes an issue, when provided support deprives users' personal freedom of taking self-determined decisions. If providers of privacy protecting tools were adhering to extreme paternalistic approaches, even by aiming at acting in the interest of users, this would contradict basic ethical principles of not invading people's right to act self-determined. In this case, even if the provider or the tool was asserting to be driven by the intention to protect the users so that their privacy and security can be ensured, this approach would be as questionable as manipulating activities driven by detrimental motivations to the disadvantages of users. Hence, it is extremely important to transparently inform the users about all conditions and functionalities of the protective measure (see Study 1), and to leave the decision to the user whether (a) to use a privacy support measure that monitors one's online behavior and (b) whether to follow the provided recommendation.

Through raising users' awareness by means of privacy interventions as presented in this work, users still have the freedom to decide on their own whether to act in accordance to the system-based suggestion or to continue disclosure as before. Users would not be deprived of their autonomy, mirroring a decisive principle in the area of persuasive research (see Chapter 8), and especially in the realm of privacy protection in which autonomy and self-determination play major roles for users' well-being and their right and need to maintain personal privacy (see Chapter 7).

20 Limitations

The limitations of each empirical study were discussed already. However, there are also some overarching limitations that will be referred to in the following.

The most central limitation pertains to the basic idea of providing users with adapted system-based privacy support measures that are able to monitor activities on SNSs with the goal to provide privacy recommendations entailing that the user discloses less personal information. The criticism to this approach might be that providers of SNSs probably would not like to provide tools for decreasing the extent of disclosed information by users, which aggravates the actual implementation of such tools in reality. In order to counteract this problem, this work suggests providing applications that can be installed by users themselves, independently from a particular social network but rather as an ad-on, which is able to regulate disclosures across different SNSs and other social media offers.

Accordingly, the opportunity to decide individually whether to install and use an application providing adapted privacy support, brings a barrier of engaging in online privacy protection and installing the measure at the same time. Since people tend to avoid effortful activities, it might be a hurdle for them to download and install the protective measure. Thus, even before the actual engagement with the protective measure is going to start, providers of the supportive measure would need to emphasize the advantages of using the system in order to give users the opportunity to engage in online privacy protection.

A further limitation lies in a paradox with regard to the empirical investigations, more precisely, in the instructions to the users in experimental settings in which the impact of persuasive system-based privacy interventions was examined. The users were told that they would test a new SNS environment by means of conducting a registration process for signing in to the social network. Although they were informed about the fact that they do not need to fill in all fields of the registration form, it might have been confusing for participants, on the one hand, being asked to provide information, and on the other hand, being warned about sensitive information disclosure.

21 Future Directions

This work addressed online privacy behavior and self-disclosure activities related to potential privacy risks on SNSs. However, the underlying concept of system-based privacy support can be attributed to many other areas of application as well. Experimental investigations in this work were built on a registration form for an SNS as pivotal measurement. Basically, all online platforms and networks (e.g., LinkedIn, Xing, Printerest, Instagram, Airbnb) require personal user data through a registration form, hence, this approach can be expanded to several other application fields. It is worthwhile to examine users' privacy behavior across different social media platforms in order to find out whether specific concerns relate to specific networks or whether they are overarching. This is especially interesting against the background of the findings of Study 2. In this study, users reported their intention to opt-out from the social network Facebook due to protection and withdrawal reasons. Strikingly, although this measure might prevent from privacy harms on the SNS Facebook, other platforms still bear privacy risks for users. Hence, it is open to question whether users who intend to opt-out from one network are exclusively concerned about privacy threats related to that specific network or whether they do not know similar measures for other networks they are registered in, or whether opting-out from one network would be the first step for further withdrawing from other networks.

Besides considering different privacy contexts (e.g., different online platforms), future studies should also focus on varying kinds of concerns, relating to different contexts of potential privacy threats. This thought arises from Study 1. Initially, interviewees in this study reported to be especially concerned about privacy harms related to horizontal privacy (i.e. other users; see Bartsch & Dienlin, 2016) and stated to somehow accept the fact that vertical privacy seems to be not protectable (i.e. providers of networks; see Bartsch & Dienlin, 2016). However, after explicitly addressing the concept of system-based privacy protection measures, users reflected more about vertical privacy issues and became increasingly concerned about the underlying mechanisms. Accordingly, it is conceivable, that users who are in general more afraid of security breaches based on website providers or companies would be more skeptical towards this tool than users being more afraid about harms related to horizontal privacy. In line with this, the expression and origin of users' privacy concerns might have an influence on the

motivation and intention to utilize a technical support measure and on the impact of that measure. To be more precise, users' who are more afraid of negative experiences with regard to the horizontal level of privacy, might wish for protective measures that focus on reducing risks such as the occurrence of cyber-mobbing, firestorms, being embarrassed, personally attacked, or exposed (referring to psychological privacy). In contrast, users who are more concerned about privacy harms based on intrusions from the government, institutions, or social network providers, might be more motivated to use privacy protection measures focusing on protection against informational privacy-related threats such as misuse of private data or data theft. Accordingly, these users might be more skeptical regarding a privacy protection tool that needs to monitor their disclosure behavior in order to provide adapted privacy recommendations (see Study 1). Future research should address this dilemma by also investigating whether people with a high need for vertical privacy might be more attracted by self-driven approaches (e.g., opting-out or increasing literacy), whereas people having stronger concerns regarding horizontal privacy might consider system-based privacy support measures more likely in order to avoid psychological privacy-related negative consequences based on other users.

One limitation outlined with regard to Studies 3 and 4 was that users' privacy behavior was investigated based on one single experimental investigations and the explained variance of observed behavior was not really high. Thus, in order to explain more variance in privacy behavior and to derive even more comprehensive conclusions with regard to future privacy preventing measures, research should focus on a long-term investigation of intrapersonal and environmental factors which influence users' online privacy decisions and behavior. This dissertation suggests combining the theory of planned behavior (Ajzen, 1991) with the protection motivation theory (Rogers, 1975) and the privacy calculus (Culnan & Armstrong, 1999) in order to comprehensively address situational and stable factors that impact users' online privacy behavior.

Thereby, the privacy calculus should decompose risks into severity and likelihood of negative consequences (as already suggested by Rogers, 1975; Krasnova et al., 2009). Likewise, it might be feasible to decompose anticipated benefits in terms of distinguishing between the level of positivity and the likelihood that benefits will arise as well. This granularity might allow for more fine-grained conclusions about users' online privacy decision-makings and subsequent behaviors, which can in turn be used

for more sophisticated elicitation of requirements with regard to system-based privacy protection.

22 Conclusion

The constantly increasing demand for online privacy protection measures in social media environments requires a comprehensive understanding of the dynamics of users' online (privacy) behavior and their concurring needs of taking advantages of social media offers due to self-presentation and self-disclosure and the desire of being an autonomous and self-determined individual without privacy risks. The interdependencies between users' psychological needs, their requirements towards privacy protection measures, and the technical challenges of providing adapted privacy support call for interdisciplinary approaches addressing this complex field of research from both, a user-centered and a system-based perspective. The present dissertation provides a valuable foundation in terms of investigations of the influence of system-based privacy interventions on users' disclosure and withdrawal behavior in an online environment under consideration of their intrapersonal characteristics and needs. Results suggest that persuasive privacy support interventions, informing about current privacy states in real-time, can decrease the amount of disclosed sensitive information. This result was revealed in two experimental studies in the course of this work, which investigated the impact of system-based persuasive privacy interventions. However, this promising result revealed a new challenge as well – the emerging paradox regarding the desire for individual and adapted privacy support and the concern about the monitoring actions of the protection system. These promising and challenging issues can be addressed in future research on attempts of empowering users of SNSs in self-determined and supported online privacy behaviors.

References

- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.*, 50(3), 44:1–44:41. doi:10.1145/3054926
- Acquisti, A., Taylor, C. R., & Wagman, L. (2016). *The Economics of Privacy* (SSRN Scholarly Paper No. ID 2580411). Rochester, NY: Social Science Research Network. Retrieved from <https://papers.ssrn.com/abstract=2580411>
- Acquisti, A., John, L. K., Loewenstein, G. (2012): The Impact of Relative Standards on the Propensity to Disclose. In: *Journal of Marketing Research* 49(2), 160–174. doi:10.1509/jmr.09.0215
- Acquisti, A. (2009), Nudging privacy: the behavioral economics of personal information. *IEEE security & privacy*, 7(6).
- Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21–29). New York, NY, USA: ACM. doi:10.1145/988772.988777
- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Lecture Notes in Computer Science: Vol. 4678. Privacy enhancing technologies*. doi:10.1007/11957454_3
- Ahn, H., Kwolek, E. A., & Bowman, N. D. (2015). Two faces of narcissism on SNS: The distinct effects of vulnerable and grandiose narcissism on SNS privacy control. *Computers in Human Behavior*, 45, 375–381. doi:10.1016/j.chb.2014.12.032
- Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research*, 29, 350–353. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=buh&AN=7705771&site=ehost-live&scope=site>
- Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, 26(9), 1113–1127. doi:10.1080/08870446.2011.613995

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. doi:10.1016/0749-5978(91)90020-T
- Alavi, R., Islam, S., & Mouratidis, H. (2014). A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. In T. Tryfonas & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 297–305). Springer International Publishing.
- Altman, D. G (1991), *Practical statistics for medical research* (Boca Raton: CRC Press).
- Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole.
- Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. Oxford, England: Holt, Rinehart & Winston.
- Ames, D. R., Rose, P., & Anderson, C. P. (2006). The NPI-16 as a short measure of narcissism. *Journal of Research in Personality*, 40(4), 440–450. doi:10.1016/j.jrp.2005.03.002
- An, J., Kwak, H., & Jansen, B. J. (2017), Automatic generation of personas using youtube social media data. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.
- Armitage, C. J., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: a meta analytic review. *The British Journal of Social Psychology*, 40(Pt 4), 471–499.
- Archer, R. L. (1980). *Self-Disclosure and Attraction: A Self-Perception Analysis*. Retrieved from <https://eric.ed.gov/?id=ED195897>
- Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological Monographs: General and Applied*, 70(9), 1-70. doi:10.1037/h0093718
- Asch, M. J. (1951). Nondirective teaching in psychology: An experimental study. *Psychological Monographs: General and Applied*, 65, i-24. doi:10.1037/h0093595
- Attrill, A. (2015). *Cyberpsychology*. Oxford, United Kingdom: Oxford University Press.

- Ayalon, O., Toch, E., Hadar, I., & Birnhack, M. (2017). How developers make design decisions about users' privacy. The place of professional communities and organizational climate. In C. P. Lee, S. Poltrock, L. Barkhuus, M. Borges, & W. Kellogg (Eds.). *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17 Companion* (pp. 135–138). doi:10.1145/3022198.3026326
- Baek, Y. M., Kim, E.-M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56. doi:10.1016/j.chb.2013.10.010
- Baker, R. K., & White, K. M. (2010). Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. *Computers in Human Behavior*, *26*(6), 1591–1597, doi:10.1016/j.chb.2010.06.006
- Balebako, R., & Cranor, L. F. (2014). Improving app Privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy*, *12*(4), 55–58. doi:10.1109/MSP.2014.70
- Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., Cranor, L. F., Sadeh, N. M. (2011). *Nudging Users Towards Privacy on Mobile Devices*.
- Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York, NY, US: W H Freeman/Times Books/ Henry Holt & Co.
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter?: Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*, 1–21. doi:10.1016/j.im.2015.08.001
- Bang, M., Torstensson, C., & Katzeff, C. (2006). The PowerHhouse: A Persuasive Computer Game Designed to Raise Awareness of Domestic Energy Consumption. In W. A. IJsselsteijn, Y. A. W. de Kort, C. Midden, B. Eggen, & E. van den Hoven (Eds.), *Persuasive Technology* (pp. 123–132). Springer Berlin Heidelberg.
- Barber, B. (1983). *The Logic and Limits of Trust*. Rutgers University Press.
- Bargh, J. A. (1997). The automaticity of everyday life. In R. S. Wyer, Jr. (Ed.), *Advances in social cognition, Vol. 10. The automaticity of everyday life: Advances in social cognition, Vol. 10*, pp. 1-61. Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers.

- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). doi:10.5210/fm.v11i9.1394
- Barry, C. T., Doucette, H., Della Loflin, C., Rivera-Hudson, N., & Herrington, L. L. (2017). “Let me take a selfie”: Associations between self-photography, narcissism, and self-esteem. *Psychology of Popular Media Culture*, 6(1), 48–60. doi:10.1037/ppm0000089
- Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147–154. doi:10.1016/j.chb.2015.11.022
- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication*, 67(1), 26–53. doi:10.1111/jcom.12276
- Baumeister, R. F., Heatherton, T. F., & Tice, D. M. (1994). *Losing control: How and why people fail at self-regulation*. San Diego, CA, US: Academic Press.
- Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, 64(4), 635–657. doi:10.1111/jcom.12106
- Beaver, K., Barnes, J. C., & Boutwell, B. (2014). *The Nurture Versus Biosocial Debate in Criminology: On the Origins of Criminal Behavior and Criminality*. London. doi:10.4135/9781483349114
- Bechara, A. (2005). Decision making, impulse control and loss of willpower to resist drugs: a neurocognitive perspective. *Nature Neuroscience*, 8, 1458–1463. doi:10.1038/nn1584
- Belk, M., Germanakos, P., Fidas, C., & Samaras, G. (2014). A Personalization Method Based on Human Factors for Improving Usability of User Authentication Tasks. In V. Dimitrova, T. Kuflik, D. Chin, F. Ricci, P. Dolog, & G.-J. Houben (Eds.), *User Modeling, Adaptation, and Personalization* (pp. 13–24). Springer International Publishing.
- Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenber, K., & Stamatiou, Y. (2014). User acceptance of privacy-ABCs: An exploratory study. In T. Tryfonas & I. Askoxylakis (Eds.), *Lecture Notes in Computer Science: Vol. 8533. Human Aspects*

of Information Security, Privacy, and Trust (pp. 375-386). doi:10.1007/978-3-319-07620-1_33

- Bergman, S. M., Fearington, M. E., Davenport, S. W., & Bergman, J. Z. (2011). Millennials, narcissism, and social networking: What narcissists do on social networking sites and why. *Personality and Individual Differences*, *50*(5), 706–711. doi:10.1016/j.paid.2010.12.022
- Bertrams, A., & Dickhäuser, O. (2009). Messung dispositioneller Selbstkontroll-Kapazität. *Diagnostica*, *55*(1), 2–10. doi:10.1026/0012-1924.55.1.2
- Beyth-Marom, R., & Fischhoff, B. (1997). Adolescents' decisions about risks: A cognitive perspective. In J. Schulenberg, J. L. Maggs, & K. Hurrelmann (Eds.), *Health risks and developmental transitions during adolescence* (pp. 110-135). New York, NY, US: Cambridge University Press.
- Bierhoff, H.-W. & Herner, M. J. (2006). Narzissmus. In H.-W. Bierhoff & D. Frey (Hrsg.), *Handbuch der Sozialpsychologie und Kommunikationspsychologie* (S. 57-62). Göttingen: Hogrefe.
- Birnholtz, J., Burke, M., & Steele, A. (2017). Untagging on social media: Who untags, what do they untag, and why? *Computers in Human Behavior*, *69*, 166–173. doi:10.1016/j.chb.2016.12.008
- Błachnio, A., Przepiorka, A., Bałakier, E., & Boruch, W. (2016). Who discloses the most on Facebook? *Computers in Human Behavior*, *55*, 664–667. doi:10.1016/j.chb.2015.10.007
- Błachnio, A., Przepiorka, A., Boruch, W., & Bałakier, E. (2016). Self-presentation styles, privacy, and loneliness as predictors of Facebook use in young people. *Personality and Individual Differences*, *94*, 26–31. doi:10.1016/j.paid.2015.12.051
- Blank, M. B., Himelhoch, S. S., Balaji, A. B., Metzger, D. S., Dixon, L. B., Rose, C. E., ... Heffelfinger, J. D. (2014). A Multisite Study of the Prevalence of HIV With Rapid Testing in Mental Health Settings. *American Journal of Public Health*, *104*(12), 2377–2384. doi:10.2105/AJPH.2013.301633
- boyd, D. (2014). It's complicated: The social lives of networked teens. *Yale University Press*.

- boyd, d. m., and Marwick, A. (2011). Social Steganography: Privacy in Networked Publics. International Communication Association Conference, 26-30 (Boston, MA: ICA), 93.
- boyd, d. m., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15(8). doi:10.5210/fm.v15i8.3086
- boyd, d. m. (2010), Risk reduction strategies on Facebook. Retrieved from <http://www.zephorio.org/thoughts/archives/2010/11/08/risk-reduction-strategies-on-facebook.html>
- boyd, d. m., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230. doi:10.1111/j.1083-6101.2007.00393.x
- Brand, M., Heinze, K., Labudda, K., & Markowitsch, H. J. (2008). The role of strategies in deciding advantageously in ambiguous and risky situations. *Cognitive Processing*, 9(3), 159–173. doi:10.1007/s10339-008-0204-4
- Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, 4(3), 340–347. doi:10.1177/1948550612455931
- Brehm, J. W. (1966). A theory of psychological reactance. New York, NY: Academic Press.
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165. doi:10.1002/asi.20459
- Büchi, M., Just, N., & Latzer, M. (2016). Modeling the second-level digital divide: A five- country study of social differences in Internet use. *New Media & Society*, 18(11), 2703–2722. doi:10.1177/1461444815604154
- Buffardi, L. E., & Campbell, W. K. (2008). Narcissism and social networking web sites. *Personality and Social Psychology Bulletin*, 34(10), 1303–1314. doi:10.1177/0146167208320061
- Bujała, A. (n.d.). Gender differences in Internet usage (2011). *Acta Universitatis Lodzianensis. Folia Sociologica, Acta Universitatis Lodzianensis, Folia Sociologica nr*

- 43/2012. Retrieved from
http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.hdl_11089_2647
- Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association*, 6(1), 206–249. doi:10.1080/23808985.1982.11678499
- Buss, A. (2001). *Psychological dimensions of the self*. Thousand Oaks, CA, US: Sage Publications, Inc.
- Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology*, 42(1), 116–131. doi:10.1037/0022-3514.42.1.116
- Carenini, G. (2001). An Analysis of the Influence of Need for Cognition on Dynamic Queries Usage. In *CHI '01 Extended Abstracts on Human Factors in Computing Systems* (pp. 383–384). New York, NY, USA: ACM. doi:10.1145/634067.634293
- Carpenter, A., & Greene, K. (2016). Social penetration theory. In C. R. Berger & M. E. Roloff (Eds.), *The international encyclopedia of interpersonal communication* (1st ed., pp. 1-4). Hoboken, NJ: Wiley-Blackwell. doi:10.1002/9781118540190.wbeic0160
- Cavoukian, A. (2011). Privacy by Design: Best Practices for Privacy and the Smart Grid. In N. Pohlmann, H. Reimer, & W. Schneider (Eds.), *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference* (pp. 260–270). Wiesbaden: Vieweg+Teubner. doi:10.1007/978-3-8348-9788-6_25
- Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291–302. doi:10.1016/j.chb.2017.01.003
- Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting Oneself Online: The Effects of Negative Privacy Experiences on Privacy Protective Behaviors. *Journalism & Mass Communication Quarterly*, 93(2), 409–429. doi:10.1177/1077699016640224
- Chen, J. V., Widjaja, A. E., & Yen, D. C. (2015). Need for affiliation, need for popularity, self-esteem, and the moderating effect of big five personality traits affecting individuals' self-disclosure on Facebook. *International Journal of Human-Computer Interaction*, 31(11), 815–831. doi:10.1080/10447318.2015.1067479

- Chen, J. V., Chen, C. C., & Yang, H.-H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management & Data Systems*, 108(1), 87–106. doi:10.1108/02635570810844106
- Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology*, 58(6), 1015-1026. doi:10.1037/0022-3514.58.6.1015
- Chester, A., & Bretherton, D. (2007). *Impression management and identity online*. Oxford University Press. Retrieved from <https://researchbank.rmit.edu.au/view/rmit:9849>
- Child, J. T., Petronio, S., Agyeman-Budu, E. A., & Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior*, 27(5), 2017-2027. doi:10.1016/j.chb.2011.05.009
- Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5), 987–995. doi:10.1016/j.chb.2010.02.012
- Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of adolescent research*, 27(6), 714-731. doi:10.1177/0743558411432635
- Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, 12(3), 341–345. doi:10.1089/cpb.2008.0226
- Cialdini, R. B., Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, 55(1), 591–621. doi:10.1146/annurev.psych.55.090902.142015
- Clarke, R. (2006). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Available at <http://www.rogerclarke.com/DV/intro.html> (accessed: 4th November, 2018)
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale, NJ: Erlbaum.

- Coventry L.M., Jeske D., Blythe J.M., Turland J & Briggs P. (2016). Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. *Front. Psychol.* 7:1341. doi: 10.3389/fpsyg.2016.01341
- Cranor, L. F., Arjula, M., & Guduru, P. (2002). Use of a P3P user agent by early adopters. In S. Jajodia, & P. Samarati (Eds.), *Proceeding of the ACM workshop on Privacy in the Electronic Society - WPES '02* (pp. 1–10). doi:10.1145/644527.644528
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. doi:10.1287/orsc.10.1.104
- Curseu, P. L. (2006). Need for cognition and rationality in decision-making. *Studia Psychologica*, 48(2), 141.
- Dabas, P., & Sharma, S. (2018). Privacy and security issues in social networks with prevailing privacy preserving techniques. *Journal of Network Communications and Emerging Technologies*, 8(2), 54–56. Retrieved from <http://www.jncet.org>
- D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., De Montjoye, Y.-A., & Bourka, A. (2015). Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. *arXiv preprint arXiv:1512.06000*.
- Das, S., Echambadi, R., McCardle, M., & Lockett, M. (2003). The effect of interpersonal trust, Need for Cognition, and social loneliness on shopping, information seeking and surfing on the web. *Marketing Letters*, 14(3), 185–202. doi:10.1023/A:1027448801656
- Davidson, A. R., & Jaccard, J. J. (1979). Variables that moderate the attitude–behavior relation: Results of a longitudinal survey. *Journal of Personality and Social Psychology*, 37(8), 1364-1376. doi:10.1037/0022-3514.37.8.1364
- Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x
- DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

- Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, *11*(4), 227–268. doi:10.1207/S15327965PLI1104_01
- Degeling, M., Lentzsch, C., Nolte, A., Herrmann, T., & Loser, K-U.(2016). Privacy by socio-technical design: A collaborative approach for privacy friendly system design. *Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing* (pp. 502–505). doi:10.1109/CIC.2016.077
- Deterding, S., 2014, Eudaimonic design, or: six invitations to rethink gamification. In *Rethinking Gamification*, edited by M. Fuchs, S. Fizek, P. Ruffino, and N. Schrape (Lüneburg: meson press), pp. 305-331
- Deterding, S., Dixon, D., Khaled, R., & Nacke, L (2011). From game design elements to gamefulness: defining "Gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, edited by A. Lugmayr, H. Franssila, C. Safran, and I. Hammouda, (New York, New York, USA: ACM).
- Devos-Comby, L., & Salovey, P. (2002). Applying persuasion strategies to alter HIV-relevant thoughts and behavior. *Review of General Psychology*, *6*(3), 287-304. doi:10.1037/1089-2680.6.3.287
- Díaz Ferreyra, N. E., & Schäwel, J. (2016). Self-disclosure in social media: An opportunity for self-adaptive systems. *Joint Proceedings of the Workshops and Doctoral Symposium on Requirements Engineering - Foundation of Software Quality (REFSQ 2016)*.
- Díaz Ferreyra, N. E., Schäwel, J., Heisel, M., & Meske, C. (2016). Addressing self-disclosure in social media: An instructional awareness approach. In *Proceedings of the 2nd ACS/IEEE International Workshop on Online Social Networks Technologies (OSNT)*.
- D. Dickenberger (2006). *Reaktanz*. In: Hans-Werner Bierhoff, Dieter Frey (Hrsg.): *Handbuch der Sozialpsychologie und Kommunikationspsychologie*. Hogrefe, S. 96–102.
- Dienlin, T. (2017). *The psychology of privacy: Analyzing processes of media use and interpersonal communication* (Doctoral Thesis, University Hohenheim, Stuttgart, Deutschland). Retrieved from <http://opus.uni-hohenheim.de/volltexte/2017/1315/>

- Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, 21(5), 368–383.
doi:10.1111/jcc4.12163
- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past?: An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285–297. doi:10.1002/ejsp.2049
- Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Half, M. Herz, & J.-M. Mönig (Eds.), *Medien und Privatheit [Media and privacy]* (pp. 105-122). Passau, Germany: Stutz.
- Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, 23, 413–422. doi:10.1080/01449290410001715723
- Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior*, 60, 508–513.
doi:10.1016/j.chb.2016.02.010
- Egelman, S., Bernd, J., Friedland, G., & Garcia, D. (2016). The teaching privacy curriculum. In C. Alphonse, J. Tims, M. Caspersen, & S. Edwards (Eds.), *Proceedings of the 47th ACM Technical Symposium on Computing Science Education - SIGCSE '16* (pp. 591–596). New York, New York, USA: ACM Press.
doi:10.1145/2839509.2844619
- Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *ACM SIGCAS Computers and Society*, 45(1), 22-28. doi:10.1145/2738210.2738215
- Egelman, S., Tsai, J., Cranor, L. F., & Acquisti, A. (2009). Timing is Everything?: The Effects of Timing and Placement of Online Privacy Indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 319–328). New York, NY, USA: ACM. doi:10.1145/1518701.1518752
- Ellison, N. B., Gray, R., Lampe, C., & Fiore, A. T. (2014). Social capital and resource requests on Facebook. *New Media & Society*, 16(7), 1104–1121.
doi:10.1177/1461444814543998

- Ellison, N. B., & boyd, d. m. (2013). Sociality through social network sites. In W. H. Dutton (Ed.), *The Oxford Handbook of Internet Studies* (pp. 151–172). Oxford, England: Oxford University Press. doi:10.1093/oxfordhb/9780199589074.013.0008
- Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social Web* (pp. 19–32). Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6
- Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society*, 13(6), 873–892. doi:10.1177/1461444810385389
- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook “Friends:” Social Capital and College Students’ Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, 12(4), 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x
- Ent, M. R., Baumeister, R. F., & Tice, D. M. (2015). Trait self-control and the avoidance of temptation. *Personality and Individual Differences*, 74, 12–15. doi:10.1016/j.paid.2014.09.031
- Eppler, M. J., & Mengis, J. (2004). The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines. *The Information Society*, 20(5), 325–344. doi:10.1080/01972240490507974
- Epstein, R. (1996). *Cognition, Creativity, and Behavior: Selected Essays*. Westport, CT: Praeger.
- European Commission. (2015). Special Eurobarometer No. 423: Cyber security. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf
- Fazio, R. H. (2007). Attitudes as Object–Evaluation Associations of Varying Strength. *Social Cognition*, 25(5), 603–637. doi:10.1521/soco.2007.25.5.603
- Fazio, R. H.; Roskos-Ewoldsen, D. R., & Powell, M. C. (1994): Attitudes, perception, and attention. In: *The heart’s eye: Emotional influences in perception and attention*. San Diego, CA, US: Academic Press, S. 197–216.

- Finneran, C. M., & Zhang, P. (2005). Flow in computer-mediated environments: Promises and challenges. *Communications of the Association for Information Systems, 15*(1), 82–101. doi:10.17705/1CAIS.01504
- Fischer-Hübner, S. (2001). IT-security and privacy: Design and use of privacy-enhancing security mechanisms. *Lecture Notes in Computer Science: Vol. 1958*. Berlin, Germany: Springer.
- Fishbein, M. (1979). A theory of reasoned action: Some applications and implications. In H. Howe & M. Page (Eds.), *Nebraska Symposium on Motivation* (pp. 65–116). Lincoln: University of Nebraska Press.
- Fitzsimons, G. J. & Lehmann, D. R. (2004). Reactance to recommendations: When unsolicited advice yields contrary responses. *Marketing Science, 23*(1), 82–94. <https://doi.org/10.1287/mksc.1030.0033>
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160. doi:10.1016/j.chb.2008.08.006
- Fogg, B. J. (2009). A behavior model for persuasive design. In S. Chatterjee & P. Dev (Eds.), *Proceedings of the 4th International Conference on Persuasive Technology* (Article No. 40). New York, NY: ACM. doi:10.1145/1541948.1541999
- Fogg, B. J. (2003). Persuasive technology: Using computers to change what we think and do. *Ubiquity, 2003(December)*, Article No. 5. doi:10.1145/764008.763957
- Fogg, B. J. (2002). Persuasive technology. Using computers to change what we think and do. *Ubiquity, 89–120*. doi:10.1145/764008.763957
- Förster, J. & Denzler, M. (2006). Selbst-Regulation. In W. Bierhoff & D. Frey (Eds.), *Handbuch der Psychologie, Band „Sozialpsychologie“* (S. 128-132). Berlin: Hogrefe.
- Fox, J., & Rooney, M. C. (2015). The Dark Triad and trait self-objectification as predictors of men's use and self-presentation behaviors on social networking sites. *Personality and Individual Differences, 76*, 161–165. doi:10.1016/j.paid.2014.12.017

- Freud, A. (1946). *The ego and the mechanisms of defence*. Oxford, England: International Universities Press.
- Fullwood, C., Nicholls, N., & Makichi, R. (2015). We've got something for everyone: How individual differences predict different blogging motivations. *New Media and Society*, 17(9), 1583-1600.
- Furby, L., & Beyth-Marom, R. (1992). Risk taking in adolescence: A decision-making perspective. *Developmental review*, 12(1), 1-44. doi:10.1016/0273-2297(92)90002-j
- Ghasemi, A., & Zahediasl, S. (2012). Normality Tests for Statistical Analysis: A Guide for Non-Statisticians. *International Journal of Endocrinology and Metabolism*, 10(2), 486–489. <https://doi.org/10.5812/ijem.3505>
- Girden, E. R. (1994). *ANOVA: repeated measures* (3. [Dr.]). *Sage university papers / Series quantitative applications in the social sciences: Vol. 84*. Newbury Park: Sage Publ.
- Girden, E. (1992). *ANOVA*. 2455 Teller Road, Thousand Oaks California 91320 United States of America: SAGE Publications, Inc. doi:10.4135/9781412983419
- Goffman, E. (1959). *Wir alle spielen Theater: Die Selbstdarstellung im Alltag* (6. Auflage). München: Piper.
- Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks: The Facebook case. In *Proceedings of the 2005 ACM Workshop on Privacy in the electronic society* (pp. 71–80). New York, NY: ACM.
- Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, 94, 19–28. doi:10.1016/j.dss.2016.10.002
- Gunther, A. C., & Mundy, P. (1993). Biased optimism and the third-person effect. *Journalism & Mass Communication Quarterly*, 70(1), 58–67. doi:10.1177/107769909307000107
- Haferkamp, N., & Krämer, N. C. (2011). Social comparison 2.0: examining the effects of online profiles on social-networking sites. *Cyberpsychology, Behavior and Social Networking*, 14(5), 309–314. doi:10.1089/cyber.2010.0120
- Haferkamp, N. (2010). *Sozialpsychologische Aspekte im Web 2.0: Impression Management und sozialer Vergleich*. Stuttgart: Kohlhammer W., GmbH.

- Halmos, P. (1953). Personal Involvement in Learning about Personality. *The Sociological Review*, *1*(1_suppl), 21–35. doi:10.1111/j.1467-954X.1953.tb03055.x
- Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. In *2014 47th Hawaii International Conference on System Sciences* (pp. 3025–3034). doi:10.1109/HICSS.2014.377
- Haugtvedt, C. P., & Petty, R. E. (1992). Personality and persuasion: Need for cognition moderates the persistence and resistance of attitude changes. *Journal of Personality and Social Psychology*, *63*(2), 308–319. doi:10.1037/0022-3514.63.2.308
- Hausawi, Y. M., & Allen, W. H. (2015). Usable-Security Evaluation. In T. Tryfonas & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (pp. 335–346). Springer International Publishing.
- Hausawi, Y. M., & Allen, W. H. (2014). Usability and Security Trade-off: A Design Guideline. In *Proceedings of the 2014 ACM Southeast Regional Conference* (pp. 21:1–21:6). New York, NY, USA: ACM. doi:10.1145/2638404.2638483
- Hausman, D. M., & Welch, B. (2010). Debate: To Nudge or Not to Nudge*. *Journal of Political Philosophy*, *18*(1), 123–136. doi:10.1111/j.1467-9760.2009.00351.x
- Heirman, W., Walrave, M., Vermeulen, A., Ponnet, K., Vandebosch, H., Van Ouytsel, J., & Van Gool, E. (2016). An open book on Facebook? Examining the interdependence of adolescents' privacy regulation strategies. *Behaviour & Information Technology*, *35*(9), 706-719.
- Hendin, H. M., & Cheek, J. M. (1997). Assessing hypersensitive narcissism: A reexamination of Murray's narcissism scale. *Journal of Research in Personality*, *31*, 588–599. doi:10.1006/jrpe.1997.2204
- Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, *53*, 1–17. doi:10.1016/j.cose.2015.05.002
- Ho, S. S., Lwin, M. O., Yee, A. Z. H., & Lee, E. W. J. (2017). Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 572–579. doi:10.1089/cyber.2017.0061

- Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). doi:10.5817/CP2016-4-7
- Hofmann, W., Friese, M., & Strack, F. (2009). Impulse and Self-Control From a Dual-Systems Perspective. *Perspectives on Psychological Science*, *4*(2), 162–176. doi:10.1111/j.1745-6924.2009.01116.x
- Hofstra, B., Corten, R., & van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, *60*, 611–621. doi:10.1016/j.chb.2016.02.091
- Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society*, *30*(6), 377–386. doi:10.1177/0270467610385893
- Hondori, J. B., Javanshir, H., & Rabani, Y. (2013). Customer preferences using conjoint analysis: A case study of Auto industry. *Management Science Letters*, *3*, 2577–2580. doi:10.5267/j.msl.2013.09.015
- Hong, W., & Thong, J. Y. L. (2013). *Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies* (SSRN Scholarly Paper No. ID 2229627). Rochester, NY: Social Science Research Network. Retrieved from <https://papers.ssrn.com/abstract=2229627>
- Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. *Psychometrika*, *30*(2), 179–185. doi:10.1007/BF02289447
- Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion; psychological studies of opinion change*. New Haven, CT, US: Yale University Press.
- Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. doi:10.1080/15252019.2010.10722168
- Hughes-Roberts, T. (2013). Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behaviour? In *2013 International Conference on Social Computing* (pp. 909–912). <https://doi.org/10.1109/SocialCom.2013.140>

- Internet Crime Complaint Center (2016). 2016 Internet Crime Report. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf
- Jackson, M. A. (2001). *Problem frames: analysing and structuring software development problems*. Harlow, England; New York: Addison-Wesley/ACM Press.
- Jędruszczak, K. (2005). Prywatność jako potrzeba w ramach koncepcji siebie. *Roczniki Psychologiczne*, 08(2), 111–135
- Jentzsch, N. (2016). *State-of-the-Art of the Economics of Cyber-Security and Privacy* (SSRN Scholarly Paper No. ID 2671291). Rochester, NY: Social Science Research Network. Retrieved from <https://papers.ssrn.com/abstract=2671291>
- Johnson, R., & Orme, B. (2003). Getting the most from CBC. Retrieved from <http://www.sawtoothsoftware.com/download/techpap/cbcmost.pdf>
- Jourard, S. M. (1971). *Self-disclosure: An experimental analysis of the transparent self*. Oxford, England: John Wiley.
- Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387–402. doi:10.1057/ejis.2008.29
- Kahneman, D. (2011). *Thinking, fast and slow* (1st ed.). New York, NY: Farrar, Straus and Giroux.
- Kappel, K., & Grechenig, T. (2009). Show-me’’: Water consumption at a glance to promote water conservation in the shower. In: *Persuasive '09, Proceedings of the 4th International Conference on Persuasive Technology* (26:1-26:6). New York, NY, USA: ACM. doi:10.1145/1541948.1541984
- Kaptein, M., Ruyter, B. de, Markopoulos, P., & Aarts, E. (2012). Adaptive persuasive systems: A study of tailored persuasive text messages to reduce snacking. *ACM Transactions on Interactive Intelligent Systems*, 2(2), 1–25. doi:10.1145/2209310.2209313
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607–635. doi:10.1111/isj.12062

- Kehr, F., Wentzel, D., Kowatsch, T., & Fleisch, E. (2015). Rethinking Privacy Decisions: Pre-Existing Attitudes, Pre-Existing Emotional States, and a Situational Privacy Calculus. *ECIS 2015 Completed Research Papers*. doi:10.18151/7217379
- Keller, J., Bohner, G., & Erb, H. P. (2000). Intuitive und heuristische Urteilsbildung– verschiedene Prozesse? Präsentation einer deutschen Fassung des „Rational-Experiential Inventory“ sowie neuer Selbstberichtskalen zur Heuristiknutzung. *Zeitschrift für Sozialpsychologie*, 31(2), 87–101
- Kelley, P. G., Bresee, J., Cranor, L. F., Reeder, R.W. (2009). A "nutrition label" for privacy. In Lorrie Faith Cranor (Hg.), *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. The 5th Symposium on Usable Privacy and Security*. Mountain View, California, 15.07.2009 - 17.07.2009. New York, New York, USA: ACM Press, S. 1.
- Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, 78, 174–182. doi:10.1016/j.chb.2017.09.034
- Kiesler, C.A., Collins, B.E., & Miller, N. (1969). *Attitude change*. Oxford, England: Wiley.
- Knijnenburg, B. P., & Kobsa, A. (2014). Increasing sharing tendency without reducing satisfaction: Finding the best privacy-settings user interface for social networks. In: Association for Information Systems (Hg.), *Proceedings of the Thirty Fifth International Conference on Information Systems*.
- Knijnenburg, B., & Jin, H. (2013). The persuasive effect of privacy recommendations. In CHI '13. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, Paper 16.
- Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology*, 67, 2587–2606. doi:10.1002/asi.23629
- Krohne, H. W., Egloff, B., Kohlmann, C.-W., & Tausch, A. (1996). Untersuchungen mit einer deutschen Version der “Positive and Negative Affect Schedule” (PANAS).

- [Investigations with a German version of the Positive and Negative Affect Schedule (PANAS)]. *Diagnostica*, 42(2), 139–156.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Kolb, N., Bartsch, S., Volkamer, M., & Vogt, J. (2014). Capturing attention for warnings about insecure password fields – Systematic development of a passive security intervention. In Theo Tryfonas & Ioannis Askoxylakis (Eds.), *Lecture Notes in Computer Science: Vol. 8533. Human Aspects of Information Security, Privacy, and Trust* (pp. 172–182). doi:10.1007/978-3-319-07620-1_16
- Koroleva, K., Krasnova, H., Veltri, N. F., & Günther, O. (2011). It's all about networking! Empirical investigation of social capital formation on social network sites. In *Proceedings of the Thirty Second International Conference on Information Systems (ICIS)* (pp. 1–20). Shanghai (China). doi:10.7892/boris.47120
- Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110, 5802–5805. <https://doi.org/10.1073/pnas.1218772110>
- Krämer, N. C., Eimler, S. C., & Neubaum, G. (2014). Selbstpräsentation und Beziehungsmanagement in sozialen Medien. In J.-H. Schmidt & M. Taddicken (Eds.), *Handbuch Soziale Medien* (S. 1–20). Wiesbaden: Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-03895-3_3-1
- Krämer, N. C., & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 127–141). Heidelberg, Germany: Springer.
- Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, 4, 127–135. doi:10.1007/s12599-012-0216-6

- Krasnova, H., & Veltri, N. F. (2010). Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1–10). doi:10.1109/HICSS.2010.307
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology*, 25(2), 109–125. doi:10.1057/jit.2010.6
- Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). "It won't happen to me!": Self-disclosure in online social networks. In K. E. Kendall & U. Varshney (Eds.), *AMCIS 2009 Proceedings* (p. 343).
- Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, 2(1), 39–63. doi:10.1007/s12394-009-0019-1
- Kuo, T., & Tang, H.-L. (2014). Relationships among personality traits, Facebook usages, and leisure activities – A case of Taiwanese college students. *Computers in Human Behavior*, 31, 13–19. doi:10.1016/j.chb.2013.10.019
- Kuo, Y.-F., & Yen, S.-N. (2009). Towards an understanding of the behavioral intention to use 3G mobile value-added services. *Computers in Human Behavior*, 25(1), 103–110. doi:10.1016/j.chb.2008.07.007
- Landis, J. R., and Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159–174.
- Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior*, 76, 149–163. doi:10.1016/j.chb.2017.07.015
- Larose, R., & Rifon, N. (2006). Your privacy is assured - of being disturbed: websites with and without privacy seals. *New Media & Society*, 8(6), 1009–1029. doi:10.1177/1461444806069652
- Larose, R., & Rifon, N. J. (2007). Promoting iSafety. Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs*, 41(1), 127–149. doi:10.1111/j.1745-6606.2006.00071.x

- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, 33(3), 22-42. doi:10.1111/j.1540-4560.1977.tb01880.x
- Lawler, J. P., & Molluzzo, J. C. (2010). A study of the perceptions of students on privacy and security on social networking sites (SNS) on the Internet. *Journal of Information Systems Applied Research*, 3(12), 1–18. Retrieved from <http://jisar.org>
- Lazarus, R S and Folkman, S, (1984). *Stress, Appraisal, and Coping*. New York: Springer.
- Leary, M. R., & Allen, A. B. (2011). Self-Presentational Persona: Simultaneous Management of Multiple Impressions. *Journal of Personality and Social Psychology*, 101, 1033-1049. doi:10.1037/a0023884
- Leary, M. R., & Kowalski, R. M. (1990). Impression management: A literature review and two-component model. *Psychological Bulletin*, 107(1), 34–47. doi:10.1037/0033-2909.107.1.34
- Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services?: A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, 71(9), 862–877. doi:10.1016/j.ijhcs.2013.01.005
- Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445–454. doi:10.1080/01449290600879344
- Levin, I. P., Huneke, M. E., & Jasper, J. D. (2000). Information processing at successive stages of decision making: Need for cognition and inclusion–exclusion effects. *Organizational Behavior and Human Decision Processes*, 82(2), 171–193. doi:10.1006/obhd.2000.2881
- Levine, M. (1999). Rethinking Bystander Nonintervention: Social Categorization and the Evidence of Witnesses at the James Bulger Murder Trial. *Human Relations*, 52(9), 1133–1155. doi:10.1177/001872679905200902
- Li, H., Luo, X. R., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management*

- Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), 62-71. doi:10.1016/j.dss.2011.01.017
- Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393-411. doi:10.1177/1461444808089415
- Logan, G. D., Schachar, R. J., & Tannock, R. (1997). Impulsivity and Inhibitory Control. *Psychological Science*, 8(1), 60-64. doi:10.1111/j.1467-9280.1997.tb00545.x
- Luce, R.D. (1997). *Individual Choice Behavior: A Theoretical Analysis*. Dover Publications. Mineola, New York.
- Madden, M. (2012). Privacy management on social media sites. Retrieved from <http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/>
- Maheswaran, D., & Meyers-Levy, J. (1990). The influence of message framing and issue involvement. *Journal of Marketing Research*, 27(3), 361-367. doi:10.2307/3172593
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355 doi:[10.1287/isre.1040.0032](https://doi.org/10.1287/isre.1040.0032)
- Martin, K., & Shilton, K. (2016). Why Experience Matters to Privacy: How Context-based Experience Moderates Consumer Privacy Expectations for Mobile Applications. *J. Assoc. Inf. Sci. Technol.*, 67(8), 1871-1882. doi:10.1002/asi.23500
- Marwick, A. E., & boyd, d. m. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051-1067. doi:10.1177/1461444814543995
- Marwick, A. E., & boyd, d. m. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13, 114-133 doi:10.1177/1461444810365313
- Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the*

- Social Web* (pp. 9–17). Berlin, Heidelberg: Springer Berlin Heidelberg.
doi:10.1007/978-3-642-21521-6_2
- Masur, P. K. (2018). *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Cham, Switzerland: Springer International Publishing
- Masur, P. K., & Scharrow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, 2, 1–13. doi:10.1177/2056305116634368
- Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica*. doi: 10.1026/0012-1924/a000179
- Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-It-Yourself Data Protection—Empowerment or Burden? In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (pp. 277–305). Dordrecht: Springer Netherlands.
doi:10.1007/978-94-017-7376-8_11
- Maxwell, K. A. (2002). Friends: The Role of Peer Influence Across Adolescent Risk Behaviors. *Journal of Youth and Adolescence*, 31(4), 267–277.
doi:10.1023/A:1015493316865
- Mayring, P. (2010). Qualitative Inhaltsanalyse. In *Beltz Pädagogik. Handbuch Qualitative Forschung in der Psychologie. Grundlagen und Techniken*, edited by G. Mey and K. Mruck (Wiesbaden: VS Verlag für Sozialwissenschaften / Springer Fachmedien GmbH Wiesbaden), pp. 601-613.
- McFadden, D. (1980). Econometric models for probabilistic choice among products. *The Journal of Business*, 53, S13-S29. Retrieved from <http://www.jstor.org/stable/2352205>
- McFadden, D. (1974). Conditional logit analysis of qualitative choice behavior. In P. Zarembka (Ed.), *Frontiers in Econometrics* (pp. 105–142). New York: Academic Press.
- Mehdizadeh, S. (2010). Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook. *Cyberpsychology, Behavior, and Social Networking*, 13(4), 357–364.
doi:10.1089/cyber.2009.0257

- Meier, Y. & Schäwel, J. (2018). *Who Cares? Investigating Determinants of Internet Users' Willingness to Use a Privacy Protecting Tool*. Manuscript submitted for publication.
- Meis, R., & Heisel, M. (2017). Pattern-Based Representation of Privacy Enhancing Technologies as Early Aspects. In J. Lopez, S. Fischer-Hübner, & C. Lambrinouidakis (Eds.), *Lecture Notes in Computer Science: Vol. 10442. Trust, Privacy and Security in Digital Business* (pp. 49–65). doi:10.1007/978-3-319-64483-7_4
- Meshi, D., Tamir, D. I., & Heekeren, H. R. (2015). The Emerging Neuroscience of Social Media. *Trends in Cognitive Sciences*, 19(12), 771–782. doi:10.1016/j.tics.2015.09.004
- Meske, C., & Potthoff, T. (2017). The DINU-model – A process model for the design of nudges. In *Proceedings of the 25th European Conference on Information Systems* (pp. 2587–2597).
- Metzger, M. J., Wilson, C., Pure, R., Zhao, Y. B. (2012): Invisible interactions: What latent social interaction can tell us about social relationships in social networking sites. In: Communello, F. (Ed.): *Networked Sociability and Individualism: Technology for Personal and Professional Relationships*. Hershey, PA, pp. 9-17.
- Miller, J. D., Gentile, B., Wilson, L., & Campbell, W. K. (2013). Grandiose and vulnerable narcissism and the DSM–5 pathological personality trait model. *Journal of Personality Assessment*, 95(3), 284–290. doi:10.1080/00223891.2012.685907
- Miller, J. D., Hoffman, B. J., Gaughan, E. T., Gentile, B., Maples, J., & Campbell, W. K. (2011). Grandiose and Vulnerable Narcissism: A Nomological Network Analysis. *Journal of Personality*, 79(5), 1013–1042 doi:10.1111/j.1467-6494.2010.00711.x
- Miltgen, C. L., & Peyrat-Guillard, D. (2014). *Cultural and generational influences on privacy concerns: a qualitative study in seven european countries* (Post-Print). HAL. Retrieved from <https://econpapers.repec.org/paper/haljournal/hal-01116067.htm>
- Moll, R., Pieschl, S., & Bromme, R. (2014). Competent or clueless?: Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior*, 41, 212–219. doi:10.1016/j.chb.2014.09.033

- Morf, C. C., & Rhodewalt, F. (2001). Unraveling the paradoxes of narcissism: A dynamic self-regulatory processing model. *Psychological Inquiry, 12*(4), 177-196. doi:10.1207/S15327965PLI1204_1
- Morton, A. (2013). Measuring Inherent Privacy Concern and Desire for Privacy - A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern. In *2013 International Conference on Social Computing* (pp. 468-477). doi:10.1109/SocialCom.2013.73
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context. *Journal of Service Research, 15*(1), 76-98. doi:10.1177/1094670511424924
- Nail, P. R., MacDonald, G. & Levy, D. A. (2000). Proposal of a four-dimensional model of social response
- Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum, 32*(1), 81-94. doi:10.1080/02732173.2012.628560
- Neubaum, G., & Krämer, N. C. (2017a). Opinion Climates in Social Media: Blending Mass and Interpersonal Communication. *Human Communication Research, 43*(4), 464-476. doi:10.1111/hcre.12118
- Neubaum, G., & Krämer, N. C. (2017b). Monitoring the Opinion of the Crowd: Psychological Mechanisms Underlying Public Opinion Perceptions on Social Media. *Media Psychology, 20*(3), 502-531. doi:10.1080/15213269.2016.1211539
- Noelle-Neumann, E. (1974). The Spiral of Silence a Theory of Public Opinion. *Journal of Communication, 24*(2), 43-51. doi:10.1111/j.1460-2466.1974.tb00367.x
- Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior, 26*(3), 406-418. doi:10.1016/j.chb.2009.11.012
- O'Connell, R., & Kirwan, G. (2014). Protection Motivation Theory and Online Activities. In A. Power & G. Kirwan (Eds.) *Cyberpsychology and New Media: A Thematic Reader* (pp.139-148). New York, NY: Psychology Press.
- O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review, 19*(1), 17-31. doi:10.1177/089443930101900103

- O’Keeffe, G. S., Clarke-Pearson, K., & Media, C. on C. and. (2011). The Impact of Social Media on Children, Adolescents, and Families. *Pediatrics*, *127*(4), 800–804. doi:10.1542/peds.2011-0054
- Ochs, C., & Lamla, J. (2017). Demokratische Privacy by Design: Kriterien soziotechnischer Gestaltung von Privatheit. *Forschungsjournal Soziale Bewegungen*, *30*(2), 189–199. doi:10.1515/fjsb-2017-0040
- Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262.
- Ong, E. Y. L., Ang, R. P., Ho, J. C. M., Lim, J. C. Y., Goh, D. H., Lee, C. S., & Chua, A. Y. K. (2011). Narcissism, extraversion and adolescents’ self-presentation on Facebook. *Personality and Individual Differences*, *50*(2), 180–185. doi:10.1016/j.paid.2010.09.022
- Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites?: The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior*, *49*, 324–332. doi:10.1016/j.chb.2015.02.062
- Panek, E. T., Nardis, Y., & Konrath, S. (2013). Mirror or megaphone?: How relationships between narcissism and social networking site use differ on Facebook and Twitter. *Computers in Human Behavior*, *29*(5), 2004–2012. doi:10.1016/j.chb.2013.04.012
- Paramboukis, O., Skues, J., & Wise, L. (2016). An exploratory study of the relationships between narcissism, self-esteem and Instagram use. *Social Networking*, *5*(2), 82–92. doi:10.4236/sn.2016.52009
- Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. doi:10.1177/0093650211418338
- Park, H. S., & Smith, S. W. (2007). Distinctiveness and influence of subjective norms, personal descriptive and injunctive norms, and societal descriptive and injunctive norms on behavioral intent: A case of two behaviors critical to organ donation. *Human Communication Research*, *33*, 194–218. doi:10.1111/j.1468-2958.2007.00296.x

- Petronio, S. (2010). Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation? *Journal of Family Theory & Review*, 2(3), 175–196. doi:10.1111/j.1756-2589.2010.00052.x
- Petronio, S., & Durham, W. (2008). Understanding and applying communication privacy management theory. In L. A. Baxter & D. O. Braithwaite (Eds.), *Engaging theories in interpersonal communication* (pp. 309–322). Thousand Oaks, CA: Sage.
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. SUNY series in communication studies. Albany, NY, US: State University of New York Press.
- Petty, R. E., & Cacioppo, J. T. (Eds.) (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. New York, NY: Springer.
- Pfitzmann, A., & Hansen, M. (2008). Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management—a consolidated proposal for terminology. Version v0, 31, 15. In Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53, 1-17.
- Pincus, A. L., Cain, N. M., & Wright, A. G. C. (2014). Narcissistic grandiosity and narcissistic vulnerability in psychotherapy. *Personality Disorders: Theory, Research, and Treatment*, 5(4), 439–443. doi:10.1037/per0000031
- Raskin, R., & Terry, H. (1988). A principal-components analysis of the Narcissistic Personality Inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology*, 54(5), 890-902. doi:10.1037/0022-3514.54.5.890
- Raynes-Goldie, K. (2010). Aliases, creeping and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1). Retrieved from <https://espace.curtin.edu.au/handle/20.500.11937/29989>
- Registriatiekamer (1995). *Privacy-Enhancing Technologies: The Path to Anonymity*. Achtergrondstudies en Verkenningen.
- Renner, B., Panzer, M., & Oeberst, A. (2007). Gesundheitsbezogene Risikokommunikation. In U. Six, U. Gleich, R. Gimmler (Hrsg.) *Kommunikationspsychologie - Medienpsychologie: Lehrbuch* (S. 251–270.). Weinheim: Beltz.

- Reynolds, J., Kizito, J., Ezumah, N., Mangesho, P., Allen, E., & Chandler, C. (2011). Quality assurance of qualitative research: a review of the discourse. *Health Research Policy and Systems*, 9(1), 43 doi:10.1186/1478-4505-9-43
- Reynolds, B., Venkatanathan, J., Gonçalves, J., & Kostakos, V. (2011). Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours. In P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, & M. Winckler (Eds.), *Human-Computer Interaction – INTERACT 2011* (pp. 204–215). Springer Berlin Heidelberg.
- Rhine, R. J., & Severance, L. J. (1970). Ego-involvement, discrepancy, source credibility, and attitude change. *Journal of Personality and Social Psychology*, 16(2), 175-190. doi:10.1037/h0029832
- Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *Journal of Consumer Affairs*, 39(2), 339–362. doi:10.1111/j.1745-6606.2005.00018.x
- Ritchie, J., Lewis, J., Elam, G., Tennant, R., & Rahim, N. (2014). Designing and selecting samples. In J. Ritchie, J. Lewis, C. McNaughton Nicholls, & R. Ormston (Eds.), *Qualitative research practice* (pp. 111–145). London, UK: SAGE.
- Rise, J., Sheeran, P., & Hukkelberg, S. (2010). The Role of Self-identity in the Theory of Planned Behavior: A Meta-Analysis. *Journal of Applied Social Psychology*, 40(5), 1085–1105. doi:10.1111/j.1559-1816.2010.00611.x
- Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In B. L. Cacioppo & L. L. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153–176). London: Guildford.
- Rogers, R. W. (1975). A Protection Motivation Theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. doi:10.1080/00223980.1975.9915803
- Rogers, E. M., & Agarwala-Rogers, R. (1975). Organizational communication. *Communication behaviour*, 218-239.
- Rohrmann, B. (2008, June). Risk perception, risk attitude, risk communication, risk management: A conceptual appraisal. In *Conferencia presentada en la Sociedad Internacional de Gerenciamiento de Emergencias*.

- Barlag, C. (2017). *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*. (A. Roßnagel, Ed.) (1. Auflage). Baden-Baden: Nomos.
- Rousseau GK, Wogalter MS. (2006). Research on warning signs. In Wogalter MS, editor. *Handbook of warnings*. Mahwah, NJ: Erlbaum.pp. 147–158
- Ruddigkeit, A., Penzel, J., & Schneider, J. (2013). Dinge, die meine Eltern nicht sehen sollten. *Publizistik*, 58(3), 305–325. doi:10.1007/s11616-013-0183-z
- Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1), 68–78. doi:10.1037//0003-066X.55.1.68
- Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, 154(4), 352–369. doi:10.1080/00224545.2014.914881
- Salehie, M., & Tahvildari, L. (2009). Self-adaptive Software: Landscape and Research Challenges. *ACM Trans. Auton. Adapt. Syst.*, 4(2), 14:1–14:42. doi:10.1145/1516533.1516538
- Santor, D. A., Messervey, D., & Kusumakar, V. (2000). Measuring peer pressure, popularity, and conformity in adolescent boys and girls: Predicting school performance, sexual attitudes, and substance abuse. *Journal of Youth and Adolescence*, 29(2), 163–182 doi:10.1023/A:1005152515264
- Schapira, M. M., Nattinger, A. B., & McHorney, C. A. (2001). Frequency or Probability? A Qualitative Study of Risk Communication Formats Used in Health Care. *Medical Decision Making*, 21(6), 459–467. doi:10.1177/0272989X0102100604
- Schäwel, J. (2017). Paving the way for technical privacy support. A qualitative study on users' intentions to engage in privacy protection. *Presented at ICA 2017*, San Diego.
- Schäwel J., Krämer N. C. (2018) How to Spread Kindness: Effects of Rewarding Elements Within a Persuasive Application to Foster Prosocial Behavior. In: Guidi B., Ricci L., Calafate C., Gaggi O., Marquez-Barja J. (eds) *Smart Objects and Technologies for Social Good. GOODTECHS 2017*. Lecture Notes of the Institute

- for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 233. Springer, Cham.
- Schiebener, J., & Brand, M. (2015). Decision making under objective risk conditions – A review of cognitive and emotional correlates, strategies, feedback processing, and external influences. *Neuropsychology Review*, 25(2), 171–198. doi:10.1007/s11065-015-9285-x
- Schrepp, M., Hinderks, A., & Thomaschewski, J. (2017). Konstruktion einer Kurzversion des User Experience Questionnaire. doi:10.18420/muc2017-mci-0006
- Selinger, E., & Whyte, K. (2011). Is There a Right Way to Nudge? The Practice and Ethics of Choice Architecture. *Sociology Compass*, 5(10), 923–935. doi:10.1111/j.1751-9020.2011.00413.x
- Siegrist, M., & Cvetkovich, G. (2000). Perception of hazards: The role of social trust and knowledge. *Risk analysis*, 20(5), 713-720. doi:10.1111/0272-4332.205064
- Six, U., Gleich, U., & Gimmler, R. (2007). *Kommunikationspsychologie - Medienpsychologie: Lehrbuch* (1st ed.). Weinheim: Beltz.
- Smith, E. R., & DeCoster, J. (2000). Dual process models in social and cognitive psychology: Conceptual integration and links to underlying memory systems. *Personality and Social Psychology Review*, 4, 108-131.
- Smock, A. D., Ellison, N. B., Lampe, C., & Wohn, D. Y. (2011). Facebook as a toolkit: A uses and gratification approach to unbundling feature use. *Computers in Human Behavior*, 27(6), 2322–2329. doi:10.1016/j.chb.2011.07.011
- Solove, D. J. (2008). *Understanding privacy*. Cambridge, Massachusetts London, England: Harvard University Press.
- Special, W. P., & Li-Barber, K. T. (2012). Self-disclosure and student satisfaction with Facebook. *Computers in Human Behavior*, 28, 624–630. doi:10.1016/j.chb.2011.11.008
- Steijn, W. M. P., Schouten, A. P., & Vedder, A. H. (2016). Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1), article 3. doi: 10.5817/CP2016-1-3

- Stieglitz, S., Potthoff, T., & Kißmer, T. (2017). Digital Nudging am Arbeitsplatz. *HMD*, 54(6), 965–976. doi:10.1365/s40702-017-0367-5
- Strack, F., & Deutsch, R. (2004). Reflective and impulsive determinants of social behavior. *Personality and Social Psychology Review : An Official Journal of the Society for Personality and Social Psychology, Inc*, 8(3), 220–247.
- Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, 52, 278–292. doi:10.1016/j.chb.2015.06.006
- Sunstein, C. R. (2014). *Nudging: A Very Short Guide* (SSRN Scholarly Paper No. ID 2499658). Rochester, NY: Social Science Research Network. Retrieved from <https://papers.ssrn.com/abstract=2499658>
- Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the Personalization-privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Q.*, 37(4), 1141–1164. doi:10.25300/MISQ/2013/37.4.07
- Sutton, S. R. 1982. “Fear-Arousing Communications: A Critical Examination of Theory and Research,” in *Social Psychology and Behavioral Medicine*, J. R. Eiser (ed.), London: Wiley, pp. 303-337.
- Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29(3), 821–826. doi:10.1016/j.chb.2012.11.022
- Taddicken, M. (2014). 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. *Journal of Computer-Mediated Communication*, 19(2), 248–273. doi:10.1111/jcc4.12052
- Taddicken, M. (2013). Selbstoffenbarung im Web 2.0. In *Die Nutzung des Web 2.0 in Deutschland* (pp. 144–153). Nomos Verlagsgesellschaft mbH & Co. KG.
- Taddicken, M. (2011). Selbstoffenbarung im Social Web: Ergebnisse einer Internet-repräsentativen Analyse des Nutzverhaltens in Deutschland. *Publizistik*, 56, 281–303. doi:10.1007/s11616-011-0123-8

- Talukder, N., Ouzzani, M., Elmagarmid, A. K., Elmeleegy, H., & Yakout, M. (2010). Privometer: Privacy protection in social networks. In *2010 IEEE 26th International Conference on Data Engineering Workshops (ICDEW 2010)* (pp. 266–269). doi:10.1109/ICDEW.2010.5452715
- Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, 38, 159–173. doi:10.1016/j.chb.2014.05.027.
- Tangney, J. P., Baumeister, R. F., & Boone, A. L. (2004). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of Personality*, 72(2), 271–324.
- Teutsch, D., Masur, P. K. & Trepte, S. (2018). Privacy in Mediated and Nonmediated Interpersonal Communication: How Subjective Concepts and Situational Perceptions Influence Behaviors. *Social Media + Society*. doi: 0.1177/2056305118767134
- Thaler, R. H. (2008). *Nudge: improving decisions about health, wealth, and happiness*. New Haven: Yale University Press.
- Theil, H. (1970). On the estimation of relationships involving qualitative variables. *American Journal of Sociology*, 76, 103–154. doi:10.1086/224909
- Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245–257. doi:10.1002/asi.20121
- Tormala, Z. L., Petty, R. E., & Briñol, P. (2002). Ease of Retrieval Effects in Persuasion: A Self-Validation Analysis. *Personality and Social Psychology Bulletin*, 28(12), 1700–1712. doi:10.1177/014616702237651
- Treem, J. W., & Leonardi, P. M. (2013). Social Media Use in Organizations: Exploring the Affordances of Visibility, Persistence, Editability, and Association. *Annals of the International Communication Association*, 36, 143-189.
- Treem, J. W., & Leonardi, P. M. (2012). *Social Media Use in Organizations: Exploring the Affordances of Visibility, Editability, Persistence, and Association* (SSRN

- Scholarly Paper No. ID 2129853). Rochester, NY: Social Science Research Network.
Retrieved from <https://papers.ssrn.com/abstract=2129853>
- Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*, 3(1). doi:10.1177/2056305116688035
- Trepte, S. & Masur, P. (2017, in press). Need for privacy. In Zeigler-Hill, V. & Shackelford, T. (Eds.): *Encyclopedia of personality and individual differences*. New York: Springer.
- Trepte, S. & Masur, P. K. (2016). Cultural differences in media use, privacy, and self-disclosure. Research report on a multicultural survey study. Germany: University of Hohenheim.
- Trepte, S., & Teutsch, D. (2016). Privacy paradox. In N. C. Krämer, S. Schwan, D. Unz, & M. Suckfüll (Eds.), *Medienpsychologie. Schlüsselbegriffe und Konzepte* (2nd ed., pp. 372–377). Stuttgart, Germany: Kohlhammer.
- Trepte, S., Dienlin, T., & Reinecke, L. (2015). Influence of social support received in online and offline contexts on satisfaction with social support and satisfaction with life: A longitudinal study. *Media Psychology*, 18(1), 74–105. doi:10.1080/15213269.2013.838904
- Trepte, S., Masur, P. K., Dienlin, T. & Scharnow, M. (2015). Privatheitsbedürfnisse verschiedener Kommunikationstypen on- und offline: Ergebnisse einer repräsentativen Studie zum Umgang mit persönlichen Inhalten. *Media Perspektiven*, 5, 250-257.
- Trepte, S. (2015). Social Media, Privacy, and Self-Disclosure: The Turbulence Caused by Social Media's Affordances. *Social Media + Society*, 1(1), 2056305115578681. doi:10.1177/2056305115578681
- Trepte, S., D., Masur, P. K., Eicher, C., Fischer, M., & Hennhöfer, A., & Lind., F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale"(OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Dordrecht: Springer. doi:10.1007/978-94-017-9385-8_14

- Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors: How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jakob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis [From the Gutenberg galaxy to the Google galaxy]* (pp. 225–244). Wiesbaden, Germany: UVK.
- Trepte, S., & Reinecke, L. (Eds.). (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Heidelberg, Germany: Springer.
- Tufekci, Z. (2014). Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls. *ArXiv:1403.7400 [Physics]*. Retrieved from <http://arxiv.org/abs/1403.7400>
- Tufekci, Z. (2008). Can you see me now?: Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20–36. doi:10.1177/0270467607311484
- Turel, O., & Serenko, A. (2012). The benefits and dangers of enjoyment with social networking websites. *European Journal of Information Systems*, 21(5), 512–528. doi:10.1057/ejis.2012.1
- Utz, S. (2015). The function of self-disclosure on social network sites: Not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. *Computers in Human Behavior*, 45, 1–10. doi:10.1016/j.chb.2014.11.076
- Utz, S., Tanis, M., & Vermeulen, I. (2012). It is all about being popular: The effects of need for popularity on social network site use. *Cyberpsychology, Behavior, and Social Networking*, 15, 37–42. doi:10.1089/cyber.2010.0651
- Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2). Retrieved from <https://cyberpsychology.eu>
- Valkenburg, P. M., Peter, J., & Schouten, A. P. (2006). Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *CyberPsychology & Behavior*, 9(5), 584–590. doi:10.1089/cpb.2006.9.584
- Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy As a Fuzzy Concept: A New Conceptualization of Privacy for Practitioners. *J. Assoc. Inf. Sci. Technol.*, 66(5), 918–929. doi:10.1002/asi.23220

- Verduyn, P., Ybarra, O., Résibois, M., Jonides, J., & Kross, E. (2017). Do social network sites enhance or undermine subjective well-being? A critical review. *Social Issues and Policy Review*, 11(1), 274–302. doi:10.1111/sipr.12033
- Vitak, J. (2015). Balancing privacy concerns and impression management strategies on Facebook. In L. F. Cranor, R. Biddle, & S. Consolvo (Eds.), *Proceedings of the Eleventh Symposium on Usable Privacy and Security*. doi:10.1002/9781119197249
- Vitak, J., & Kim, J. (2014). “You Can’t Block People Offline”: Examining How Facebook’s Affordances Shape the Disclosure Process. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 461–474). New York, NY, USA: ACM. doi:10.1145/2531602.2531672
- Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451–470. doi:10.1080/08838151.2012.732140
- Vorderer, P., Krömer, N., & Schneider, F. M. (2016). Permanently online – Permanently connected: Explorations into university students’ use of social media and mobile smart devices. *Computers in Human Behavior*, 63, 694–703. doi:10.1016/j.chb.2016.05.085
- Walther, J. B. (2011). Introduction to Privacy Online. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 3–8). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-21521-6_1
- Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., & Sadeh, N. (2014). A field trial of privacy nudges for Facebook. In M. Jones, P. Palanque, A. Schmidt, & T. Grossman (Eds.), *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14* (pp. 2367–2376). New York, New York, USA: ACM Press. doi:10.1145/2556288.2557413
- Wang, Y., Leon, P. G., Chen, X., Komanduri, S., Norcie, G., Scott, K., Acquisti, A., Cranor, L. F., Sadeh, N. M. (2013). From Facebook Regrets to Facebook Privacy Nudges. *Ohio State Law Journal*, 74(6), 1307–1334.
- Wang, Y., Leon, P. G., Scott, K., Chen, X., Acquisti, A., & Cranor, L. F. (2013). Privacy nudges for social media: An exploratory Facebook study. In : *WWW '13*

- Companion, Proceedings of the 22nd International Conference on World Wide Web* (pp. 763–770). New York, NY, USA: ACM. doi:10.1145/2487788.2488038
- Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). “I regretted the minute I pressed share”: A qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (pp. 1–12). doi:10.1002/9781118266892.ch1
- Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of Personality and Social Psychology*, 54(6), 1063–1070.
- Westin, A. F. (1967). Special report: Legal safeguards to insure privacy in a computer society. *Communications of the ACM*, 10(9), 533–537. doi:10.1145/363566.363579
- Weyns, D., Iftikhar, M. U., de la Iglesia, D. G., & Ahmad, T. (2012). A Survey of Formal Methods in Self-adaptive Systems. In *Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering* (pp. 67–79). New York, NY, USA: ACM. doi:10.1145/2347583.2347592
- Wilkinson, D., Sivakumar, S., Cherry, D., Knijnenburg, B. P., Raybourn, E. M., Wisniewski, P. J., & Sloan, H. (2017). (Work in Progress) User-Tailored Privacy by Design.
- Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science*, 7(3), 203–220. doi:10.1177/1745691612442904
- Wink, P. (1991). Two faces of narcissism. *Journal of Personality and Social Psychology*, 61(4), 590–597. doi:10.1037/0022-3514.61.4.590
- Winter, S., Neubaum, G., Eimler, S. C., Gordon, V., Theil, J., Herrmann, J., Meinert, J., Krämer, N. C. (2014). Another brick in the Facebook wall – How personality traits relate to the content of status updates. *Computers in Human Behavior*, 34, 194–202. doi:10.1016/j.chb.2014.01.048
- Wisniewski, P., Lipford, H., & Wilson, D. (2012). Fighting for my space: Coping mechanisms for sns boundary regulation. In J. A. Konstan, E. H. Chi, & K. Höök (Eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems – CHI '12* (pp. 609–618). doi:10.1145/2207676.2207761

- Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health Education & Behavior, 27*(5), 591–615. doi:10.1177/109019810002700506
- Woon, I., Tan, G.-W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *ICIS 2005 Proceedings*. Retrieved from <https://aisel.aisnet.org/icis2005/31>
- Xie, W., & Kang, C. (2015). See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior, 52*, 398–407. doi:10.1016/j.chb.2015.05.059
- Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research, 13*(2), 151–168. doi:10.1007/s10660-013-9111-6
- Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.
- Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824. Retrieved from <https://aisel.aisnet.org/jais/>
- Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-aware Marketing. *Decis. Support Syst., 51*(1), 42–52. doi:10.1016/j.dss.2010.11.017
- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58*(5), 710–722. doi:10.1002/asi.20530
- Yap, S. F., and Gaur, S. S., 2016, Integrating functional, social, and psychological determinants to explain online social networking usage. *Behaviour & Information Technology, 35*(3), 166-183.
- Yates, J. F., & Stone, E. R. (1992). The risk construct. In J. F. Yates (Ed.), *Wiley series in human performance and cognition. Risk-taking behavior* (pp. 1–25). Oxford, England: John Wiley & Sons.

- Yoganathan, D., and Kajanan, S., 2013, Persuasive technology for smartphones fitness apps. In PACIS 2013 Proceedings, Paper 185.
- Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior*, *11*(6), 763–765. doi:10.1089/cpb.2007.0240
- Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society*, *16*(4), 479–500. doi:10.1080/1369118X.2013.777757
- Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, *112*(4) (pp. 1036–1040). doi:10.1073/pnas.1418680112
- Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013). Unpicking the privacy paradox. In H. Davis, H. Halpin, A. Pentland, M. Bernstein, & L. Adamic (Eds.), *Proceedings of the 5th Annual ACM Web Science Conference – WebSci '13* (pp. 463–472). doi:10.1145/2464464.2464503
- Zhang, B., & Xu, H. (2016). Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. In : *CSCW '16, Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (pp. 1676–1690). New York, NY, USA: ACM. doi:10.1145/2818048.2820073
- Zheleva, E., & Getoor, L. (2009). To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World wide web*, edited by J. Quemada (New York, NY: ACM), pp. 531-540
- Ziegeldorf, J. H., Henze, M., Hummen, R., & Wehrle, K. (2016). Comparison-Based Privacy: Nudging Privacy in Social Media Position Paper. In *Revised Selected Papers of the 10th International Workshop on Data Privacy Management, and Security Assurance - Volume 9481* (pp. 226–234). New York, NY, USA: Springer-Verlag New York, Inc. doi:10.1007/978-3-319-29883-2_15
- Zimbardo, P. G. (1960). Involvement and communication discrepancy as determinants of opinion conformity. *The Journal of Abnormal and Social Psychology*, *60*(1), 86-94. doi:10.1037/h0040786

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, 45, 158–167.