It's a private matter!
Empirical investigations of psychological mechanisms underlying online self-disclosure and privacy protection

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 kumulative Dissertation

von

Yannic Meier
aus
Duisburg

1. Gutachterin: Prof. Dr. Nicole C. Krämer
2. Gutachterin: Prof. Dr. Sabine Trepte
Tag der mündlichen Prüfung: 15.01.2021

"Privacy is the fountainhead of all other rights. Freedom of speech doesn't have a lot of meaning if you can't have a quiet space, a space within yourself, your mind, your community, your friends, your family, to decide what it is you actually want to say."

Edward Snowden (2016)[1]

[1] https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9

Acknowledgements

I would not have been able to go this way without the help of others. For this, I would like to express my deepest gratitude.

First, I would like to express my thankfulness to my supervisor Nicole Krämer for giving me the opportunity to write my thesis at this place. Thank you for all your promotion, support, feedback, criticism, and patience. Thank you for giving me the chance to work and grow in this great team. Thank you for giving me the freedom to develop my own ideas and for getting me back to the ground when I was on the wrong track. Nicole, thank you for making this thesis possible. I would also like to thank my second supervisor Sabine Trepte for her readiness to evaluate my work. Although we were not in direct exchange throughout the development process, your research work and that of your team had a significant and essential impact on the studies of the current thesis. Next, I want to thank my co-author and friend Johanna for being a part of this thesis. Thank you for all the sophisticated discussions about privacy, all the great ideas we talked about in my early doctorate days, all the cups of coffee we sipped together, and for your recent feedback.

I want to express my deepest thankfulness to the whole SP team and all persons who have accompanied my journey. Thank you for all the teaching and mentoring, and all the fun and joy we shared. My very special thanks go to Aike, Jan, Jessie, Judith, Fili, Marcel, and Lea. I am very grateful that you were always there for me when I needed help, advice, or just needed to express my joy or anger. I thank you all for sharing your fascination for research with me. Thank you for making the office a second home for me. Thank you for all the incredible conference journeys we experienced together. I will always keep these memories in my mind and my heart. At this point, I also want to thank all persons who have left SP but have supported me in my early doctorate days. Moreover, I would like to say thank you to Sina for the great discussions about privacy that have extended my perspective and helped me developing new ideas.

I would also like to thank all persons from the *Forum Privatheit* from whom I have learned a lot about privacy outside my own field of expertise. Thank you for your feedback and discussions about my work.

My gratitude is also directed to my parents who always believed in me and who supported me throughout my whole life. Thank you so much, this work would not have been possible without you! Moreover, I would like to thank all of my friends for sharing your time with me. Thank you for all the fantastic shared moments that complement the time at work and

help get my head clear. Therefore, it is not an understatement to say that without you, I would not have been able to create this thesis. Thank you for being a part of my life!

Last and foremost, I thank Jenny for sharing the office with me for the last three years. I am so happy to have had such a great person by my side with whom I could have both professional and nonsensical conversations, with whom I could experience all the ups and downs, and who was always able to cheer me up. Thank you so much for this incredible time Jenny!

All persons who are directly and indirectly mentioned here have added to this work by contributing to make me the person I am. I am grateful that every single one of you is a part of my life. Let’s set forth to many more unforgettable shared moments.

Annotation of the papers contained in the cumulus

Study I

Meier, Y., Schäwel, J. & Krämer, N. C. (2020). *Between disclosure and protection: Internet users' desire for privacy protection and their intention to adopt a privacy-protecting tool within the privacy calculus.* Manuscript submitted for publication.

Study II

Meier, Y., Schäwel, J., Kyewski, E. & Krämer, N. C. (2020). Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions. *Proceedings of the 11th International Conference on Social Media and Society,* 21-29. https://doi.org/10.1145/3400806.3400810

Study III

Meier, Y., Schäwel, J. & Krämer, N. C. (2020). The shorter the better? Effects of Privacy Policy Length on Online Privacy Decision-Making. *Media and Communication, 8*(2), 291-301. https://doi.org/10.17645/mac.v8i2.2846

Study IV

Meier, Y. & Krämer, N. C. (2020). *The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels*. Manuscript submitted for publication.

Zusammenfassung

Ein wesentlicher Teil des menschlichen Lebens wird heutzutage durch die Nutzung des Internets geprägt. Die Nutzung von Online-Diensten und die Preisgabe persönlicher Informationen sind allerdings mit erheblichen Privatheitsrisiken verbunden. Daher ist es von immenser Bedeutung, dass Wissenschaftler*innen die psychologischen Mechanismen, die der Selbstoffenbarung und dem Privatheitsschutz zugrunde liegen verstehen, um wirksame Schutzmöglichkeiten entwickeln zu können. Die vorliegende Dissertation nähert sich dem Bereich des Online-Datenschutzes mit dem Ziel, einen vielversprechenden theoretischen Rahmen (den Privacy Calculus) besser zu verstehen und die Forschung zum Schutz der Privatsphäre und zur Verbesserung der Transparenz weiter voranzutreiben. Dieser Privacy Calculus geht davon aus, dass Menschen Risiken und Nutzen vor der Datenpreisgabe abwägen. Vier quantitative Studien zielen darauf ab diesen Ansatz durch Privatheitsschutzintentionen zu erweitern und zu untersuchen, wie die Schaffung von Transparenz den Prozess der Abwägung von Risiken und Nutzen beeinflussen könnte.

Studie I übernahm ein kontextuelles Verständnis von Privatheit und erweiterte den Privacy Calculus durch einen Wunsch nach mehr Privatheitsschutz sowie die Intention, ein privatheitsschützendes Tool zu nutzen. Die Ergebnisse zeigten, dass während die Datenpreisgabe kontextabhängig war, der Wunsch der Teilnehmenden nach mehr Privatheitschutz sowie ihre Intention, das Tool zu nutzen, unabhängig von bestimmten Websites waren. Allerdings scheint der Rahmen des Privacy Calculus geeignet zu sein, sowohl die Datenpreisgabe als auch den Privatheitsschutz zu untersuchen, wobei kontextuelle und kontextübergreifende Perspektiven kombiniert werden.

In Studie II wurde ein anderer Ansatz angewandt (die Protection Motivation Theory), der sich allerdings teilweise mit dem Privacy Calculus überschneidet. Die Theorie besagt, dass Menschen potenzielle Bedrohungen als ernst, als verhinderbar und eine Schutzreaktion als wirksam wahrnehmen müssen, damit sie Schutzverhalten an den Tag legen. Außerdem können Furchtappelle ein probates Mittel sein, um die Schutzmotivation zu erhöhen. Allerdings hatten die in Studie II gezeigten Warnmeldungen keinen Effekt auf die Schutzintention von Facebook-Nutzenden. Dennoch erwies sich die Theorie als geeignet, um Privatheitsverhaltensweisen zu untersuchen: wahrgenommene Privatheitsbedrohungen sowie der Glaube, dass Privatheitsschutz wirksam ist, sagten die Schutzbereitschaft vorher, während die Selbstoffenbarungsintention durch die Wahrnehmung von Vorteilen und Risiken sowie Selbstwirksamkeit vorhergesagt wurde.

Studie III nahm eine situative Perspektive von Privatheit ein und untersuchte den kognitiven Prozess, der dem Lesen von Datenschutzerklärungen zugrunde liegt und ob Internetnutzende von kurzen Datenschutzerklärungen profitieren würden, wenn sie sich auf Websites anmelden. Die Ergebnisse zeigten, dass die Teilnehmenden in der Tat davon profitierten, eine kurze Datenschutzerklärung zu sehen. Sie wiesen ein höheres situatives Wissen auf, was zu einer realistischeren Wahrnehmung des Privatheitsniveaus der Situation führte. Dies wiederum beeinflusste die Wahrnehmung von Privatheitsrisiken und Vorteilen. Schließlich führte das Empfinden von mehr Vorteilen zu einer höheren Datenpreisgabe.

Studie IV konzentrierte sich schließlich auf den Abwägungsprozess des Privacy Calculus. Es wurde wieder eine situative Perspektive von Privatheit eingenommen, wobei diesmal allerdings drei verschiedene Situationen untersucht wurden, um inner-personelle Varianz zu erzeugen. Die Ergebnisse zeigten, dass während Unterschiede zwischen den Teilnehmenden durch unterschiedliche Wahrnehmungen der Vorteile aber auch Entscheidungsfindungsstile erklärt werden können, der innerpsychologische Abwägungsprozess stabil wirkte und Risiken und Vorteile sich gegenseitig überschreiben können. Darüber hinaus deuten die Befunde darauf hin, dass manche Personen eher rationale Privatheitsentscheidungen treffen, wohingegen andere zur intuitiven Datenpreisgabe tendieren. Daher sollte die grundlegende Idee des Privacy Calculus von gänzlich rationalen Privatheitsentscheidungen hinterfragt werden.

Durch diese vier Studien leistet die vorliegende Dissertation einen Beitrag zum Bereich der Privatheit im Internet, indem der Privacy Calculus sowie Privatheitsschutz in verschiedenen Kontexten und Situationen untersucht wurde, indem verschiedene technologische Möglichkeiten zur Erhöhung von Transparenz bei Nutzenden sowie deren Effekte erforscht wurden und indem der Privacy Calculus durch verschiedene Einflussfaktoren sowie die Untersuchung des innerpsychologischen Abwägungsprozesses erweitert wurde.

Abstract

A substantial part of human life today is shaped by the use of the Internet. Using online services and disclosing personal information, however, entails substantial risks to people's privacy. Therefore, it is of immense importance that researchers comprehend the psychological mechanisms underlying online self-disclosure and privacy protection to develop effective protection possibilities. The present dissertation approaches the field of online privacy with the aims to better understand a promising theoretical framework (i.e., the privacy calculus) and to forge ahead with research on privacy protection and transparency enhancement. This privacy calculus assumes people to weigh risks and benefits before self-disclosure. Four quantitative studies aim to expand this approach by privacy protective intentions and to examine how transparency enhancement could affect the process of weighing risks and benefits.

Study I adopted a contextual understanding of privacy and extended the privacy calculus approach by a desire for privacy protection and the intention to use a privacy protecting tool. The results revealed that whereas self-disclosure was context-dependent, participants' desire for privacy protection and their intention to use the tool were independent of certain websites. However, the privacy calculus framework appears to be suitable to investigate both self-disclosure and privacy protection while combining contextual and cross-contextual perspectives.

In study II, a different approach (the protection motivation theory) was applied that partly overlaps with the privacy calculus. The theory predicts that people must perceive a potential threat as severe, as feasible to cope with, and a protective response as effective to engage in protective behaviors. Moreover, fear appeals can be an appropriate means to enhance protection motivation. However, the warning message shown in study II had no effects on Facebook users' protection intention. Still, the theory proved valid to investigate people's privacy behaviors: perceived privacy threats and thinking that privacy protection is effective predicted protection willingness, while self-disclosure intention was predicted by benefit perception, risk perception, and self-efficacy.

Study III adopted a situational perspective on privacy and examined the cognitive process that underlies reading privacy policies and whether Internet users would benefit from shorter privacy policies while registering on websites. Results showed that participants indeed greatly benefited from seeing a short privacy policy. They exhibited higher situational privacy knowledge which lead to a more realistic perception of the situation's privacy level. This in

turn affected the perception of privacy risks and benefits. Finally, perceiving higher benefits led to more self-disclosure.

Finally, study IV focused on the weighing process of the privacy calculus. Again, a situational perspective of privacy was adopted, however, this time examining three different situations to create within-person variance. The findings revealed that whereas differences between persons can be explained by differences in people's benefit perceptions but also decision-making styles, the weighing process within persons was stable and risk and benefit perceptions can overwrite each other. Moreover, results implied that some people are more likely to make rational privacy decisions whereas others tend to self-disclose intuitively. Hence, the general privacy calculus notion of entirely rational privacy decisions has to be questioned.

By means of these four studies, the present dissertation contributed to the field of online privacy by investigating the privacy calculus and privacy protection in different contexts and situations, by exploring different technological means that could enhance transparency among users and effects of these mechanisms, and by expanding the privacy calculus by scrutinizing different impacting factors as well as the inner-psychological weighing process of risks and benefits.

Contents

Figures

I INTRODUCTION

The emergence of increasingly networked information and communication technologies has brought substantial changes to everyday life within the last decades. Today, devices like smartphones have a connection to the Internet at almost every location. Hence, lots of activities have shifted to the online world. Buying new clothes or groceries, watching movies, listening to music, reading the news, booking a flight or hotel room, or talking to friends and presenting oneself to one's *network*—almost everything can be done comfortably by means of one's PC or smartphone. To be able to use all these free services, all one needs to do is accepting the relevant privacy policy or entering one's e-mail-address and a few additional details from time to time. But all these great advantages, facilitations, and positive effects the Internet has brought have led to a downside: the erosion of personal privacy (Wheatley et al., 2016). In 2019, the revenue of Facebook was about USD 70.7 billion. In the same year, Google's holding company Alphabet achieved a revenue of around USD 162 billion. This is of importance here because the business models of both companies are based on *mining* or *harvesting* personal data of their users (Esteve, 2017). The original meanings of these two words already indicate that private user data are considered as an infinite raw material or a crop plant that can be cultivated. Not surprisingly, data has been termed to be like oil—a resource that brings wealth and power to its owners. Zuboff (2019) and West (2019) have heralded a new age of capitalism that is based on surveillance and the collection of personal data. Oftentimes, users have to disclose personal data and consent to the collection, processing, or dissemination of these and further personal information to use certain services. These data are processed in the mills of *big data* to make sense of the enormous amount of information. Big data can loosely be described as the automated, algorithmic processing of large quantities of data that are automatically accrued by the use of new technologies to make predictions about the future (Baruh & Popescu, 2017; boyd & Crawford, 2012; Matzner, 2014). The aim behind this is to identify specific groups of persons that act and think similarly and to make predictions about these groups' future behaviors (Matzner, 2014) or to modify their behavior, for example, by personalized advertisements (Zuboff, 2019). Personalized ads are following people across the web—and they do no longer serve commercial purposes only (Kruikemeier et al., 2016; Zuiderveen-Borgesius et al., 2018). It can be assumed that a company called Cambridge Analytica that used personal data of millions of Facebook users under dubious circumstances has substantially contributed to the outcomes of both the 2016 US presidential election and the Brexit referendum (Cadwalladr, 2017). Thus, big data can not only pose a threat to personal privacy and freedom based on

surveillance capitalism (Zuboff, 2015, 2019) but it can also threaten democratic structures in general (West, 2019).

For these reasons, researchers of all imaginable disciplines deal with topics that spin around the question of how personal privacy can be preserved while still enjoying the benefits of the Internet. The present dissertation will approach the topic of *online privacy* from a psychological perspective and will present four empirical studies. The focus is put on people's decision to disclose personal data on the Internet, on their willingness to protect their privacy online and on effects of technologies that can increase transparency of oftentimes invisible privacy threats. A large body of research has found that people's online self-disclosure decisions are the result of a *privacy calculus* (e.g., Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2010). This privacy calculus approach assumes people to balance the perceived online privacy risks and anticipated benefits of disclosure before disclosing personal information (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Laufer & Wolfe, 1977). That Internet users' self-disclosure decisions are merely the result of a rational weighing process, however, has been subject to criticism as behaviors are affected by biases, heuristics, or impulsivity (Acquisti & Grossklags, 2003, 2005; Knijnenburg et al., 2017; Ostendorf et al., 2020; Wilson & Valaich, 2012). Therefore, in the present dissertation, parts of the criticism will be addressed to further elaborate the nature of privacy decisions online. For instance, the privacy calculus will be investigated in different contexts (cf. Nissenbaum, 2010), as affected by subjective perceptions of the situational privacy level (cf. Teutsch et al., 2018) and further situational circumstances (cf. Masur, 2018), as well as personality traits (Hamilton et al., 2016) and beliefs (Hoffmann et al., 2020). In addition to these factors, the internal weighing process of privacy risk and benefit perceptions shall be scrutinized by separating between- from within-person variance. By these means, new insights into people's online privacy choices and the privacy calculus approach shall be generated.

In the second major area of the current work, the focus is put on Internet users' willingness to protect their privacy online and on technical solutions that should raise awareness of mostly invisible privacy threats. Internet companies do not solely collect and process information that is actively and knowingly disclosed by users, but they automatically track, store, and process user data often without users' knowledge or awareness (Bilogrevic et al., 2014; Bujlow et al., 2017). At least, users can avoid some of these privacy risks by using protective tools or by not visiting certain websites (Ebbers, 2020; Matzner et al., 2016). Hence, providing users with knowledge about potential privacy risks in different situations might be an effective means to support people in making more privacy aware choices while preserving

users' decisional autonomy. Moreover, raising awareness for online privacy threats could motivate privacy protection efforts. Hence, in parts, the studies focus on users' wish to have more privacy online and their intentions to actively protect their personal information. One study utilizes the *protection motivation theory* (Rogers, 1975, 1983) that describes how people can be effectively motivated to engage in self-protective behaviors. The theory suggests persuading people to protect themselves by employing fear appeals and information on how to shield the potential threat (Rogers, 1975). Two other studies focus on potential means to raise people's awareness for privacy threats and how an increase in awareness affects subsequent privacy perceptions and behaviors.

In sum, by means of the present dissertation's studies, more privacy risk aware self-disclosure and protection intentions and behaviors shall be studied and understood. The findings of the empirical works can contribute to the discussion about the nature of self-disclosure decisions and to the further understanding of Internet users' intentions to protect their privacy online. Moreover, practical insights will be gained of how people make privacy choices, how than can be motivated to more self-privacy protection, and how they might be supported effectively.

II THEORETICAL BACKGROUND

1 Privacy in theory – a brief overview

What is privacy? Finding a universal answer to this question is challenging since privacy is viewed from various directions and its focus varies depending on the respective discipline and even within disciplines. This section, however, aims to give a brief overview of some of the most influential privacy theories. Tracing back the term 'privacy' to its origins, leads to the Latin word *privatus* meaning "connected with or pertaining to a private person" (Berger, 1968, p. 651) stemming from Roman law and being the counterpart to the word *publicus* which means "connected with, pertinent to, available to or in the interest of the Roman people" (Berger, 1968, p. 661). The Latin words *privus* and *privare* mean 'single', 'free of something', or 'release', respectively. Hence, in its literal sense, privacy stands for something (or someone) that is not available to the public but only to specific persons and is associated with concepts like freedom or solitude.

In a prominent approach, Westin (1967) defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" and as "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" (p. 7). He further argued that solitude, intimacy, anonymity, and reserve constitute different states of privacy. Hence, a person can feel private when she is all for herself, but also when she is intimately chatting to a friend or to several persons in a group. Moreover, Westin (1967) argues that privacy is requisite to achieve personal autonomy, emotional release, and having the opportunity for self-evaluation and limited and protected communication. Therefore, having privacy is fundamental to experience important psychological functions. Whereas the theory of Westin focused on functions and states of privacy, the theory of Altman (1975) focused on characteristics of privacy while defining privacy as "the selective control of access to the self or to one's group" (p. 18). He differentiates between desired and actual privacy levels that fluctuate as a non-monotonic function. When one's current level deviates a desired level, people try to adjust the circumstances to reach their optimal state of privacy. Moreover, privacy consists of both in- and outputs. Important to Altman's (1975) theory is the idea that a person is in control of the information that may or may not pass one's personal *boundaries*. This metaphor implies that persons are able to manage which information can pass this boundary. It gets apparent that privacy is a non-negotiable necessity to human beings—although the *need*

for privacy differs and fluctuates on both inter- and intrapersonal levels (Trepte & Masur, 2020)—because miscellaneous states of privacy are condition for a proper psychological functioning (Margulis, 2003). Moreover, Margulis (1977) suggested that privacy as control in interpersonal transactions serves the aim to increase autonomy and to decrease vulnerability. Consequently, a loss of privacy would mean that a person gets vulnerable to attacks by other parties. Burgoon (1982) agreed with Altman in arguing that privacy includes control over personal information. She further noted that privacy is experienced on different dimensions. Physical privacy refers to one's actual presence in the physical world and describes the spatial distance towards other individuals. Social privacy describes one's proximity or distance to other people on a relationship level. On this dimension, states of intimacy or reservedness can arise. Furthermore, on a psychological dimension, people can control their affective in- and outputs. Finally, informational privacy refers to information output that evades personal control like information about daily habits, hair color or one's body height. Hence, on all of these dimensions, different forms of privacy can be experienced, and privacy invasions can occur with different degrees of severity. It gets clear that the revelation and the concealment of personal information are *dialectically* related (Petronio, 2002). People perceive themselves as the owners of their personal information which is why they want to be in control of this personal information (Petronio & Durham, 2008).

These examples should serve as a first brief overview of the concept of privacy and indicate the scope of the topic. It gets apparent that privacy is essential to individuals, groups, and also societies that benefit from independent opinion formation, critical voices, and diverse ideas (cf. Margulis, 2003). Privacy includes personal control which is fundamental for individual autonomy (Altman, 1975; Westin, 1967). On the individual or group level, privacy leakages are accompanied by increased vulnerability (Margulis, 1977). Therefore, adequately managing one's privacy is important to avoid privacy intrusions (Petronio, 2002). Consequently, privacy is a fundamental need to both individuals and societies and the comprehension of how Internet technologies threaten privacy is of immense importance in finding effective ways to better preserve privacy.

2 Privacy in online contexts

So far, the presented literature provided an overview of classical privacy theories. With the advent of the digital age, however, personal privacy was increasingly affected by new information technologies like computers, smartphones, or wearables. As the present dissertation deals with privacy issues on the Internet, this section will give an overview of whether privacy online is different from privacy offline and why the Internet constitutes a challenge for personal

privacy. To a large part, classical privacy theories deal with questions of physical privacy, that is the perceived presence or absence of others (Burgoon, 1982; Westin, 1967). However, online, the physical privacy dimension is only indirectly affected (Krämer & Haferkamp, 2011), for instance, by communicating one's location. Hence, privacy online is mainly affected by information that can be assigned to the informational, psychological, or social dimension (cf. Burgoon, 1982). Trepte & Dienlin (2014) argue that online privacy is not a new psychological construct and should not be considered separately from offline privacy. Hence, online privacy can be described as a point of contact between a person's personal privacy and the usage of information and communication technologies. The various characteristics of the Internet can contribute to both increasing (e.g., anonymity) or reducing (e.g., privacy intrusion) privacy depending on the level of personal information that must be actively disclosed or that is automatically collected and the purposes for which these data are subsequently used. However, frequently "users do not pay with money but with their data" (Bräunlich et al., 2020, p. 15) to use the various "free" offers of the Internet which is why privacy is regularly challenged (Papacharissi, 2010). Others even claim that "if you are not paying for it, you are the product" (Papadopoulos et al., 2017) pointing to the fact that many free websites, apps, and services invade people's privacy for commercial purposes. Zuboff (2015, 2019) and West (2019) coined the concepts of *surveillance capitalism* and *data capitalism*, respectively. This new form of capitalism can loosely be described as the mining of personal information for commercial purposes with the aims to extract, predict, and sell user information and finally modify and manipulate user behavior (Susser et al., 2019; West, 2019; Zuboff, 2015, 2019). Other actors like governmental institutions and secret services are also involved in harvesting private data (Debatin,2011; Lutz & Strathoff, 2014). Hence, the purposes of data collection are not merely commercial ones but also crime prevention or terror defense. Nevertheless, personal data are mainly used for commercial purposes like personalized product or service advertisements and microtargeting (Boerman et al., 2017), and sometimes for personalized political advertisements and microtargeting (Kruikemeier et al., 2016; Zuiderveen-Borgesius et al., 2018) which pose threats to individual's decisional autonomy (Susser et al., 2019). Moreover, as new technologies are widely used for communication purposes, other users can pose threats to one's personal privacy, too (Debatin, 2011; Masur, 2018). Thus, privacy is largely affected by the usage of Internet technologies as the processing of personal data has become an essential nature of the Internet. The next section introduces different forms of information revelation, followed by a detailed depiction of online privacy threats.

2.1 Self-disclosure

Privacy theories have already pointed to active and voluntary communication as one means to reveal private matters (Altman, 1975; Burgoon, 1982; Petronio, 2002; Westin, 1967). In the studies of the present dissertation, communication intentions and behaviors will be one of the main variables that will be assessed. The active revelation of personal information is called *self-disclosure*. Classically, self-disclosure has been "defined as any information about himself which Person A communicates verbally to Person B" (Cozby, 1973, p. 73) and as "the process of making the self known to other persons" (Jourard & Lasakow, 1958, p. 91). It becomes evident that self-disclosure is inherently a social process. Online, however, the revelation of personal information is often used for specific purposes other than merely social ones, for instance, when someone discloses personal information to purchase a product. In general, all information that can be associated with one specific person can be referred to as *personal data.* The General Data Protection Regulation (GDPR) of the European Union provides a definition of personal data in article 4 paragraph 1:

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (*The protection of natural persons with regard to the processing of personal data and on the free movement of such data,* Regulation 2016/679)

As mentioned above, Internet companies, governments and other parties are highly interested in collecting vast amounts of these data (West, 2019; Zuboff, 2019). One part of the information is the one that is deliberately disclosed, for instance, when a person creates an account on a website, when someone reveals one's address and payment information for shipment, or when someone leaves a *post* on a friend's Facebook "wall". However, another huge part of personal data is the one that is automatically collected mostly without users' direct awareness (Bujlow et al., 2017; Gillespie, 2014; Hannak et al., 2014). Hence, disclosures can be divided into active and passive forms and those that are intended or unintended (Bräunlich et al., 2020). Moreover, two axes of information flow that can become sources of privacy threats can be distinguished (Debatin, 2011; Masur, 2018; Raynes-Goldie, 2010). On a horizontal (or social) axis, people communicate to friends, peers, acquaintances, or strangers, that means to other natural persons. This axis normally comprises the active disclosure of information. A vertical (or institutional) axis describes the information flow between natural persons and

superior instances like companies, institutions, or governments. On this axis, both active and passive as well as intended and unintended disclosures occur. The present dissertation will focus on people's active and intended self-disclosure (intentions) both on the horizontal and the vertical dimension. Moreover, different privacy protective behaviors that can be a means to avoid passive disclosures will be examined in order to better comprehend the factors underlying privacy protection.

2.2 New challenges for privacy

In all four studies of the present dissertation, people's perceptions of online privacy risks will be assessed. Therefore, the present section aims to address some of these threats to provide a basic understanding for privacy risks online and why it is important to shield them. Both the active disclosure of personal information but also the mere visiting of websites can pose threats to one's privacy. This is because user behaviors are almost constantly recorded and processed by algorithms that make predictions about users based on the collected personal data (Baruh & Popescu, 2017; boyd & Crawford, 2012; Gillespie, 2014; Matzner, 2014). The inferences that are drawn from these data can be used to modify and manipulate user behavior (Matz et al., 2020; Solove, 2008; Zuboff, 2019), for instance, by commercial or political advertising (Kruikemeier et al., 2016; Zuiderveen-Borgesius et al., 2018). Hence, both actively and passively disclosed data can potentially lead to serious privacy breaches. Some researchers claim that they were able to accurately predict Facebook users' personality traits due to their *likes* on Facebook (Kosinski et al., 2013), people's sexual orientation due to their profile pictures on a dating website (Wang & Kosinski, 2018), and signs of a depression due to shared photos on Instagram (Reece & Danforth, 2017). Therefore, obviously harmless pieces of disclosed information that do not reveal much about someone can be combined with other pieces of information and lead to sensitive predictions about aspects, someone may have wanted to keep private. This process can be termed *aggregation* (Solove, 2008) or *context collapse* (Marwick & boyd, 2014). Nissenbaum (2010) introduced the perspective that people perceive privacy as contextually. What is appropriate to disclose in one context, is inappropriate to disclose in another. She notes that online privacy is shaped by the properties of each context (Nissenbaum, 2018)."[Online privacy] contexts are defined by the properties of respective media, systems, or platforms whose distinctive material characteristics shape—moderate, magnify, enable—the character of the activities, transactions, and interactions they mediate" (Nissenbaum, 2018, p. 836). This, however, is problematic to people's privacy online when information from different contexts are combined. Although single acts of self-disclosure appear to be harmless, in sum, they can lead to deep insights. This is comparable to a puzzle:

the more pieces fit together, the more concrete the picture becomes. The issue is that users disclose single "puzzle pieces" without the awareness and expectation that some entity puts them together (Nissenbaum, 2010; Solove, 2008). Whereas users seem to have a rather high awareness for horizontal privacy risks which is reflected in their readiness to shield risks that stem from other users, they do not seem to be aware of vertical threats in the same way (Masur & Scharkow, 2016; Raynes-Goldie, 2010; Young & Quan-Haase, 2013). Teutsch and colleagues (2018) identify this challenge to privacy online by pointing to different audiences: "Beyond other users, the [Internet] audiences include service providers, surveillance agencies, and other third parties that typically do not exist in nonmediated communication settings" (p. 3). A major issue with vertical online privacy threats for both lay persons as well as experts is its elusiveness, invisibility, and intangibility (Acquisti et al., 2015; Masur, 2018). Hence, people seem to have some form of natural awareness for social privacy situations as depicted in traditional privacy theories (Altman, 1975; Burgoon, 1982; Westin, 1967), however, this natural awareness might be missing in non-social settings. Derived from this observation, it follows that this lack of awareness must be compensated, for instance, by technological means. This is why one focus of the present dissertation is put on the investigation of technical means to enhance users' awareness for privacy threats.

In addition to these threats to personal privacy, some characteristics of the Internet coerce users into self-disclosure. *Affordances* and *dark patterns* can lead to higher disclosures than intended (Trepte, 2015, 2020; Waldman, 2020). Livingstone and colleagues (2019) describe affordances "as the fundamental properties of an object that define its potential uses in an environment" (p. 48). Further, the researchers divide affordances into Internet design characteristics, network effects, and practices of organizations (Livingstone et al., 2019). Dark patters manipulate users to perform unintended actions like self-disclosure (Bösch et al., 2016; Waldman, 2020) undermining informational self-determination (Hornung & Schnabel, 2009). "Online environments are built not only to constrain users, but to coerce disclosure and trigger cognitive biases that encourage us to give up and cede control over our privacy" (Waldman, 2020, p. 108). It becomes apparent that the special characteristics of the Internet frequently threaten personal privacy and informational self-determination although some of the Internets' properties also have the potential to enhance privacy. In the studies of the present dissertation, people's perception of these privacy threats will be assessed with the interest to investigate how the awareness of privacy threats interacts with other perceptions and can alter behaviors.

Summed up, individual privacy online is challenged because in addition to intentionally disclosed information behavior is constantly recorded (Bujlow et al., 2017; Gillespie, 2014;

Hannak et al., 2014), people can be tricked into self-disclosure (Bösch et al., 2016; Waldman, 2020), companies attempt to modify people's behaviors based on collected information (Solove, 2008; West, 2019; Zuboff, 2019), and information from different contexts are brought together (Marwick & boyd, 2014; Nissenbaum, 2010, 2018; Solove, 2008) which can lead to extremely sensitive inferences about Internet users (Kosinski et al., 2013; Reece & Danforth, 2017; Wang & Kosinski, 2018). Moreover, shared information can potentially be used (e.g., disseminated to unintended audiences) by other Internet users posing additional challenges to privacy (boyd and Marwick, 2011; Trepte, 2020; Trepte & Reinecke, 2011). However, users have a higher awareness for the horizontal axis than for the vertical one (Masur & Scharkow, 2016; Raynes-Goldie, 2010; Young & Quan-Haase, 2013) probably because of natural awareness for social privacy situations and because of the invisibility and abstractness of the vertical axis (Acquisti, et al., 2015; Masur, 2018). Hence, one major aspect of the current dissertation is the investigation of different means to make these horizontal and vertical privacy threats more visible to Internet users. The focus is on both self-disclosure and privacy protection. As the main theoretical model to understand self-disclosure (and privacy protection), the privacy calculus approach is applied.

3 Online privacy decisions: the privacy calculus

When using the Internet and disclosing personal information entails so many severe risks to personal privacy, why do users engage in self-disclosure to such an extent? This section will introduce the core approach of the current dissertation that describes why people actively disclose personal data to companies and other users on the Internet. This so-called *privacy calculus* assumes Internet users to balance the anticipated advantages of information disclosure with the anticipated privacy costs (Culnan & Armstrong, 1999; Dinev & Hart, 2006). The result of this weighing process renders self-disclosure likely or unlikely. Historically, the privacy calculus is rooted in the late 70s: Laufer and Wolfe (1977) wrote that

> in many instances the individual has to ask himself/herself: If I am seen engaging in this behavior or that behavior or am seen with this person or that person, what are the consequences for me in the future, in new situations, and so on? (pp. 35-36)

The researchers believed that people take the anticipated consequences of their privacy behaviors into account before disclosing personal information and accordingly manage their information. They termed this rationale the *calculus of behavior* which posited that the perception of positive consequences of disclosure would lead to an increase of disclosure whereas associating negative consequences with information revelation would lead to no disclosure or its adaption. Two decades later, Culnan and Armstrong (1999) transferred the core

principle of the calculus of behavior to the online world. Firstly using the term *privacy calculus*, they noted that "individuals are willing to disclose personal information in exchange for some economic or social benefit subject to the "privacy calculus," an assessment that their personal information will subsequently be used fairly and they will not suffer negative consequences" (Culnan & Armstrong, 1999, p. 106). Remarkably, they linked information disclosure to the premise that the disclosed information is treated confidentially which was supported by their empirical findings: Culnan & Armstrong (1999) found that consumers' privacy concerns did not impact their intention to disclose personal information to an interactive service provider when they believed this service provider treated their personal data fairly. Building on these findings, Dinev and Hart (2006) extended the privacy calculus to the field of information disclosure to online retailers. The results of their investigation showed that the perception of privacy risks and privacy concerns reduced participants' willingness to share personal information. Contrary, trust and one's affinity towards Internet interactions increased the intended disclosure to the retailer. Since then, the privacy calculus has been applied to a variety of different contexts and settings and has been extended by several additional variables. Despite the e-commerce context, privacy calculus notions were also found on social network sites (Dienlin & Metzger, 2016; Krasnova et al., 2010), electronic health records (Dinev et al., 2016), among the adoption of smart devices (Princi & Krämer, 2020a, 2020b), and the use of mobile apps (Keith et al., 2013). Moreover, it was found that people's perceptions of privacy risks and disclosure benefits are related to self-disclosure independently of a specific context (i.e., website; Bol et al., 2018) and even independently of the culture, however, placing different weightings on risks and benefits in collectivistic and individualistic cultures (Trepte et al., 2017). Moreover, the privacy calculus framework has also been extended by a second outcome variable: self-withdrawal (Dienlin & Metzger, 2016). It was found that Facebook users are more intended to withdraw (i.e., to protect their online privacy) when they perceive privacy risks. The researchers concluded that the framework is useful to predict both self-disclosure and privacy protective behaviors. Hence, the current work aims to further elaborate these finding by not only investigating self-disclosure, but also protective wishes and intentions within the privacy calculus framework.

3.1 Perceived self-disclosure benefits

The privacy calculus approach describes that the expected benefits of self-disclosure positively affect Internet users' disclosure of personal information (Culnan & Armstrong, 1999). However, the literature lacks a concrete definition of benefit perceptions. The perceived benefits can be described as people's anticipation of advantages they will receive in the future

due to consenting to data processing or actively disclosing personal information in the current situation. Hence, the anticipation of concrete benefits is depending on the respective context and situation. The notion of context-specific benefits also coincides with Nissenbaum's (2010) description of contextual privacy: one would disclose medical issues to his/her doctor but probably not to one's employer as one expects the doctor to cure one's health issues. This is supported by findings of Dienlin and colleagues (2019) who found that only specific benefits predicted self-disclosure but not general benefits. Some benefits that have been investigated together with self-disclosure are social capital (Ellison et al., 2011), social support (Taddicken, 2011), relationship maintenance (Christofides et al., 2009), enjoyment (Krasnova et al., 2010), entertainment, and information attainment (Khan et al., 2014). Other benefits of information disclosure include convenience, price premiums (Pötzsch, 2008), and tailored information (Bol et a., 2018). Hence, to understand why a person has disclosed personal information, one needs to know which benefits a specific context or situation had to offer to that person. In the studies of the present dissertation, participants' benefit perception will be assessed as one predictor of their self-disclosure intentions and behaviors.

3.2 Perceived online privacy costs

As it has been outlined earlier (see section 2.2), there are multiple threats to people's privacy online which are often abstract and intangible, especially on the vertical axis (Masur, 2018). Thus, it is of utmost interest how people perceive the invisible costs to their privacy and how behavior as subsequently affected. The literature identifies three main concepts that can be subsumed under the umbrella of expected privacy costs. These three are privacy concerns, privacy risk beliefs and perceived privacy risks or threats (cf. Bol et al., 2018). Although, different definitions for the three concepts of cost perceptions can be found, these are not always selective and seem to overlap from time to time. Therefore, in the following it will be tried to carve out three distinct descriptions. Whereas privacy risk perception and beliefs are rather cognitive, privacy concerns represent an affective form of privacy cost perception. Dienlin and Trepte (2015) state that "privacy concerns capture the negatively valenced emotional attitude that people feel when personal rights, information, or behaviors are being regressed by others" (p. 286). Others, however, note that privacy concerns can be both affective and cognitive (Bol et al., 2018). Still, because online privacy concerns reflect people's worries about potential negative consequences resulting from the handling of their personal data in the Internet, they are inherently rather affective than cognitive. A similar yet more cognitive construct are privacy risks beliefs. Malhotra and colleagues (2004) note that "[privacy] risk beliefs refer to the expectation that a high potential for loss is associated with the release of personal information"

(p. 341). These risk expectations, however, rather remain on a superficial level and "measure people's general perceptions" (Bol et al., 2018, p. 373). People's more concrete perceptions, in contrast, are captured by their perceived privacy risks. In general, risks comprise both a detrimental event as well as a certain probability that the event will occur (Rohrmann, 2008). This is also reflected in the perception of risks: "privacy risk perceptions are two-dimensional and consist of the likelihood people attach to privacy breaches and the severity of the privacy breaches" (Bol et al., 2018, p. 373). Hence, both likelihood assessment and the perception of severity must be high to perceive a privacy risk. A similar notion is made by Rogers (1983) in the *protection motivation theory*. He notes that the perception of a threat consists of the perception of the severity of the threat as well as the perceived susceptibility (i.e. the perceived likelihood to suffer from the threat). Perceived severity of risks and perceived likelihood are, however, not equally impacting subsequent intentions or behaviors. For instance, Schäwel (2019) found that participants' perception of risk severity was more important for their decision to self-disclose than their assessment of risk likelihood whereas Krasnova and colleagues (2009) found the perceived likelihood of privacy violations to be more strongly related to privacy concerns than the perceived damage. Summarized, whereas affective privacy concerns and cognitive privacy risk beliefs represent rather abstract feelings and thoughts about potential privacy harms, perceived privacy risks represent a concrete form of cognitive risk appraisal. Similar to the result that specific but not general benefits impact self-disclosure (Dienlin et al., 2019), Bol and colleagues (2018) found that privacy risk perception was the strongest predictor of self-disclosure intentions when analyzed together with privacy concerns and privacy risk beliefs. All four studies of the present dissertation will therefore assess participants' perception of privacy risks (or threats).

3.3 A rational privacy calculus?

The main tenet of the privacy calculus is that people weigh the perceived privacy costs and benefits before they decide to self-disclose. This view is subject to a rational notion of privacy decision-making, implying that self-disclosure is always logic and deliberate with the aim to maximize benefits and minimize costs (*rational choice theory*; Simon, 1955; *expectancy theory*; Vroom, 1964). The notion of rationality, however, is subject to the criticisms that privacy behaviors are affected by biases, heuristics, and bounded rationality (Acquisti & Grossklags, 2005), that rational decisions are unlikely due to lacking feedback of long-term consequences (Ostendorf et al., 2020), or that findings of privacy calculus studies are the result of participants' post-hoc rationalizations (Knijnenburg et al., 2017). Therefore, some researchers have already declared the privacy calculus dead (Knijnenburg et al., 2017). Another

popular notion views privacy behaviors not as rational but as paradoxical. This so-called *privacy paradox*, however, has been solved by several empirical investigations (Dienlin & Trepte, 2015; Lutz et al., 2020; Pötzsch, 2008). Hence, both rational as well as paradoxical privacy notions can be criticized. One of the most popular explanations why people are considered to obviously behave paradoxically is the privacy calculus approach. As already stated earlier, numerous studies have found empirical evidence in favor of privacy calculus notions (Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2010; Princi & Krämer, 2020a, 2020b). However, these studies reveal that the perception of benefits increases the *likelihood* of self-disclosure and the perception of risks decreases the *likelihood* for information disclosure. They do not show that all Internet users are always behaving completely consciously, logically, and deliberately.

Hence, the nature of the inner-psychological privacy calculus process needs to be scrutinized in order to find more evidence for or against the approach. A general observation from previous studies is that the weights of risk and benefit perceptions do not seem to be equal. It was found that anticipated benefits have a higher effect on self-disclosure intentions than perceived privacy risks (Bol et al., 2018) and privacy concerns (Dienlin & Metzger, 2016). The same pattern was also found for actual self-disclosure behavior (Dienlin et al., 2019). An explanation for these findings can be found in the following: “Generally, it should be kept in mind that data protection is usually not a priority for users, as they are mostly focused on achieving their primary goal, for instance, acquiring a commodity or obtaining access to an online service” (Efroni et al., 2019, p. 358). This observation can be used to re-interpret the privacy calculus approach as it can no longer be expected that risk and benefit perceptions equally contribute to privacy behaviors. This might be because benefits are immediate and will be obtained with a high probability whereas privacy risks are intangible, uncertain, and in the distant future (Ostendorf et al., 2020). Additionally, dark patterns might increase benefit perceptions (Bösch et al., 2016; Waldman, 2020). “Situational cues mitigate potential risks in the distant future and emphasize immediate benefits as users exhibit a tendency to favor immediate rewards on the short term at the expense of future risks” (Barth & De Jong, 2017, p. 1047). Online privacy behaviors are complex and determined by a variety of different influence factors while many gearwheels mesh in the background. Hence, the argument that privacy behaviors are solely the result of a rational weighing of risk and benefit perceptions might be too shallow. A similar proposition is made by Bol and colleagues (2018) in their investigation of the privacy calculus:

> We follow a probabilistic understanding of the calculus: Although experiencing costs and benefits affects chances of self-disclosure significantly, it does not follow a deterministic pattern. Behavior remains partially fortuitous, and other factors such as emotions, subjective norms, behavioral control, heuristics, or habits are also likely to influence self-disclosure (e.g., Heirman, Walrave, & Ponnet, 2013). (p. 371)

This argumentation combines the original privacy calculus assumptions while respecting its criticism at the same time. Therefore, in the present dissertation, the privacy calculus will not be considered as a completely rational approach, but rather as an approximation towards people's self-disclosure intentions and behaviors that is affected and distorted by several factors. Hence, both psychological and environmental factors that might impact the perception of privacy risks and benefits will be examined in the current dissertation. Studies I, III, and IV, for instance, investigate the privacy calculus with contextual and situational notions, respectively, and study IV scrutinizes the inner-psychological process of weighing risks and benefits.

3.4 Contextual and situational privacy

Online, obviously harmless personal information people would carelessly disclose offline, can lead to serious privacy invasions because information is aggregated from several sources and decisional inferences about users are made (Marwick & boyd, 2014; Nissenbaum, 2010; Solove, 2008). As stated above, people expect that the recipient of disclosed information will adhere to the principle of contextual integrity (Nissenbaum, 2010, 2018). Hence, in general, privacy behaviors are context dependent. Beyond the understanding of privacy as being a matter of context, another theory aims to describe Internet privacy behaviors as being the result of both context and situation. Masur's (2018) theory of *situational privacy and self-disclosure* provides very detailed understanding of online privacy. According to his approach, privacy perceptions and behaviors are tied to specific situations. Situations differ from contexts, as a context can be described as the "structured social setting" (Nissenbaum, 2010, p. 130) in which a situation is embedded. This means that if a person meets with his or her colleagues every morning in the coffee kitchen, the context will always be the same (provided that the colleagues are the same every morning), however, the situation will be a different one every morning. A situation can only be fully grasped if one knows the inner states of the individuals involved in the situation, like their perceptions, emotions, or motives (Masur, 2018). Additionally, non-situational factors like personality traits or attitudes determine situational decision making. This indicates that a situation adopts a psychological perspective whereas a context is a sociological concept (Masur, 2018). The theory is an important extension of previous studies that have frequently assessed

accumulated pictures of participants' privacy behaviors combining several situations (cf. Masur, 2018). Hence, privacy behaviors cannot be fully comprehended without knowledge of the context, but contexts can be considered independently of concrete situations. The investigation of both contextual privacy and situational privacy is important to understand how they impact subsequent behaviors. In the current dissertation, study I will explicitly investigate contextual effects on privacy behaviors and studies III and IV examine a situational perspective.

3.5 Online privacy perceptions

Many privacy theories have in common that they implicitly focus on people's perceptions of privacy. For instance, Altman (1975) noted that every person possesses an idea of one's optimal privacy level. Hence, when someone perceives having too much or too little privacy, one is inclined to reach one's personal optimum. This view is revived by the privacy process model (Dienlin, 2014). Dienlin (2014) argues that the more privacy people perceive to have in a situation, the more people will disclose about themselves. According to Trepte and Reinecke (2011), however, perceptions of online privacy often deviate from objectively measurable levels of privacy. They write:

> As long as online data (e.g., on social network sites) are scaled, mined, and sold, these data are not private and all utterances that may be perceived as psychologically or socially private are not private from an informational point of view. However, the users' subjective experiences have to be taken into account as well as the objective facts. (Trepte & Reinecke, 2011, p. 71)

Hence, it would be important for researchers to comprehend how different perceptions of privacy emerge. Dienlin (2014) states that each situation elicits a distinct perception of privacy in us both in the physical as well as in the digital world: "First comes the situation, second its perception and third the behaviour" (Dienlin, 2014, p. 114). Similarly, Masur (2018) puts forward: "The level of privacy is determined by the perception of the environment and is thus situational" (p. 138). Teutsch and colleagues (2018) "define privacy perceptions as individuals' situational experiences with and assessments of their given privacy level" (p. 4). These three quotes imply that people always possess a certain feeling how private a situation is. However, it is still an open question as no studies have yet empirically people's situational feeling of a situation's given privacy level (cf. Teutsch et al., 2018). As it has been described above, privacy threats are often invisible (Masur, 2018) which is why people might perceive more privacy than there actually is (Trepte & Reinecke, 2011). Hence, one objective of the present dissertation is the investigation of a situational influence on Internet users' situational privacy perception (Study III).

4 Privacy protection online

The last section dealt with Internet users' communication intentions and behaviors. However, this dissertation focuses on both self-disclosure and privacy protection among Internet users. Section 2.2 presented in detail why individual privacy online is heavily challenged. Büchi and colleagues (2016) note that "users' self-help privacy protection is gaining in relative importance, mainly because companies have an economic interest in user data and states are ill-adapted to keep pace with highly dynamic technological developments and corresponding know-how requirements" (p. 2). Therefore, understanding why Internet users already protect their privacy and how they might be motivated to protect themselves online even better is a crucial task and "could help to develop interventions that can create awareness, empower people, and help them to change their behavior when necessary" (Boerman et al., 2018, p. 3). Hence, illuminating individual online privacy decision-making is not only relevant for scholarship, but especially for giving practical advices to the public, and for politicians to design regulations and principles that are consistent with people's needs and behaviors. Because users often lack knowledge of and awareness for privacy threats online and because affordances and dark patterns might coerce users to reveal too much information, Krämer and Schäwel (2020) "posit that users need to be supported in order to not be 'tricked' into revealing more than would be beneficial when deciding rationally" (p. 70). A way to counteract such decisional biases would be the application of privacy protection strategies by individuals. Yao (2011) stated that "the burden of online privacy protection is primarily shouldered by an individual's own conscious effort" (p. 112). Therefore, it is extremely important to understand users' motivations to protect themselves and the underlying psychological mechanisms of different protection strategies. Generally, active protection strategies can be distinguished from passive ones (Ebbers, 2020; Matzner et al., 2016; Yao, 2011). Active privacy protection strategies include the active adoption of strategies or additional tools and software, for instance, to anonymize one's identity, block user tracking mechanisms, or encrypt information (Ebbers, 2020; Matzner et al., 2016; Yao, 2011). Passive strategies, on the contrary, comprise behaviors like withdrawal (Matzner et al., 2016), reliance on others (Yao, 2011), and avoidance (Ebbers, 2020). In addition, privacy protection can be divided into preventive and corrective (Lampinen et al., 2011) or pre- and post-disclosure strategies (Ebbers, 2020). However, researchers raise doubts towards the effectiveness of corrective strategies like asking a company to delete collected personal data (Lampinen et al., 2011). Another distinction concerns the earlier mentioned horizontal and vertical privacy axes (Debatin, 2011; Matzner et al., 2016): people can protect themselves against privacy threats

stemming from other users, for instance, by managing one's privacy settings and they can shield privacy risks of governments and institutions, for example by using a web-tracking blocker. The studies of this work focus on people's desire for more privacy protection, both active and passive protection intentions, and effects of transparency enhancement.

4.1 Enhancing transparency

Several approaches to support users' privacy decisions are proposed, among them privacy nudges (Acquisti et al., 2017; Wang et al., 2013), privacy seals (LaRose & Rifon, 2007), privacy icons (Efroni et al., 2019; Rossi & Palmirani, 2019), and privacy prompts (Schäwel, 2019). Whereas some of these approaches aim to alter people's behavior in a soft-paternalistic way (Acquisti et al., 2017), others aim to enhance transparency preserving people's decisional autonomy (Efroni et al., 2019). The increase of transparency is a special case for privacy protection and can be described as equipping users with information about the invisible processing of their personal data (Janic et al., 2013). Transparency does not automatically protect users' privacy but provides users with situational knowledge of privacy threats or how they can protect themselves by applying both active and passive strategies. Transparency can work as both a preventive and a corrective strategy. Some transparency enhancing measures are legally required (e.g., privacy policies), others are voluntarily and system-sided (e.g., privacy icons or seals), and again others can be actively adopted by users (e.g., tools like Lightbeam). Generally, transparency interventions aim to assist and support users in their online privacy choices (Acquisti et al., 2017). Hence, transparency can be seen as a basis for privacy awareness (Pötzsch, 2008) and subsequent protective behaviors (Janic et al., 2013).

On the legal and system side, privacy policies currently represent the common approach to transparency. In recital 58, the GDPR prescribes that "any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used" (*The protection of natural persons with regard to the processing of personal data and on the free movement of such data,* Regulation 2016/679). Many privacy regulations (like the GDPR) mainly focus on the *notice and choice* principle meaning that users are informed about the usage of their personal data and have to give active ("informed") consent about the use of their data (Warner & Sloan, 2013). However, scholars raise serious concerns about the practicability of the notice and choice principle (Matz et al., 2020) speaking of a *consent dilemma* (Solove, 2013) or *non-informed consent* (Bechmann, 2015). Hence, understanding the psychological nature of online privacy decisions is relevant for legislators since some of the current regulations imply a conception of Internet users that does not correspond to the reality (e.g., a completely informed and rational

user). This becomes apparent when looking at the heart of the notice and choice principle, privacy policies, which are by law intended to provide more privacy protection by informing users about the use of their data. However, they are often so long and incomprehensible that it seems irrational for users to ever read them. Although the GDPR prescribes comprehensible privacy policies, polls show that a majority of Internet users does not or only partly read privacy policies (European Commission, 2019). An empirical study revealed that it would take an adult about half an hour to read a standard-length privacy policy (around 8000 words), however, the medium reading time was about 74 seconds whereby more than 80% of participants spent less than a minute reading (Obar & Oeldorf-Hirsch, 2018). Therefore, the notion of informed consent is invalid in fact since "a website visitor's consent to a business's data collection and use practices is informed if the visitor has sufficient knowledge of the practices to make a reasonable evaluation of the risks and benefits of disclosing information" (Warner & Sloan, 2013, p. 7). However, most people give their consent without having *sufficient* knowledge of the underlying data processing (European Commission, 2019; Obar & Oeldorf-Hirsch, 2018). McDonald and Cranor (2008) calculated the time it would take a person in one year to read the privacy statement of every visited website once and came to a result of more than 200 hours. This number could even be higher today since the Internet is still growing and data processing is getting more complex. In conclusion, standard length privacy policies seem to be an impractical basis for an actually *informed* consent. Hence, the current dissertation aims to test the effectiveness of alternatives to provide transparency and raise awareness for online privacy threats and its effects on privacy decision-making (studies II and IV). Study III, for instance, directly addresses the criticism of too long privacy policies and examines whether Internet users would benefit from shorter policies.

4.2 Protection motivation theory

On one side, the studies of the present dissertation aim to focus on the effects of transparency enhancement. On the other side, participants' privacy protection (intentions) are targeted. A theory that is suitable to systematically examine online privacy protection (intention) is Roger's (1975, 1983) *protection motivation theory* (PMT). The theory was developed to understand how to increase people's motivation to protect against health risks and suggests that one way to persuade people to engage in self-protective behaviors are fear appeals (Rogers, 1975). Fear appeals are described to consist of different components that have a direct impact on the perception and assessment of the persons addressed: a fear appeal should contain information about the severity and probability of occurrence of a potential threat, and a recommendation of a possible protective measure. Ideally, these components of the fear appeal

should then lead to a high perception of threat seriousness, an assessment of high threat susceptibility, and the appraisal that the recommended response will be effective in shielding the threat (Rogers, 1975). Hence, people will be motivated to engage in protective behavior, if they perceive the threat to be severe, to be vulnerable towards the threat, and a protection strategy as effective. In a revised version of the theory, Rogers (1983) more elaborately describes the theory by adding further components and by separating two distinct cognitive processes. One process includes the perceived rewards of a maladaptive behavior like brain stimulation by smoking cigarettes and the perceived severity and vulnerability of, for instance, suffering from lung cancer. Hence, the perceived rewards and risks are balanced against each other. If one, for instance, appreciates the company of other smokers during the coffee breaks, this person will be unlikely to quit smoking, provided that the perceived health threat does not outweigh this reward perception. The second cognitive process comprises the perception that quitting smoking prevents getting lung cancer (i.e., response efficacy), the perception to be actually able to perform the protective behavior, in this example quitting to smoke or smoking less (i.e., self-efficacy), and the perception of costs that arise from the protective behavior (i.e., response costs), which could be fear of withdrawal symptoms.

Transferred to the field of privacy online, the theory has several implications. First, there is the notion of perceived rewards of a maladaptive behavior. Because online privacy behaviors are not maladaptive in the original meaning of the term, they should be referred to as reward perception of online behaviors that might negatively affect privacy. At this point, it is also important to note that privacy behaviors like self-disclosure and individual privacy protection are not two extremes on a continuum but are two rather independent behaviors (Büchi et al., 2016) unlike maladaptive health behaviors like smoking cigarettes (which would describe one behavior on a continuum ranging from smoking to non-smoking and including all intermediate steps). However, people can highly protect their privacy and simultaneously disclose huge amount of personal information. Moreover, there is the threat perception which consists of the perception of severity and likelihood of potential privacy threats. This notion of opposed benefits and threats resembles the privacy calculus approach (Culnan & Armstrong, 1999). In addition, there is the perception of the response towards the threat. People have to perceive privacy protection as actually effective, they have to believe that they are themselves capable of performing the protective behavior, and they have to perceive the costs of adopting a protective response to be low. Rogers (1983) stated that both threat appraisal and coping appraisal must be high so that people are motivated to protect themselves. Boerman and colleagues (2018) empirically investigated different protection behaviors among Internet users

while applying the PMT. They found that participants' perception of privacy threat severity and their appraisal of the effectiveness of the protective measures were predictors of privacy protection. Dienlin and Metzger (2016) extended the privacy calculus framework by integrating parts of the PMT (i.e., privacy protection motivation and privacy protection self-efficacy). They showed that this extended privacy calculus framework is useful to predict both self-disclosure as well as self-privacy protection of Facebook users. They investigated a protective behavior which they called self-withdrawal. "Withdrawal can be determined by physical aspects such as clothes, walls, or spatial distance; similarly, withdrawal can also be determined by immaterial aspects such as choosing not to disclose certain information (Westin, 1967)" (Dienlin & Metzger, p. 3). In their empirical study they found that whereas perceived benefits were the main predictor of self-disclosure, privacy concerns were the main predictor of self-withdrawal. These findings indicate that both the privacy calculus and the PMT are applicable to the field of online privacy behaviors. Although the privacy calculus will be the theoretical foundation of this thesis, the PMT will be the theoretical foundation of study II. Fortunately, the privacy calculus and the PMT are complementary theories which is why investigating both self-disclosure and privacy protection can reveal insights on both theorical approaches simultaneously.

4.3 Privacy resignation

Rogers (1975) noted that people who think that nothing can be done to protect themselves, will not engage in protection behavior. In privacy research, a similar notion can be found in concepts like privacy cynicism (Hoffmann et al., 2016; Lutz et al., 2020), privacy fatigue (Choi et al., 2018), online apathy (Hargittai & Marwick, 2016), and surveillance realism (Dencik & Cable, 2017). Privacy cynicism has been defined "as an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile" (Hoffmann et al., 2016, Introduction, para. 4). Choi and colleagues (2018) describe privacy fatigue resulting from a perceived lack of control, resignation, and an excessive demand with the manifold possibilities to protect oneself online. They found that people who were privacy fatigued had an increased intention to reveal personal information and a decreased willingness to protect their privacy. Lutz and colleagues (2020) showed that privacy resignation was associated with a decrease in privacy concerns and a reduced engagement in actual protection behavior. This decrease in privacy concerns, however, does not result from a reduced privacy risk awareness but rather represents a coping mechanism (Hoffmann et al., 2016). In fact, researchers found that resignation corresponds to a high risk or surveillance perception combined with the feeling of powerlessness (Draper & Turow, 2019;

Hoffmann et al., 2016). Therefore, a high perception of privacy threats does not always result in better protection attempts but can also lead to less thoughtful privacy behaviors when people think that privacy protection is needless. Thus, two studies of the current work (directly and indirectly) address the concern of privacy resignation and its effects on self-disclosure and privacy protection. Nevertheless, the present thesis mainly aims to investigate potential means to empower users with knowledge and to potentially overcome privacy resignation.

Altogether, this work will make various attempts to advance research on privacy protection. Different means to increase transparency and knowledge about potential privacy threats will be tested. This also includes the examination of a fear-appeal as described by Rogers (1983). Moreover, different privacy protection intentions and behaviors are assessed. Finally, one study will focus on participants' desire to have their personal data better protected online.

5 Research Objectives

It has been outlined that threats to people's privacy online are manifold, yet abstract and intangible (see section 2.2). Moreover, as depicted above, one widely applied approach to online self-disclosure decisions—the privacy calculus—is criticized for several reasons (see section 3.3 ff.). Consequently, the two superordinate aims of the current dissertation are to extent the comprehension of the privacy calculus approach and the application of stimuli that can raise participants' awareness for privacy risks. Hence, all studies investigate participants' self-disclosure intentions or behaviors and their privacy protection intentions and/or a form of transparency-enhancing stimulus. The majority of studies investigating online self-disclosure focused on one specific context, for instance, social media (Dienlin & Metzger, 2016; Dienlin & Trepte, 2015; Krasnova et al., 2010) or commerce (Dinev & Hart, 2006). Hence, the present dissertation aims to draw a broader picture and consider multiple contexts (simultaneously). Thus, contextual and situational perspectives are adopted in the studies to investigate how self-disclosure and privacy protection might vary in different contexts and situations, respectively. Moreover, rather stable factors like beliefs and personality traits are part of the studies. Figure 1 constitutes the amalgamation of the hypothesized relations of all four studies and illustrates the combination of situational (Masur, 2018), contextual (Nissenbaum, 2010), and stable factors.

Dienlin and Metzger (2016) expanded the privacy calculus by a privacy protective behavior. Hence, one aim of study I is to investigate whether the privacy calculus framework would also be suitable to predict privacy protection behaviors outside of social networking sites. It is argued that people feel a general desire for more privacy protection on the Internet (Schäwel, 2019) which impacts their willingness to use active protection strategies. Moreover,

because Bol and colleagues (2018) found the privacy calculus to be context independent, another aim of study I is to test whether privacy protection would also be independent of different contexts.

Focusing primarily on participants' privacy protection motivation, study II aims to investigate Facebook users' privacy behaviors by means of the protection motivation theory (Rogers, 1975, 1983). Still, the study is able to make statements about the privacy calculus. Additionally, a fear appeal as described by Rogers (1975) in the form of a warning message is presented to participants as a special form of transparency enhancement. According to the PMT, inducing fear of weak privacy settings should lead to an increased threat appraisal and protection motivation. Since previous studies investigated only parts of the PMT (Dienlin & Metzger, 2016), did not include fear appeals in their studies (Boerman et al., 2018), or investigated fear appeals loosely of the PMT (LaRose & Rifon, 2007), study II will include the theory as a whole.

Study III is designed based on the criticism on privacy policies. As most people do not read privacy policies or only skim parts of it (European Commission, 2019; Obar & Oeldorf-Hirsch, 2018) because it would take ridiculously much time to fully read all necessary privacy policies (McDonald & Cranor, 2008), it will be tested whether shorter privacy policies could be a suitable solution to enhance transparency among persons who register on a website. As a theoretical basis, a situational perspective on the privacy calculus (Masur, 2018) is adopted, investigating participants' subjective privacy perception of the give situation. Moreover, as most previous studies captured participants' intentions, study III assessed behavioral data.

Study IV, finally, aims to disentangle the privacy calculus on a within-person level. As the approach assumes people to rationally weigh risks and benefits, however, research indicates that people use different decision-making strategies (Hamilton et al., 2016; Scott & Bruce, 1995), it will be tested whether perceived benefits and privacy risks still impact self-disclosure intentions on an individual level. Moreover, different decision-making styles and privacy resignation will be investigated in relation to the privacy calculus in study IV. Finally, study IV examines another form of transparency enhancing tool that is inspired by a nutrition label. This nutrition label, the Nutri Score which indicates the level of healthiness by colors and letters, has been found to be most comprehensible when compared to other nutrition labels (Egnell et al., 2019). Since perceived risks or threats are a good indicator for protection behaviors (Boerman et al., 2018; Rogers, 1975) it was investigated how this score would affect participants' privacy risk perception and subsequent disclosure intentions.

In sum, the four studies of the present dissertation will contribute to the further theoretical and practical understanding of the privacy calculus approach, to people's intentions to protect their privacy online, and to possibilities of enhancing awareness for privacy risks caused by using the Internet.

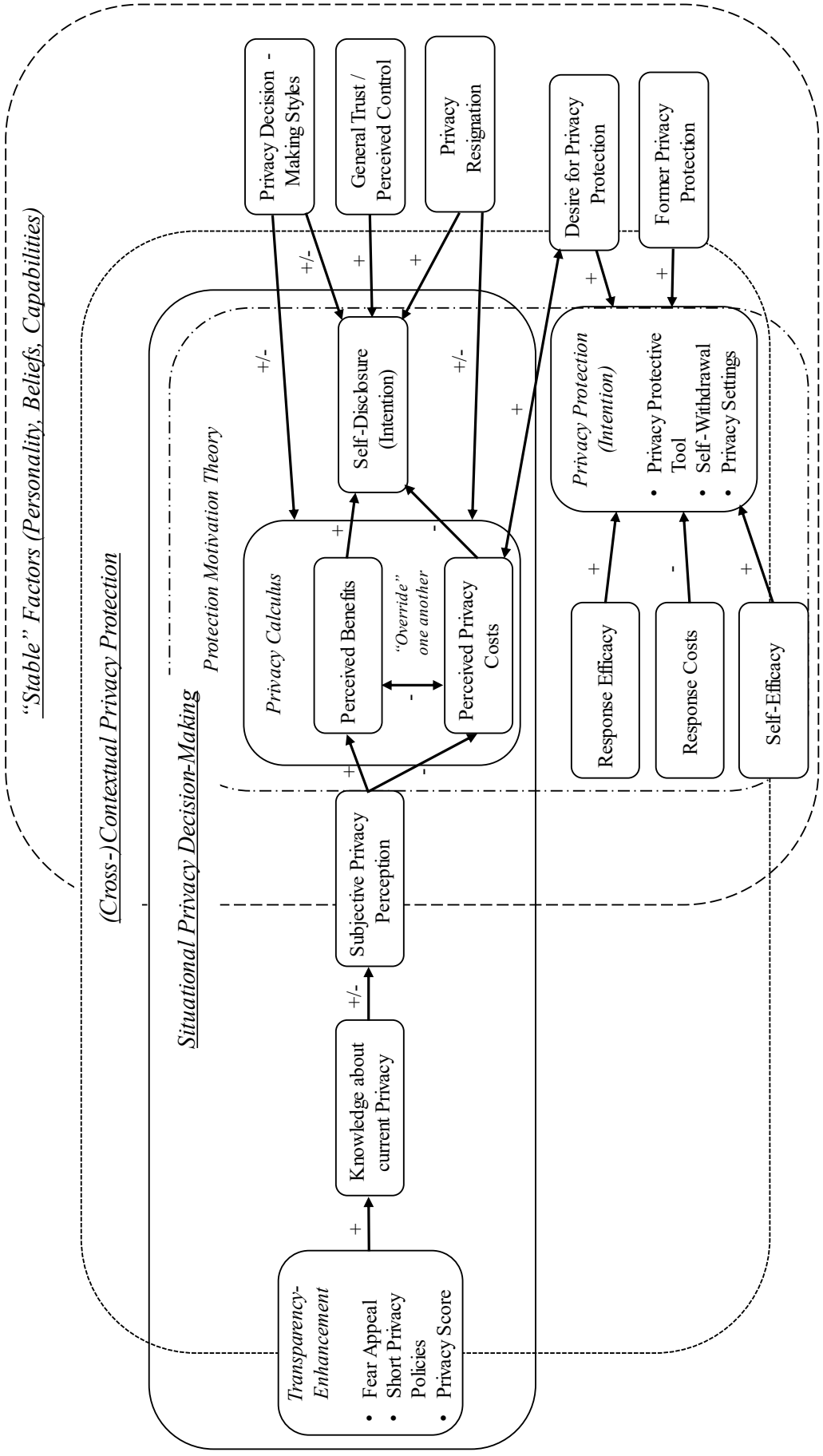

Figure 1. Conceptual Model connecting all four studies.

III SUMMARY OF THE RESEARCH PAPERS CONTAINED IN THE CUMULUS

The following chapter will provide extensive summaries of the four research articles of the current dissertation. Each of the articles covers an independent area under the umbrella of online privacy. Yet, all studies are related in that they investigate the privacy calculus framework and forms of privacy protection intentions and/or possibilities to enhance transparency.

6 Article 1: Between disclosure and protection: Internet users' desire for privacy protection and their intention to adopt a privacy-protecting tool within the privacy calculus

Internet users regularly disclose personal information in order to receive the various advantages websites and online services offer. So far, there is an overweight of studies that have investigated people's self-disclosure intentions and behaviors (e.g., Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2010). Moreover, many studies that examined privacy protection did not assess people's self-disclosure (e.g., Boerman et al., 2018; Büchi et al., 2016). However, self-disclosure and privacy protection are not exact mirror images but are rather independent (Büchi et al., 2016). Hence, to receive a more complete picture of both disclosing as well as protecting behaviors and behavioral tendencies and its underlying psychological mechanisms, it is important to examine both privacy behaviors in one study. In this respect, Dienlin and Metzger (2016) showed that the privacy calculus that assumes people to weigh privacy risks and benefits before disclosure can be suitable to predict both self-disclosure and privacy protection of Facebook users. They found privacy concerns to be positively related to participants' intention to protect their privacy on Facebook by self-withdrawal. Hence, the present study aimed to test whether the privacy calculus framework would also be applicable to predict privacy protection and self-disclosure in contexts other than the social one. Further, because people are motivated to engage in privacy regulations when they perceive to have too little privacy (Altman, 1975; Dienlin, 2014), and many people seem to have high privacy risk perceptions and privacy concerns (Bol et al., 2018), it was argued that people develop a wish to have more online privacy protection. This *desire for privacy protection* (Schäwel, 2019) might be a driving factor for Internet users to engage in privacy protective behaviors. Hence, we argued that the same factors (i.e., privacy risk perception, trust in a website, perceived control over personal information, and perceived benefits) that would impact participants'

intention to self-disclose could also affect the desire for protection which would then impact their intention to use a privacy protecting tool. Figure 2 provides a schematic overview of study I.

Additionally, and because a previous study found the privacy calculus to be stable across three different contexts (operationalized as different kinds of websites; Bol et al., 2018), another objective of this study was to examine whether self-disclosure and the desire for protection would be stable across three different contexts. Based on the theory of contextual integrity, it can be argued that although privacy behaviors are context specific (Nissenbaum, 2010), they are still affected by a cost-benefit calculation in every context (cf. Bol et al., 2018). Finally, it was of interest to investigate whether the contexts, and characteristics of the privacy protecting tool (developers: non-profit vs. profit organization; data collection: tool collects user data vs. tool does not collect user data) would influence the hypothesized relation between participants' desire for protection and their willingness to use the privacy protecting tool.

In a scenario-based online experiment, 511 participants were recruited and randomly assigned to the experimental conditions. Participants were instructed to imagine visiting three different kinds of websites (social networking site, e-health website, e-commerce website). Next, they should think of using a privacy protecting tool when visiting the same websites again. The tool was described to provide both increased privacy protection and transparency of how the website affects user privacy. The scenarios' realism was increased by showing a mockup of the tool. Tool developers and data collection of the tool were varied. Hence the study comprised a 3 (context) x 2 (source) x 2 (data-record) between-subjects design. Results were analyzed in a structural equation model with additional multigroup analysis.

Independently of the manipulations, results supported the assumptions of the privacy calculus: perceived privacy risks were negatively, and perceived benefits positively related to participants' self-disclosure intention. Perceived control but not trust was positively related to self-disclosure intention. Participants' desire for privacy protection on the Internet was found to be very high and was positively predicted by perceiving privacy risks and negatively by trust in websites and perceived control over information. Benefit perception and the protection desire were unrelated. Respondents' who stated to wish better privacy protection were did not have a decreased self-disclosure intention but were slightly more likely to use the portrayed privacy tool. Concerning the manipulations, results revealed a context-dependency of the privacy calculus predicting self-disclosure. In some contexts, perceived privacy risks, trust, perceived control, and perceived benefits were related to self-disclosure in others not. No context-dependency, however, was found for the effects predicting the desire for protection and the

relationship between participants' protection desire and their willingness to use the privacy protecting tool. Moreover, respondents who wished to have better online privacy protection made no distinction between a tool that was developed by a profit or non-profit organization. However, participants with a high desire for protection would forego using the tool when it collects their data for better protection efficiency.

Study I revealed several interesting insights into Internet user's perceptions and motivations to both disclose personal data online and protect their privacy. First, results confirmed that the privacy calculus framework seems to be applicable for both privacy protective as well as revealing privacy behaviors (Dienlin & Metzger, 2016). As the privacy calculus predicts (Culnan & Armstrong, 1999; Dinev & Hart, 2006), perceiving privacy risks reduces one's disclosure intention whereas perceiving disclosure to be beneficial increases this intention. Thinking that control over information is maintained after its release was also positively related to participants' willingness to reveal personal data. However, unlike in previous studies (Bol et al., 2018; Culnan & Armstrong, 1999), trust that a website confidentially handles one's data was unrelated to information disclosure intention. By integrating a desire for privacy protection into the privacy calculus model, it was shown that privacy risk perceptions and the privacy protection desire are highly related which supported the notion that constant risk perceptions can lead to a desire to be protected from these risks. Trust in different websites and perceived control over one's own information can slightly decrease one's protection wish. People who desire protection are not less likely to disclose personal information. However, they were more willing to use the presented privacy protecting tool.

Another aim of the present study was to investigate whether the found effects would differ across different contexts (cf. Nissenbaum, 2010). The results contradicted the findings of Bol and colleagues (2018), who found the weighing of risks and benefits being stable across three different websites. In this study, the three contexts influenced whether perceived risks, trust, perceived control, and perceived benefits were related to participants' intention to self-disclose or not. Because self-disclosure, perceived risks, and perceived benefits were assessed on a general level it might, however, be that the found effects are an anomaly of these general measurement. Because each context should be perceived differently, different benefits and risks should lead to the disclosure of different types of information. The desire for protection, in contrast, was found to be stable across the three contexts. This makes sense because self-disclosure is rather a situational behavior (Masur, 2018), whereas the desire for better privacy protection and one's willingness to protect oneself by using a tool are rather cross-situational

and cross-contextual. Finally, users' desire for protection was related to their willingness to use the privacy protecting tool independently whether it was developed by a profit or non-profit organization. However, this relationship was only present when the tool was described to refrain from collecting users' personal information.

Altogether, study I extended previous research by investigating both participants' self-disclosure intentions and their privacy protection intentions together with their desire for protection. Whereas former studies investigated people's general need for privacy (Trepte & Masur, 2020), study I found that Internet users also highly desire privacy and its protection online. Although participants' desire for privacy protection was high, its impact on the willingness to use the tool was rather small and there was no relation to participants' self-disclosure intention which provided further evidence that disclosure and protection are rather independent behaviors (Büchi et al., 2016).

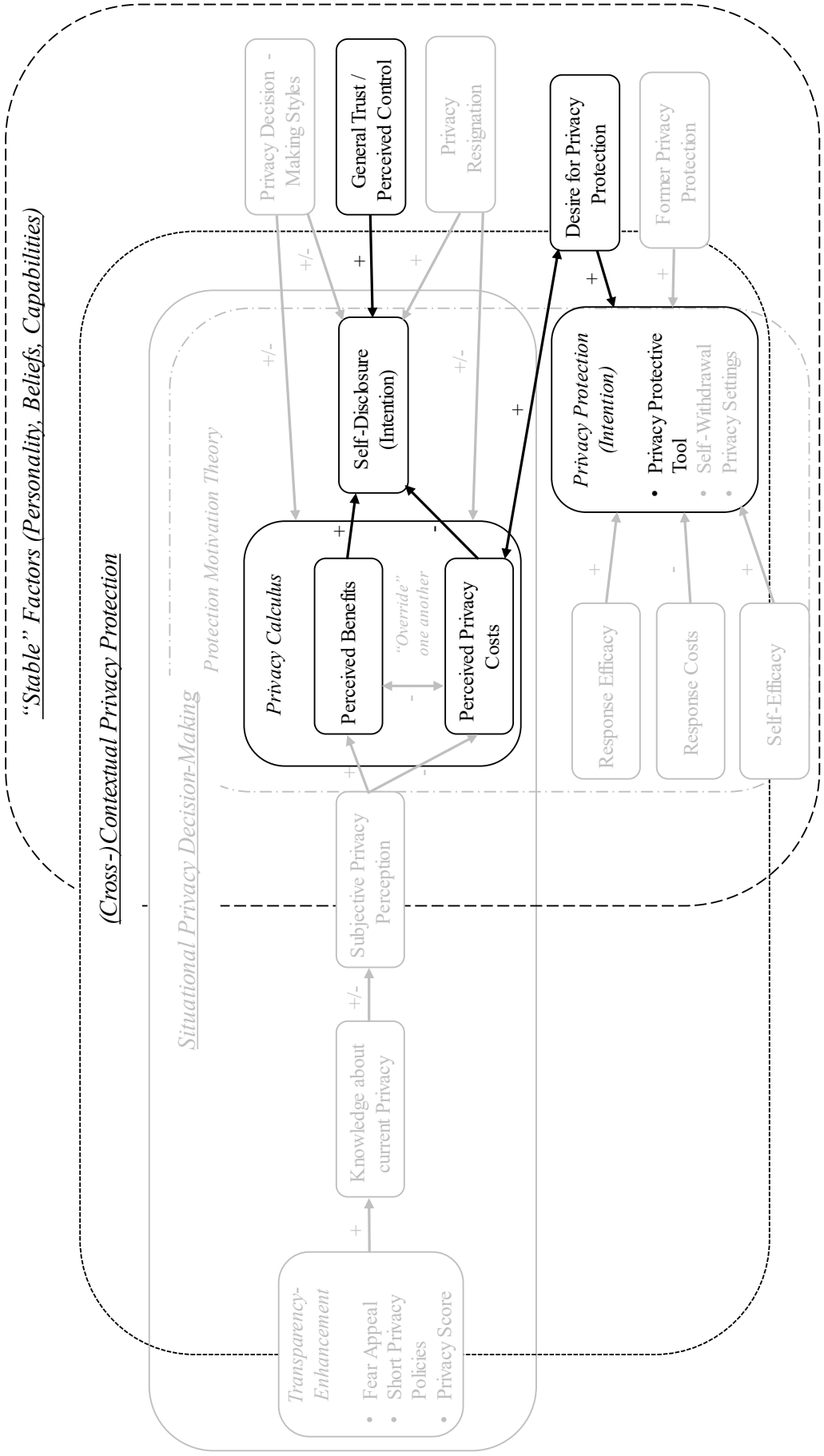

Figure 2. Schematic overview of study I.

7 Article 2: Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions

Whereas study I focused on participants' willingness to use a privacy protecting tool, study II targeted social media users' privacy protection motivation by confronting them with a fear appeal. In social media, one means to protect one's (predominantly horizontal; cf. Debatin, 2011) privacy is the usage of privacy settings. However, Facebook's privacy settings are complex, are regularly modified by the network, and are often very openly pre-set by default (Acquisti et al., 2015). Therefore, it was argued that Facebook users might benefit from regular status reports about how loosely or strictly their privacy settings are and whether risks might occur. One way of such a status report that might motivate users to better protect their Facebook privacy would be fear appeals. According to the protection motivation theory (Rogers, 1975, 1983) fear appeals must convey information of a threat's severity and likelihood as well as a protection response (see section 4.2 for more details). Moreover, previous studies showed that the perception of the protection behaviors of other individuals impacts one's own protection motivation (Spottswood & Hancock, 2017; Utz & Krämer, 2009). Hence, another main aim of study II was to integrate information of privacy protection norms into the fear appeal.

Previous studies either only included parts of the PMT into their analyses (Dienlin & Metzger, 2016) or they focused on privacy protection outside of Facebook (Boerman et al., 2018). Therefore, all constructs that were described by Rogers (1983) to be relevant in increasing or decreasing people's protection motivation were measured in study II. Similar to the notions of the privacy calculus (Culnan & Armstrong, 1999; see section 3), Rogers (1983) assumed that people balance the anticipated rewards of a behavior that entails a potential threat against their perception of this threat (i.e., severity and likelihood of occurrence). This cognitive process is termed threat appraisal. In a second cognitive process, the coping appraisal, people must perceive the response behavior as effective, their own ability to engage in the protective behavior to be given, and the costs of the response behavior to be low in order to be motivated to protect oneself (Rogers, 1983). Both threat appraisal and coping appraisal must be high, otherwise people would not be motivated to engage in self-protective behavior. In addition to these variables of the PMT, previous protection behavior on Facebook was hypothesized to be related to people's protection intention, since a previous study found protection behavior to be quite stable (Boerman et al., 2018). Like in study I, both self-disclosure intention as well as participants' protection intention (measured as self-withdrawal; cf. Dienlin & Metzger, 2016) were integrated in study II.

304 participants of an online experiment were included in the analyses. Participants were randomly assigned to the experimental conditions of a 2 (fear appeal vs. neutral appeal) x 3 (high norms vs. low norms vs. control) between-subjects design. At first, participants should indicate their normal protection behavior by means of several items that primarily resembled the choices Facebook's privacy settings provide. After this, they saw the fear or neutral appeal including information on social norms which they should believe would be based on their previous protection behavior. Data were analyzed in regression analyses and analyses of variance.

Results showed that neither the fear appeal nor social norms had an impact on privacy threat perception, self-withdrawal intention, and self-disclosure intention. However, analyzing the PMT variables revealed that some of the theory's predictions are applicable for privacy protection on Facebook. Self-withdrawal intention was positively predicted by participants' privacy threat perception, response efficacy perception, and previous protection behavior. Self-disclosure intention, in contrast, was positively predicted by participants' benefit perception and self-efficacy and it was negatively predicted by privacy threat perception and previous protection behaviors.

Although, the fear appeal did not lead to any significant effects in participants' perceptions or intentions, study II revealed several useful insights into Facebook users' self-disclosure and privacy protection behaviors. First, it was found that the perception of online privacy threats is a reliable predictor of online privacy protection motivation which is in line with previous studies (Boerman et al., 2018; Dienlin & Metzger, 2016). Moreover, thinking that protecting one's privacy on Facebook by means of its privacy settings is really effective in shielding privacy threats (i.e., response efficacy) was also positively related to respondents' intention to protect oneself. This corresponds to Rogers (1983) notion that both threat appraisal and coping appraisal contribute to protection motivation. Eventually, previous protection was also largely contributing to participants' future protection motivation indicating that privacy protection once adopted is a rather stable behavior. This was also found by Boerman and colleagues (2018) for general online privacy protection. Hence, it seems that some Internet users generally engage in better privacy protection attempts than others. Concerning self-disclosure, privacy calculus assumptions were found (Culnan & Armstrong, 1999; Dinev & Hart, 2006). This means that perceived privacy threat reduced participants' willingness to provide personal information whereas the anticipation of receiving benefits by disclosure increased their intention to reveal personal information. The effect of perceived benefits was larger than the effect of perceiving privacy threats confirming previous observations (Bol et al.,

2018; Dienlin & Metzger, 2016). Interestingly, believing that one has the abilities to protect one's privacy on Facebook led to an increase in participants' self-disclosure intention but was unrelated to self-withdrawal. This finding contradicts previous results (Dienlin & Metzger, 2016). We explained this finding by arguing that persons who have a high self-efficacy might either be actually better protected, or they might misperceive their actual protection and have a false sense of protection. Both scenarios could than lead to a higher disclosure (cf. Brandimarte et al., 2012). Finally, participants' previous protection behavior decreased their willingness to disclose personal information.

All in all, study II provided some important contributions to understanding the privacy behaviors of social media users. Perceiving one's privacy being threatened and thinking that something can be done to protect one's privacy are important factors for an increased protection motivation. Contrary, perceiving high benefits of social media use but also believing that one is able to engage in effective protection behaviors leads to an increase in self-disclosure intention. Although the fear appeal did not influence participants' perceptions and intentions, we argued that it is extremely important to provide social media users with information about privacy threats, their current protection level, and potential coping responses.

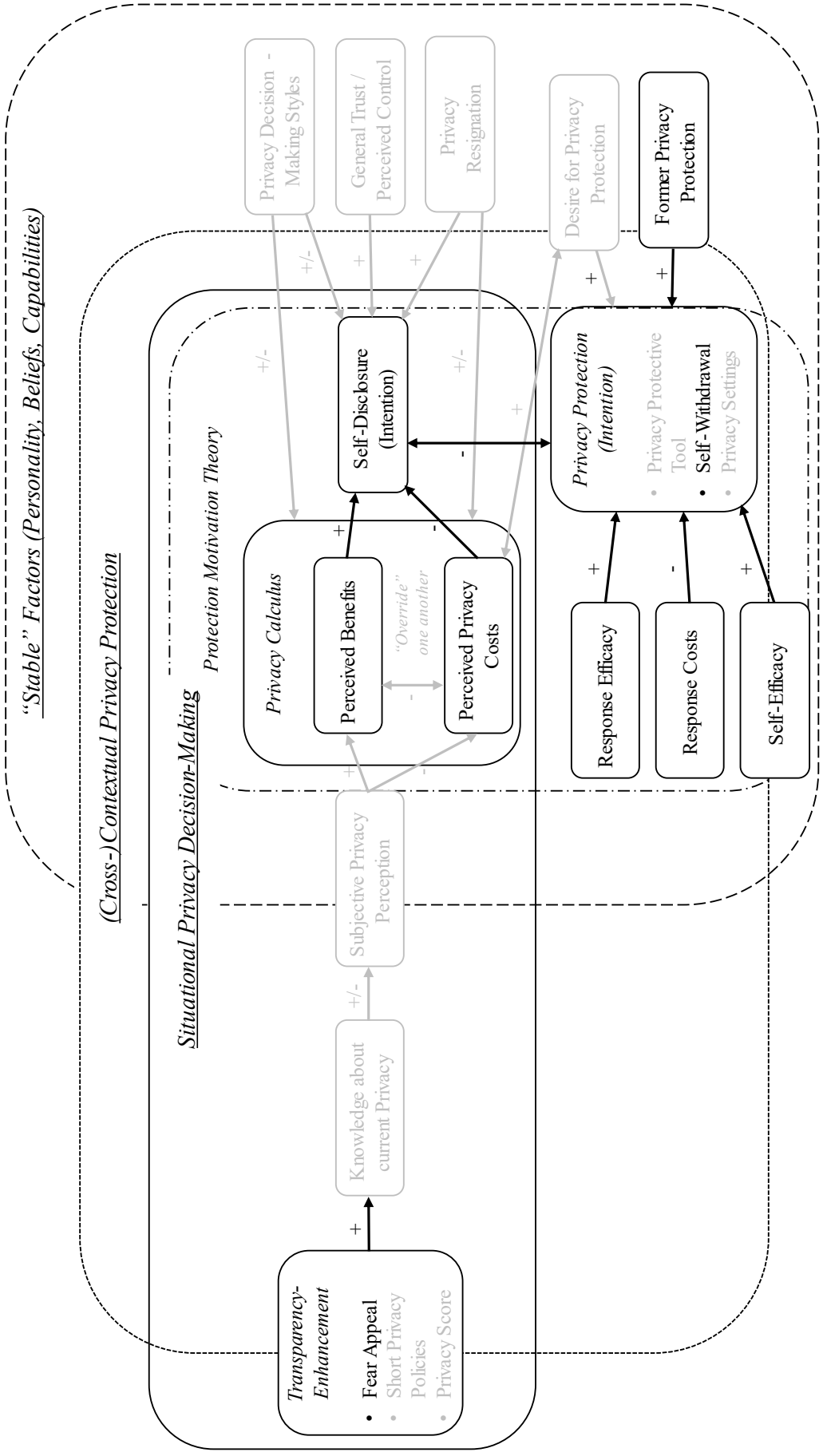

Figure 3. Schematic overview of study II.

8 Article 3: The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making

Studies I and II focused on protection and transparency providing tools users can apply as a form of privacy protection strategies (Matzner et al., 2016) assessing participants' behavioral intentions. Study III aimed to assess actual user behavior and to scrutinize a form of transparency provision that is governmentally prescribed, i.e., privacy policies (see section 4.1). Privacy policies contain information about, for instance, which information a website collects, the reasons for data collection, how data are processed, for which purposes they are used, how long they are stored, and with which third parties they are shared. This means that, on the one hand, they serve to inform users of the degree of violation or preservation of privacy, but on the other hand they also serve to protect the responsible company from legal action, since it is proven that the data processing is legal. However, the usefulness of privacy policies in terms of providing transparency must be seriously questioned since both surveys and empirical studies find privacy policies to be impractical (Bechmann, 2015; McDonald & Cranor, 2010). In a recent survey, only 13% of respondents stated to fully read privacy policies (European Commission, 2019). Empirically, Obar and Oeldorf-Hirsch (2018) found that most participants spend very little time to read privacy policies which would be way too little to comprehend data processing even rudimentarily. The reasons for not reading or only scanning policies is that they are too long, incomprehensible, and use difficult language (European Commission, 2019). In study III, we argued that people are not motivated to engage in reading privacy policies because of too much anticipated cognitive effort (Lang, 2000, 2017). This notion is supported by the observation that information overload is one reason for spending less time reading policies (Obar & Oeldorf-Hirsch, 2018). Therefore, one of the major aims of study III was the investigation if short privacy policies are more practicable in providing transparency.

Theoretically, study III is built on Dienlin's (2014) privacy process model, Masur's (2018) perspective of situational privacy (see section 3.4), and the privacy calculus (Culnan & Armstrong, 1999; see section 3). Dienlin (2014) argued that people form a perception of privacy in every situation based on the situation's circumstances. However, perceptions of online privacy and real levels of online privacy can (and frequently do) diverge (Dienlin, 2014; Trepte & Reinecke, 2011; see section 3.5). Hence, one aim of the study was the investigation of whether short privacy policies can positively influence people's perception of privacy (in terms of a more realistic perception). People's subjective privacy perceptions were defined as the experience, sense, and evaluation of one's current level of privacy, accompanied by trust towards the information recipient and a perception of control over information and as the

perception of how well the information recipient protects personal data. Next, it was argued that these situational privacy perceptions would impact and distort people's perception and weighing of privacy risks and disclosure benefits (cf. Masur, 2018). These situational perceptions of risks and benefits were then hypothesized to lead to different amounts of self-disclosure (Culnan & Armstrong, 1999). As such, we modelled a process of information flow originating in reading (or not reading) the privacy policies of a website, which would elicit a situational perception of privacy, impact the weighing and experienced risks and benefits, and finally impact one's extent of disclosed personal information.

To investigate these assumptions, we asked participants of an online experiment to register on a self-made social networking site that was described to give personalized recommendations for various leisure time activities and connect with peers. Before respondents were asked to provide personal information to their profile page which would additionally serve to personalize the recommendations, they had the chance to read the network's privacy policy. In addition to the policies' length, the network's level of privacy was varied creating a 2 x 2 between-subjects design. 305 participants were included in the analysis of a structural equation model. Instead of the total reading time, we calculated the reading time participants spend per word.

Results indicated that the mere length of a privacy policy did not affect participants' amount of knowledge of the policy content. However, the short policies led to a significant increase in the reading time participants spend per word which then positively influenced their knowledge. Participants' knowledge impacted their situational perception of current privacy (negatively in the privacy intrusive condition and positively in the privacy friendly condition). Moreover, an additional path from policy knowledge to perceived risk likelihood had to be drawn based on model modification indices. The more participants knew the privacy policies' content, the more likely they assessed privacy risks in the intrusive condition and the less likely they assessed privacy risks in the friendly condition. Participants' privacy perception negatively impacted their appraisal of privacy risk likelihood and positively influenced their perception of network benefits. Finally, perceived benefits were found to increase the amount of disclosed information, however, the likelihood of privacy risks did not significantly reduce self-disclosure.

Study III found further evidence for the impracticability of privacy policies in its current form (European Commission, 2019; McDonald & Cranor, 2010; Obar & Oeldorf-Hirsch, 2018). Simultaneously, however, it was shown that shortening privacy policies to a possible minimum can be very advantageous for users. The results revealed that respondents who saw a

short privacy policy had a higher reading time per word which was associated with increased knowledge about the content of the policy. This indicates that reducing the density of information can reduce cognitive effort and motivate people to inform themselves about a website's privacy practices (Lang, 2017; Obar & Oeldorf-Hirsch, 2018). However, results also demonstrated that reducing the complexity and density of privacy policies is not a panacea in itself but that users are still responsible for obtaining sufficient information. Moreover, the study has several theoretical and practical implications. First it was shown that knowledge about the current level of privacy leads to a more accurate subjective perception thereof (cf. Dienlin, 2014). In other words, the more participants knew about the network's privacy principles, the more the subjective privacy level corresponded to the objective level (cf. Trepte & Reinecke, 2011). Additionally, knowledge led to a more realistic perception of privacy risk likelihood. Next, the more participants assessed the situation to be private, the more they perceived the network to be beneficial and the less likely they assessed privacy risks. This implies that situational experiences influence the privacy calculus as suggested by Masur (2018). Hence, the weights of privacy risks and benefits are not stable but fluctuate depending on the specific situation. Eventually, results did not support privacy calculus assumptions, i.e., that perceiving privacy risks reduces self-disclosure whereas anticipating benefits with disclosure increases disclosure (Culnan & Armstrong, 1999; Dinev & Hart, 2006). We proposed some possible explanations for the finding. It might be that privacy calculus assumption do not hold when analyzed with actual behavior but that they are only a post-hoc rationalization of behavior (Knijnenburg et al., 2017). However, a recent study demonstrated the opposite, showing that perceived risks were negatively related to actual disclosure (Dienlin et al., 2019). Hence, it might be a result of the artificial study situation (the effect from perceived benefits on disclosure was rather small, thus, participants might have felt pushed to disclose information as a part of the study), or it could be that only assessing perceived risk likelihood without severity is not sufficient in predicting self-disclosure. In general, participants' appraisal of the risk likelihood was not very high which also points to the possibility that participants have felt quite save because self-disclosure in the network was part of an experiment.

Altogether, study III revealed several important findings that are relevant to both theory and praxis. Reducing the length of privacy policies could be one means to enhance transparency by reducing users' cognitive effort and strengthen users' informational self-determination (Hornung & Schnabel, 2009). However, this would only be a first step since not all users would profit from this action. Moreover, it was found that knowledge about the given privacy level is a central determinant in privacy decision making as it directly affects a subjective privacy

perception which then impacts the perception of risks and benefits within the privacy calculus. Finally, perceiving more benefits increased the amount of disclosed data.

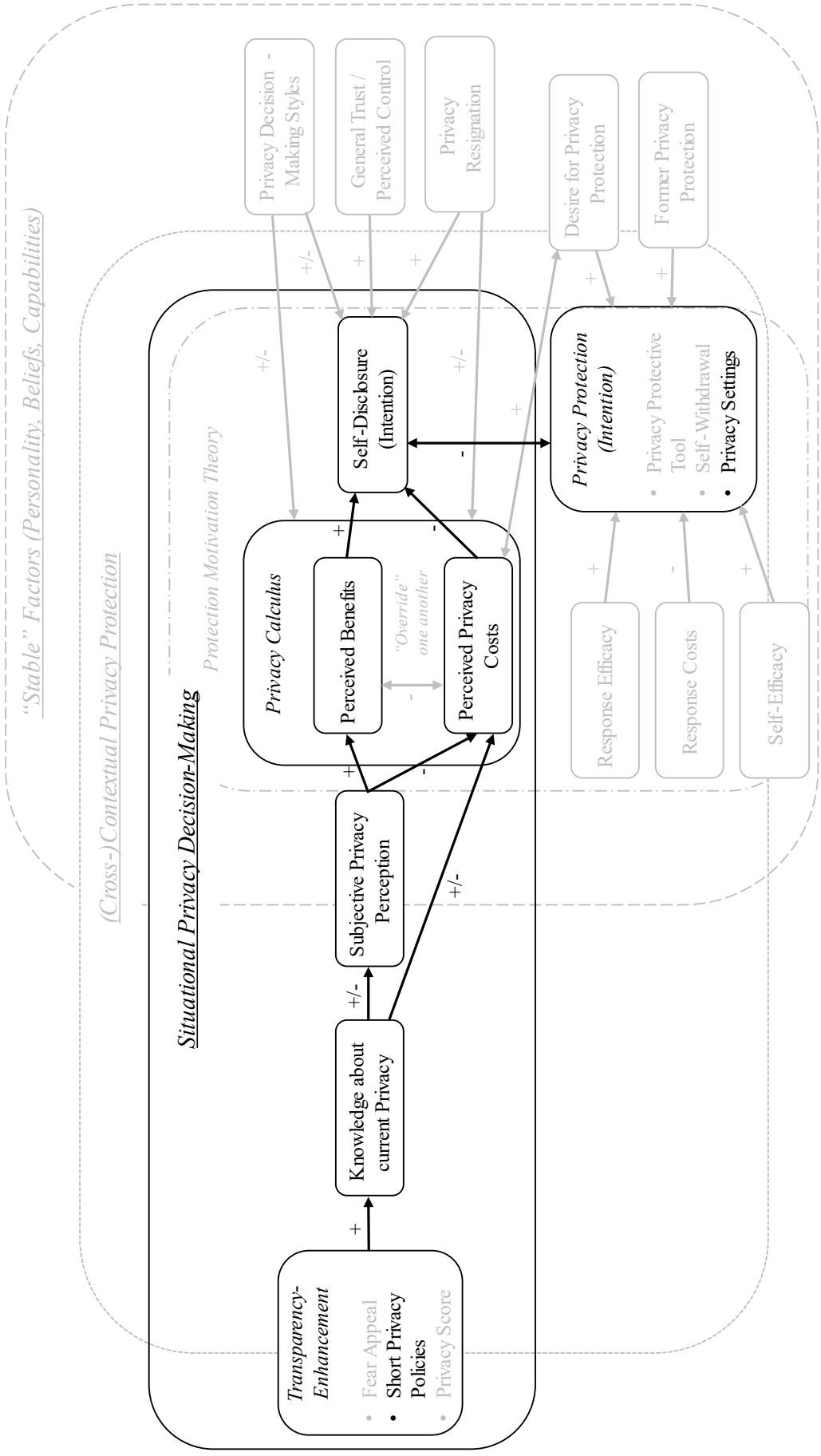

Figure 4. Schematic overview of study III.

9 Article 4: The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels

Whereas study I investigated Internet users' motivation to use protective tools, and studies II and III examined effects of threat induction and textual transparency enhancement, respectively, study IV aimed to investigate effects of a simplified transparency enhancing tool. Based on a nutrition label, a *privacy score* was tested displaying a website's privacy level with different colors. Moreover, the privacy calculus was scrutinized by investigating the approach on both between- and within-person levels, by examining the effects of a rational and intuitive privacy decision-making style, and privacy resignation (see section 4.3). This study aimed to further explore transparency enhancement (see section 4.1) as a possible means for more aware privacy decisions and to respond to the criticism of the privacy calculus (see section 3.3). The notion of the privacy calculus is that people weigh perceived privacy risks and perceived benefits before they decide to self-disclose (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Hence, this weighing process might differ in every situation as people's perceptions or environmental cues might change (cf. Masur, 2018). Research, so far, has investigated differences *between* individuals and not differences *within* one person. This means that former studies found people who anticipate more benefits than others to also have an increased self-disclosure intention, or people who perceive higher privacy costs than others having a reduced intention to disclose personal information (Bol et al., 2018; Dienlin & Meztger, 2016; Krasnova et al., 2010). However, the question of interest would be whether one person who perceives higher benefits in one situation also has an increased intention to self-disclose and if someone who perceives higher privacy risks than normally has a reduced willingness to disclose. Investigating within-person questions with between-person designs is not unusual in psychological research but can lead to errors (Hamaker, 2012). Hence, it is important to examine within person processes by looking at the within-subject variance. The assumptions made on the within person level were the same for the between person level, that is that perceiving higher privacy risks in a situation would lead to a decreased intention to reveal personal information whereas the perception of higher benefits would lead to an increase in a person's intention to reveal information. In addition, we hypothesized that a person's perception of privacy risks and benefits would be negatively related in one situation because former studies also found a negative association between privacy costs and benefits (Bol et al., 2018; Krasnova et al., 2010).

Due to the criticism of the privacy calculus approach, it was further argued that there are interindividual differences based on traits or beliefs. Hence, a rational and an intuitive

decision-making style were added to the analyses as well as privacy resignation. Some people rather base their decisions on deliberation and consider positive and negative consequences whereas others decide based on their intuition and gut feelings (Hamilton et al., 2016; Scott & Bruce, 1995) which is also reflected by two distinct operating cognitive systems (Bechara, 2005; Kahneman, 2003; Strack & Deutsch, 2004). Hence, some persons are more likely to make more rational choices whereas others tend to decide more intuitively. These different kinds of decision-making styles might lead to a different processing within the privacy calculus. We assumed that people who make rather rational privacy choices would have a higher risk awareness and a reduced self-disclosure intention (cf. Dienlin et al., 2019). Persons who make rather intuitive privacy decision were hypothesized to be more prone for short-term gratifications which would positively influence self-disclosure intention (cf. Ostendorf et al., 2020). Finally, it was argued that also state variables might affect the privacy calculus. In study IV, privacy resignation which constitutes a sub-facet of privacy cynicism was examined (Hoffmann et al., 2016; Lutz et al., 2020). It was argued that because some people are aware of constantly eroding online privacy, they resign to take protective measures or limiting their disclosure (Draper & Turow, 2019; Hoffmann et al., 2016). Hence, although resigned persons perceive high privacy risks, these perceptions would not lead to a decrease in disclosure intention.

In study IV, a privacy score was investigated as a means for potential transparency enhancement. This privacy score was a condensed version of the nutrition label *Nutri-Score* which provides consumers with easy understandable information about the healthiness of food products (Julia & Hercberg, 2017). The Nutri-Score that uses letters A to E and colors green to red to indicate healthiness was found to be more comprehensible than other nutrition labels that show more detailed information (Egnell et al., 2019). In study IV, the privacy score ranged from letters A (green) to C (red) to indicate a website's level of privacy. It was argued that the privacy score would impact people's privacy risk perception and that intuitive privacy decision-makers would find the score to be especially effective since they are not particularly aware of privacy risks (cf. Ostendorf et al., 2020).

To investigate the hypotheses, we asked participants of an online experiment to test a new browser tool (i.e., the privacy score) in three different situations. Participants were asked to imagine visiting three websites with three different goals while the privacy score showed a random category. The websites comprised a news-website, an e-health-website, and an e-commerce website. The reasons for visiting these websites (i.e., the benefits) were described in the respective scenarios. 485 participants were included in the analyses of a random intercepts

cross-lagged panel model (RI-CLPM) which allows to separate between- from within-person variance. Privacy decision-making styles and resignation were integrated as control variables.

The results revealed that the privacy score was a good means to enhance privacy risk awareness in each situation. The RI-CLPM showed that persons who perceived higher benefits than others had a higher self-disclosure intention than others. However, the relationships between privacy risk perception and self-disclosure intention as well as between privacy risk and benefit perceptions lost statistical significance when the control variables were added. Hence, participants who perceived higher privacy risks than others had neither a reduced intention to self-disclose nor a reduced benefit perception than other participants. On the within-person level, however, privacy calculus assumptions were found. A person who perceived higher benefits than in the other situations had an increased intention to reveal personal information and a decreased risk perception in that situation. If a person had a higher risk perception than in the other situations, self-disclosure intention was reduced. Further, the rational privacy decision-making style was found to be related to a higher perception of privacy risks, to a reduced perception of benefits and a reduced self-disclosure intention. However, for the intuitive style and for privacy resignation, no general patterns were found. Finally, intuitive privacy decision-makers found the privacy score more helpful.

Together, the findings of study IV contribute to the general understanding of online privacy decision-making. While differences between persons (except for the relation between benefit perception and self-disclosure intention) seem to be rather the result of personality traits and beliefs than of different perceptions of privacy risks, the inner-psychological process was found to be stable. Someone who perceived higher privacy risks in one situation had a reduced readiness to self-disclose in that situation. In contrast, a person who perceived higher benefits in a moment, had an increased disclosure intention. Moreover, the perceptions of benefits and privacy risks were negatively related which indicates a kind of weighing process in which one perception can override the other (Dinev & Hart, 2006) leading to an increased or decreased willingness to reveal sensitive data. Rational privacy decision-makers seem to have “natural” advantages as they generally perceive higher privacy risks, and sometimes lower benefits which is why they sometimes show a reduces intention to self-disclose. Intuitive privacy decision makers and resigned persons were not found to show such general pattern. Hence, they might sometimes more strongly react to benefits and sometimes more strongly react to privacy risks. Finally, the study found indications that some users groups might be in higher need for privacy protection as others. Given that intuitive privacy decision-makers are more prone to anticipated

benefits (Ostendorf et al., 2020), they might especially profit from privacy tools like the privacy score.

Altogether, study IV found that people indeed engage in a weighing of positive and negative aspects of self-disclosure which increases or reduces the likelihood of self-disclosure. However, it is unlikely that this process has a completely rational nature as it is probably still affected by biases and heuristics (Acquisti & Grossklags, 2005) and people differ in their decision-making styles. The results of this study point to the immense importance to provide people with easily accessible and comprehensible information of privacy levels since this could trigger the inner weighing process towards a more careful privacy behavior.

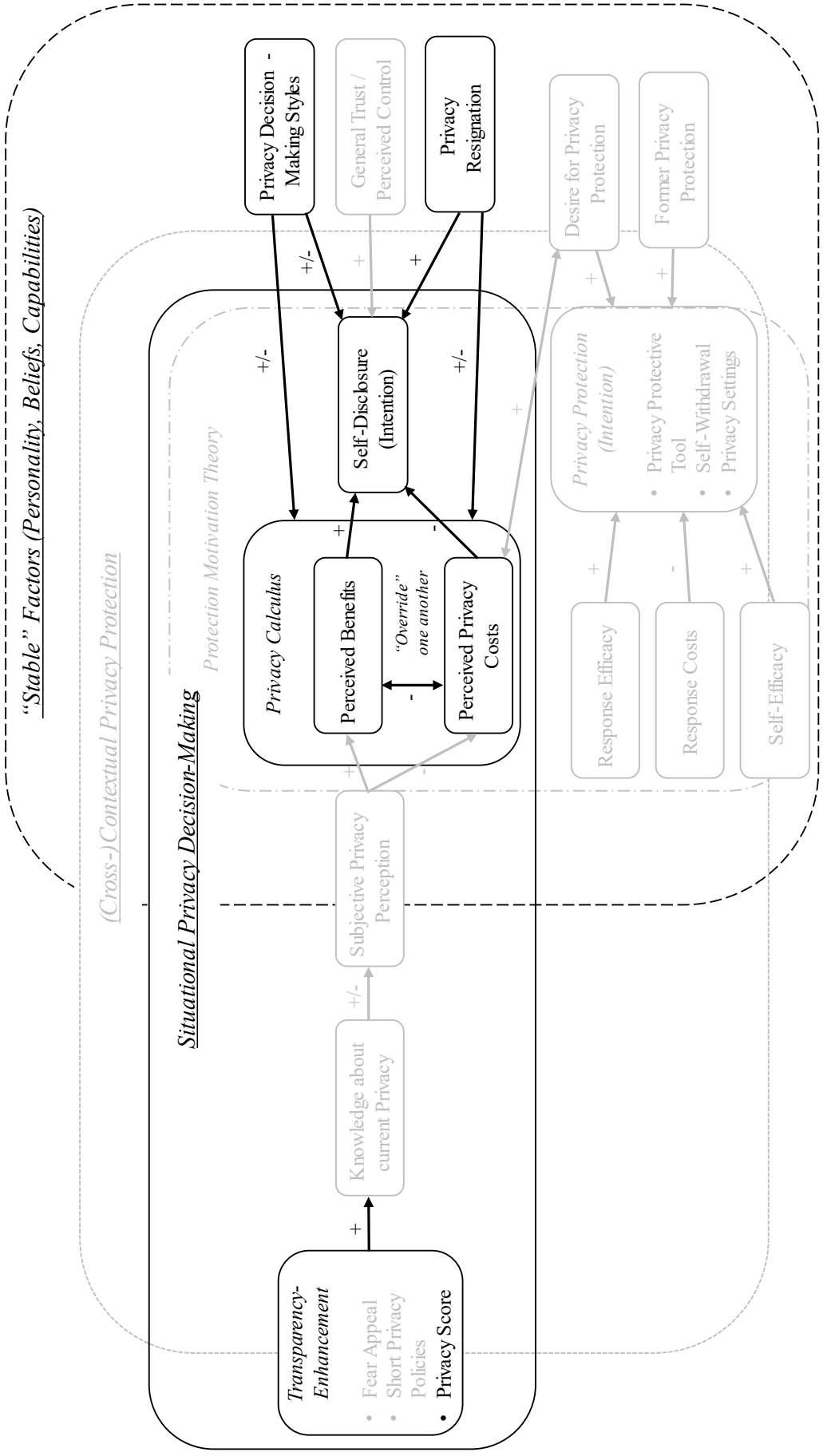

Figure 5. Schematic overview of study IV.

IV GENERAL DISCUSSION

The present dissertation aimed to investigate psychological mechanisms underlying self-disclosure and privacy protection on the Internet. This chapter will provide a broader picture of the four studies that were conducted as a part of this thesis. The implications and findings of the four research articles will be compared and reconciled. Figure 6 depicts a general overview of the results of all four studies and Figure 7 constitutes an alternative separation of the variables into the categories of stable, contextual, and situational factors.

10 Determinants of self-disclosure

One of the two main variables of interest within the current dissertation, was the active revelation of personal information. On that account, three of the four studies assessed participants' self-disclosure intention and one study captured actual self-disclosure behavior. This section will, therefore, carve out what the four studies found out about participants' online self-disclosure intentions and behaviors. In general, the studies found that participants' intention to reveal personal information was rather low. Assessing self-disclosure behavior, however, revealed that participants disclosed quite a lot: on average, about half of the possible input fields of the social network were filled. Before interpreting this descriptive observation, the nature of self-disclosure in the four study contexts must be identified. In study I, self-disclosure was described as a mix of disclosure to one of three websites and to the other users of these websites, whereas in study II, self-disclosure was purely social. Study III assessed participants' self-disclosure behavior to a social networking site, but also to the other users of the network. Finally, study IV captured people's intention to disclose personal information to three different websites. One explanation for the observation that participants' self-disclosure intentions were lower than their actual behavior is that it might be harder for participants to foresee their actual behavior when they are confronted with a hypothetical situation. A refutation of this logic is that participants might have felt a pressure to disclose personal information in study III as part of the study. In general, however, it should also be noted that disclosing personal information about oneself has inherently a rewarding nature (Tamir & Mitchell, 2012). Thus, in the perceived absence of privacy threats, disclosing personal information could also be beneficial without receiving external benefits. This might be underlined by the fact that privacy risk perception was not significantly related to disclosure behavior and even the positive effect of the perceived external benefits was relatively small.

The assessed benefits did not capture how rewarding the mere act of self-disclosure was, but whether practical benefits were associated with disclosure.

The overall goals of the present dissertation were to expand the understanding of psychological factors underlying Internet users' self-disclosure and privacy protection and the effects of transparency enhancement. These three major goals will be discussed in detail in the next sections.

10.1 Risk and benefit perceptions

All four studies assessed participants' perceptions of privacy threats and self-disclosure benefits. Three of the studies applied the privacy calculus framework (Culnan & Armstrong, 1999) and study II used the protection motivation theory (Rogers, 1975, 1983) which also assumes people to balance positive and negative aspects of a threat-entailing behavior. Hence, all four studies assessed one kind of privacy risk perception measurement and participants' perception of disclosure benefits. In study II, privacy risks were termed privacy threats (being a part of the PMT; Rogers, 1975) which, however, means effectively the same in the context of online privacy. Studies I and II showed that participants who perceived higher privacy risks (or threats) than others had a decreased willingness to reveal personal information. In contrast, those who perceived higher benefits of disclosure than others, had an increased self-disclosure intention. These findings are largely in line with the predictions made by the privacy calculus (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Laufer & Wolfe, 1977) and with the findings of several other privacy calculus studies (Bol et al., 2018; Dienlin & Metzger, 2016; Krasnova et al., 2010). Studies III and IV, however, could not replicate this pattern. In study III actual user behavior was assessed showing that only participants' anticipation of benefits was positively related to the amount of disclosed data. The negative association between privacy risk likelihood and self-disclosure was not significant. This might either be explained by the notion that the privacy calculus is not a description of actual user behavior (Knijnenburg et al., 2017) which, however, has already been shown in another study (Dienlin et al., 2019), or by participants' awareness of the artificiality of the study situation. Moreover, study IV that separated between- and within-person variance and further controlled for the influence of privacy decision-making styles and privacy resignation, did not find that privacy risk perceptions were negatively related to self-disclosure intentions or benefit perceptions on the between-subject level. This finding indicated that, for instance, persons who perceived higher privacy risks than others did not have a lower intention to self-disclose than others. This relationship was affected by different decision-making styles and privacy resignation. It is conceivable that, for instance, a person who relies on an intuitive decision-making style when

self-disclosing perceived higher privacy risks than someone else, however, does not have a general reduced intention to disclose than the other person. However, on the within-person level, privacy calculus assumptions were again found. Even more so, results did not only reveal that when a person perceived higher benefits in one situation, her self-disclosure intention was increased, and when she perceived higher privacy risks compared to other situations, her intention to self-disclose was decreased, but also that risk and benefit perceptions were negatively related. This means that someone who perceives higher privacy risks than usually has a decreased perception of disclosure benefits rendering self-disclosure unlikely. When someone perceives situationally increased benefits, one's awareness for privacy risks will descend, making self-disclosure more likely. Hence, study IV showed that privacy risk and benefit perceptions have the potential to override each other as implied by the privacy calculus approach (Dinev & Hart, 2006). Altogether, the four studies found support for the general privacy calculus assumptions of risk and benefit perceptions impacting self-disclosure. Moreover, study IV may be the first study that actually found empirical evidence for the "weighing process". This does not mean that the view of general rational privacy decisions was adopted or shown (see section 18.2 for a discussion of rationality and privacy online). However, perceptions of privacy costs and benefits seem to be in a kind of dialectical relation with one having the capacity to override the other. Despite the questions of rationality, the privacy calculus framework seems to be a very promising approach in explaining participants' willingness to reveal personal information both to other users (horizontal axis) as well as to websites (vertical axis).

Beyond that, the effects of perceived benefits on self-disclosure exceeded those of perceived privacy costs in studies I, II, and IV (in study III, too, but the relation between privacy risks and self-disclosure was non-significant) which was also found in prior investigations (Bol et al., 2018; Dienlin et al., 2019; Dienlin & Metzger, 2016). There are some explanations for this pattern: the benefits users relate to self-disclosure are the primary reason why the revelation of personal data is considered at all (Efroni et al., 2019). Hence, avoiding privacy risks is an obstacle for users to reach their goal of receiving the currently salient benefit. Moreover, benefits occur mostly immediately and with a very high certainty, whereas privacy risks are obscure, timely delayed, and uncertain (Masur, 2018). However, situations or objects in one's near future impact perceptions and behaviors to a higher extent than situations or objects in one's distant future (Trope & Liberman, 2010). In their construal level theory, Trope and Liberman (2010) argue that this is because of differences in one's *mental construals* (i.e., representations) of future events: the more an event is in the near future, the more concrete

one's mental representation of this event becomes and the higher its impact is on perception and intention. Contrary, people possess rather abstract representations for distant future events which barely affect perception and conduct. Hence, Internet users might have rather concrete mental representations of the benefits, but rather abstract representations of the privacy risks. As a consequence, benefit perceptions impact intentions and behaviors more than perceptions of privacy risks. A similar notion can be found in prospect theory (Kahneman & Tversky, 1979). The *certainty effect* basically describes that humans choose events with certain outcomes over events with uncertain outcomes. Although, the theory did not compare gains and losses but only gains or losses among each other, it may be transferred to the field of online privacy decisions. The benefits of sharing personal information are almost always completely certain and also known to individuals. Privacy risks, in contrast, are uncertain to appear and probably not entirely known to people. Hence, psychological theories can give plausible explanations why people often chose benefits over risks and do not behave *paradoxically* (see section 18.1). Further explanations include that people weigh anticipated benefits and perceived privacy risks but perceive benefits as high enough to take the risks (Trepte et al., 2015) or that heuristic processing leads to a distorted perception of benefits and risks and to a false sense of safety (Masur, 2018). Moreover, people could sometimes feel peer-pressure to use a certain website, app, or service (e.g., all friends of a person use a certain social network) or be obliged to use certain websites, apps, or services for their school, university, or job and therefore have no other option than to use the service and disclose personal information.

Summed up, perceptions of privacy risks and disclosure benefits were found to be reliable predictors of participants' online self-disclosure intentions. For actual user behaviors, no relation between risk perception and disclosure but only between the anticipation of benefits and self-disclosure was found. However, this finding is likely due to participants' awareness of the study situation as discussed above. In addition, changes in self-disclosure intentions within persons were found to be the result of a weighing process like implied by the privacy calculus literature. Differences between persons, however, seem to be the result of different personality characteristics or beliefs, rather than of differences in risk perceptions. Finally, the expectation of benefits is the major reason for individuals to reveal personal data whereas the avoidance of privacy risks is less important but not insignificant. Transferred to an actual situation, the following example can be illustrative. Imagine a person wants to buy a new sweater. Because she has little time to go to the mall, she browses the Internet and finds an object she likes a lot. In order to order the desired object, the selling company asks her to create a personal account on their website. She expects very high benefits from wearing the sweater one day and showing

it to her friends who will definitely tell her how stunning she looks. With only having the benefits on her mind, she refrains from reading the website's privacy policy and although she is aware of the fact that many websites use personal data for personalized advertisements, or disseminate them to other parties like data brokers, she discloses the required information to the company and gives her uninformed consent to data processing. Her friend has a similar affinity towards clothes and likes it to show off with newly bought clothing. However, she always informs herself about the downside of giving away personal information and carefully weighs the pros and cons which is why she would not have disclosed personal data to that website offering the sweater. This illustrates an example where a person discloses personal data to a website despite perceiving general privacy risks, because the benefit perception overrides a cautious privacy behavior in that situation. Moreover, the example illustrates that general different behavioral patterns determine behavior to a larger extent than the mere perception of privacy risks and benefits. When the person who bought the sweater needs to buy a birthday present for her nephew, she again approaches the Internet. This time her benefit perception is tied to the anticipated joy of her nephew when she hands him the present. She found some Lego toys on a website and knows that the child would enjoy playing with it. However, she also recognizes the website's poor data handling practices and continues her search until she finds another toy of which she also knows that her nephew's joy will be not less than with the first toy. In the second example of that woman, her privacy risk perception outweighed her perception of the benefit because there were other options in obtaining the gift.

10.2 Trust, perceived control, and perceived privacy

Study I expanded the privacy calculus framework by users' trust in different websites and their perception to be in control of how websites use one's personal information. Unlike in previous studies (Bol et al., 2018; Culnan & Armstrong, 1999; Dinev & Hart, 2006; Metzger, 2006), trust had no significant positive effect on participants intention to self-disclose. However, participants who believed that they could control how and for which purposes websites process their data, had an increased disclosure intention. This finding was in line with previous studies and conceptual works (Brandimarte et al., 2012; Culnan & Armstrong, 1999; Krasnova et al., 2010; Teutsch et al., 2018) and underlined that the feeling of being able to determine what happens to one's personal information is an important factor for (online) privacy (Altman, 1975; Burgoon, 1982; Teutsch et al., 2018). This also implies that misperceptions of how much control someone has in a given situation can easily lead to unintended consequences. Brandimarte and colleagues (2012) termed this observation the control paradox. They found participants whose perception to control personal information was

increased, sharing more personal information which resulted in effectively less privacy. Additionally, study I revealed a high positive relationship of perceived control and trust towards websites. Therefore, it was concluded that the two factors are not independent of each other, and that, although trust was not directly related to participants' self-disclosure intention, it might at least indirectly contribute to information sharing. This assumption leads to study III which assessed participants' situational assessment of the given privacy level. So far, studies have not directly investigated people's perception of situational privacy, although this variable has been indirectly part of lots of studies and conceptual works (cf. Dienlin, 2014; Teutsch et al., 2018). Teutsch and colleagues (2018) conducted an interview study in which they asked participants about their online privacy perceptions. In this study, results in combination with theoretical work revealed that perceptions of online privacy comprise a control perception as well as trust. Hence, in study III, participants' situational assessment of the given privacy level was a combination of trust, perceived control, a feeling of privacy, and perceived data protection. Results showed that these four variables build a very homogenous factor supporting the notion of study I that trust and perceived control are greatly related constructs rather than independent factors. Although participants' subjective perception of the current situation's privacy level did not have a direct effect on self-disclosure, it was negatively related to participants' risk likelihood assessment and their anticipation of benefits. Hence, the privacy perception (including trust and perceived control) had an indirect positive effect on self-disclosure. This finding further strengthens the point how important an accurate perception of privacy, trust, and control is to adequately determine one's online privacy behaviors.

10.3 Self-efficacy

In study II, results showed that self-efficacy was positively contributing to participants' intention to disclose personal information in their Facebook profile. Self-efficacy was assessed as part of the protection motivation theory (Rogers, 1985) and describes a person's belief that he or she is able to perform a certain conduct (Bandura, 1977). According to Bandura (1977), one's self-efficacy belief affects if a coping response is initiated, the amount of effort people spend on the coping response, as well as the duration of the coping response. In the context of online privacy, self-efficacy can be described as people's conviction of their own capabilities to protect their personal privacy online by shielding potential privacy threats. Lee and colleagues (2008) found that people who believed in their ability to shield computer viruses, had a higher intention to engage in virus protection behavior. In the field of online privacy, Dienlin and Metzger (2016) showed that Facebook users that possessed higher amounts of privacy protection self-efficacy, had a higher intention to self-withdraw. Self-disclosure

intention was not affected by self-efficacy. Hence, it is a rather unintuitive finding that privacy protection self-efficacy had no effect on self-withdrawal, but in contrast a positive effect on self-disclosure among Facebook users in study II. In the paper of study II, we proposed three different explanations for this observation. We argued that a person who believes she has the ability to protect herself, but who believes that protection is pointless (see section 4.3), does not engage in protection. Indeed, privacy resignation might also explain why individuals do not engage in protecting behaviors, but disclose personal information instead (Hoffmann et al., 2016). The second explanation comprised a positive relation between privacy self-efficacy and previous privacy protection: persons with higher self-efficacy already appeared to be better protected than others, and they may not be motivated to further protection because they perceive their current level of protection as sufficient. This explanation can also explain why people have an increased self-disclosure intention, because they do not perceive self-disclosures as risky (cf. control paradox; Brandimarte et al., 2012). The third explanation follows a similar line of argumentation. Persons with a high faith in their protection abilities could only think that they are better protected than others resulting in a false feeling of security. This idea can be recognized in the so-called *experience effect* describing the phenomenon that more experienced users have a reduced perception of privacy threats (Rifon, et al., 2005). Bartsch and Dienlin (2014) found that Facebook using time was negatively related to protecting behaviors: the more time people spend using Facebook, the less they cared to protect themselves. In sum, trusting one's own privacy protection abilities seems to be important for people to engage in protective behaviors at all. However, it can seemingly at times also lead to less protective privacy behaviors when people think they are well protected, when they are resigned, or when they lose protection motivation. In the future, studies should further investigate under which circumstances self-efficacy can lead to more or to less protective privacy behaviors.

10.4 Privacy decision-making style

In study IV, two privacy decision-making styles were assessed. Whereas persons who rather intuitively self-disclose were not found to have an increased or decreased self-disclosure intention, rational privacy decision-makers had a decreased intention to provide personal information on the vertical axis. The rational privacy decision-making style was described as a tendency to obtain sufficient information before making decisions and to weigh positive and negative aspects. This is in line with findings of Dienlin and colleagues (2019) who found that participants who claimed to have made more deliberate privacy choices, disclosed less information. An explanation for this pattern is that when people think longer about positive and negative aspects, privacy costs become increasingly salient. Dienlin and colleagues (2019)

found privacy deliberation being positively related to privacy concerns and in study IV results showed that rational privacy decision-makers perceived more privacy risks. Having a higher awareness for negative aspects of self-disclosure, increases the likelihood that perceived benefits are overwritten which leads to a decreased likelihood of self-disclosure.

11 Determinants of privacy protection

Whereas the previous section covered determinants of self-disclosure, this section will deal with determinants of privacy protection. Although limiting one's disclosure is also a form of protection, the section covers protection measures other than the non-disclosure of information. Study I assessed participants' willingness to use a privacy protecting tool, study II focused on Facebook users' intention to self-withdraw and use Facebook's privacy settings to shield horizontal and vertical privacy threats, and study III captured participants' protection behavior through privacy settings on a self-made social networking platform. In contrast to respondents' self-disclosure intention and behavior, their protection intention and behavior was rather high. The privacy tool that was described in study I was described as enhancing users' online privacy by automatically blocking common web tracking mechanisms and to enhance transparency by providing users with information about website's privacy practices. Descriptive results showed that participants' willingness to adopt the tool was relatively high. Self-withdrawal intention was assessed as participants' privacy protection motivation in study II. Self-withdrawal generally asked for several different privacy protective behaviors people can engage in to protect their online privacy, for instance, limiting profile visibility, not accepting friend requests, or deleting personal information. Study III revealed that people were rather likely than unlikely to restrict the range of their disclosures via a social networking site's privacy settings. Altogether, the studies found people's protection willingness and behavior was medium to high which rather contradicts findings of Boerman and colleagues (2018) who noted that Internet users "rarely to occasionally protect their online privacy" (p. 15). However, in contrast to the Boerman-study, the current studies used convenience samples that were rather young and highly educated which may have biased some of these findings. On a general level, however, Internet users seem to be willing to protect their online privacy (Boerman et al., 2018; Büchi et al., 2016).

11.1 Desire for privacy protection

People have a general need for privacy which is higher among some individuals and lower amongst others (Trepte & Masur, 2020). Study I examined whether Internet users also have a wish or desire to have their privacy better protected online. Because people are willing

to adjust their privacy when they desire more privacy than they currently have (Altman, 1975; Dienlin, 2014), it was argued that an awareness of Internet companies' data collection and processing practices may lead to uncomfortable feelings and the wish that companies or governments better safeguard personal information (cf. Schäwel, 2019). The results of study I showed that participants had an extraordinarily high desire for online privacy protection. While people's privacy risk perceptions and their desire for privacy protection were strongly related, participants who desired more privacy protection were only slightly more willing to use the privacy protecting tool than participants who do not wish better online safety. We proposed some explanations why people who wish for better privacy protection, might protect themselves only mildly better. First, people have various possibilities to protect their online privacy and using the tool was only one among many. Moreover, participants were put in a hypothetical situation and might not be motivated to use the hypothetical tool as they already have implemented high protection strategies. Second, people's desire for privacy protection could be targeted to companies or governments because people do not think that they have the capabilities to adequately protect their privacy. Third, some participants might have given up protecting their privacy because they do not believe that privacy threats can effectively been avoided (see section 4.3). Finally, the relationship was affected by one of the study's manipulations. Half of participants were told that the privacy protecting tool must itself collect personal information of its users to guarantee best possible privacy protection. Among those respondents who were told that the tool collects personal data, the desired protection was not related to the intention to us it. In the other group, the effect approached a medium size. Hence, whether protective tools are adopted also depends on characteristics of the software. Notwithstanding, study I showed that the desire for higher online privacy protection among Internet users exists and is very high. Moreover, it seems that individuals who feel a desire for more privacy protection are also more likely to engage in active protection strategies like using privacy and transparency enhancing tools (Ebbers, 2020; Matzner et al., 2016). However, the results also indicated that although the majority of respondents wanted to have more Internet privacy, they did not feel that they were in the right position to entirely realize this wish.

11.2 Privacy risk perception

The protection motivation theory suggests that perceiving a threat to the own person leads to an increased motivation to protect oneself from the threat (Rogers, 1975, 1983). As study II was based on the general idea to apply the PMT to the field of online privacy, participants' perception of threats towards their online privacy were assessed. Generally, a privacy threat was not considered to be different from a privacy risk as both cover potentially

unwanted negative consequences for user privacy. Hence, both risk perception and threat perception comprise people's perceived severity of a noxious or hazardous event and their assessment of the probability of occurrence of that event (Rogers, 1975; Rohrmann, 2008). Study II showed that participants' privacy threat perception was very high indicating that participants found it both severe and likely that they will experience privacy threats. The analyses found privacy threat perception being a good indicator of protection motivation on Facebook. Persons who perceived a severe and likely threat to their privacy, had an increased motivation to engage in protective effort. Although study I did not test the direct effect from privacy risk perceptions on respondents' intention to use the privacy protective tool, an indirect effect was observed. Because risk perception and the desire for privacy protection were largely related, persons who perceived major risks to their privacy were also more willing to use the protecting tool. Like in study II, participants perceived high risks to their privacy online. The results of study III did not support the implications of studies I and II. Here, participants were asked to register on a new social networking site and after they disclosed their information in their personal profile, they should specify their individual privacy settings. In contrast to the first two studies, study III assessed participants' estimated likelihood of privacy risks. However, persons who perceived privacy risks to be more likely did not restrict their privacy to a higher degree than those who perceived privacy risks to be less likely. In total, participants assessed privacy risks as moderately probable (about 50%). This means that they considered the chance that privacy risks would occur as large as the chance that they would not occur. Hence, we believed that because participants were aware that the registration process was part of an experiment, they might have not believed that actual privacy risks might happen to them or that their data would be used for purposes other than the study. Altogether, privacy threat or risk perceptions seem to be a good a reliable predictor of online privacy protection intentions and behaviors which is also stressed by the findings of further studies (Boerman et al., 2018; Dienlin & Metzger, 2016).

11.3 Response efficacy

Response efficacy was also investigated as a part of the protection motivation theory (Rogers, 1983) in study II. Response efficacy describes the belief that a coping response towards a threat is actually effective in shielding the potentially hazardous event. This notion shares some basal similarities with privacy cynicism and resignation since people who belief that protection is pointless will not engage in protective attempts (Draper & Turow, 2019; Hoffmann et al., 2016; Lutz et al., 2020). The PMT further assumes that people need to perceive both response efficacy and self-efficacy to be motivated to protect themselves (Rogers, 1983).

Other than predicted, only response efficacy was positively related to participants' self-withdrawal intention. Self-efficacy was surprisingly positively predicting their self-disclosure intention (see section 10.3). However, the general idea of the PMT that people have to believe in the effectiveness of the protective behavior was supported. Another study also found response efficacy but not self-efficacy being related to people's general online privacy protection behavior (Boerman et al., 2018). In conclusion, people do not only need to perceive privacy threats as severe and probable, but also protective attempts to be effective in shielding the threat. Hence, informing people about both risks associated with information sharing and Internet usage as well as effective means to bypass these risks would be crucial to support them in their online privacy behaviors (see section 17.4). This can be either achieved by supportive privacy tools, or by teaching people general media and privacy literacy (Bartsch & Dienlin, 2016; Livingstone et al., 2019; Masur, 2020; Trepte et al., 2015).

12 Privacy protection and self-disclosure

Büchi and colleagues (2016) noted that privacy protection and self-disclosure are not two extremes on a continuum but two distinct and rather independent behaviors. For instance, a person who is aware of online privacy threats, might use an additional browser tool to shield some of the online risks, however, continues to disclose personal data due to the anticipation of benefits. Another person might not apply privacy protection strategies but disclose as much as the first person. Hence, disclosure and privacy protection may be rather independent. The studies of the present dissertation indicate that disclosure and protection intentions and behaviors may be slightly negatively related. However, it gets also apparent that disclosure and protection are very different in nature (see section 13). Study II revealed that persons who stated having protected their privacy on Facebook well, had a lower intention to self-disclose personal information. Study III revealed a similar pattern. Participants who disclosed more information than others kept the privacy settings of the social network more public. This observation can be explained by the following logic. Whereas self-disclosure is driven by the anticipation of benefits and inhibited by the expectation of privacy risks, limiting access to the self by setting strict privacy settings might reduce the experienced benefits. As study II and III investigated social networking sites where the major benefits are social in nature (Christofides et al., 2009; Ellison et al., 2011; Khan et al., 2014; Taddicken, 2011), the benefit might be to express one's self to other persons. Limiting the visibility of disclosure would have lowered the expected benefit. Hence, one's motivation for horizontal privacy protection on social media can be reduced by expecting a high benefit. Similarly, Utz and Krämer (2009) found that persons who had a high motivation for impression management set less restrictive privacy settings.

Consequently, it can be expected that persons who perceive a high benefit of disclosure and rather little privacy risks would engage in less privacy protective behaviors when the protection effort leads to a reduced or no experience of the anticipated benefit. This notion is also stressed by findings of study I, where participants who wished to have better online privacy protection did not have a generally reduced intention to self-disclose. Thus, information revelation and protective efforts might be independent behaviors as long as the protective effort does not affect the obtainment of benefits. For instance, someone who uses an anti-tracking tool in his or her browser for an increased privacy protection will continue to use the tool until websites do restrict access due to the tool, loading of videos or webpages gets impaired, or browser performance decreases. In conclusion, whereas information revelation and privacy protection are rather independent, they depend on perceptions of privacy risks and benefits. Whereas privacy risks are one of the primary reasons for protection and benefits are the main reason for disclosure, risk perceptions can also reduce disclosures, and benefit anticipations can hamper protective attempts.

13 Context, situation, and privacy

As outlined in section 3.4, privacy behaviors are context- and situation-specific (e.g., Masur, 2018; Nissenbaum, 2010). According to Nissenbaum (2010), people perceive different privacy norms in different contexts, that means that they have certain expectations for which purposes disclosed data will be used. In accordance with these expectations, Internet users might be more motivated to protect their data in certain contexts. Hence, study I adopted a contextual perspective following the question whether self-disclosure or privacy protection would be different in three contexts (social, health, and commerce). In general, it was found that the assessed privacy calculus variables did not equally explain participants' self-disclosure intentions in the three contexts. Hence, in contrast to a former study that did not find the privacy calculus to be context specific (Bol et al., 2018) study I found a context specificity. This means that the perceptions of risks and benefits, perceived control and trust differed between the three websites leading to different disclosure intentions. The following attempts have been made to explain the findings. In each context, different kinds of benefits and privacy risks drive or inhibit self-disclosure (e.g., social benefits and social risks on social networking sites). However, the assessed items were rather general, and might have been unsuitable for some websites but appropriate to others. It is particularly suspicious that for the social networking context, not one of the four assessed privacy calculus variables significantly predicted the intention to self-disclose. Hence, the context-dependency of the privacy calculus might have been due to a measurement problem in this study. Moreover, the analysis method used

subsamples to investigate the question of context-specificity. Consequently, statistical power in subsamples may have been too low to detect the effects. In contrast to study I, study IV found the privacy calculus being stable across different contexts (i.e., news, health, and commerce) which means that a weighing of risks and benefits takes place regardless of the specific website (note: in study IV, participants experienced three different situations that occurred in three different contexts). These findings are in line with the general understanding of privacy decisions being the result of risk and benefit perceptions (Culnan & Armstrong, 1999; Dinev & Hart, 2006) and also with the findings of Bol and colleagues (2018). This does, however, not imply that self-disclosure would not be context dependent. As already noted, each context specifies which kind of benefits and privacy risks are involved and which kinds of information are appropriate to share (Nissenbaum, 2010).

In contrast to self-disclosure, study I revealed that privacy protection was not context specific. This finding indicates that participants' desire for privacy protection was stable across the three contexts and that participants were equally likely to use the protecting tool throughout the websites. This finding is intuitive insofar as, for instance, people would visit different websites (i.e., contexts) with the same web browser but may use one single protecting tool in their browser. Hence, the desire of people to have their personal information better protected is not context-dependent but seems to refer to the general situation that most Internet companies collect, process, and disseminate personal data (West, 2019; Zuboff, 2019). Thus, whereas self-disclosure is contextual (and situational), privacy protection can be (and oftentimes is) stable across contexts and situations. Hence, the expansion of the privacy calculus approach by protective behaviors (Dienlin & Metzger, 2016; study I) combines a situational and a cross-situational and even cross-contextual perspective. Future studies should further elaborate this compound of different situational and contextual levels and whether the privacy calculus framework is the right tool to investigate both variables. It is conceivable that situational perceptions would best predict self-disclosure whereas rather general and cross-situational perceptions might drive one's protective attempts.

Studies III and IV contained notions of Masur's (2018) theory of situational privacy and self-disclosure. Whereas study III investigated the impact of situational knowledge and a situational privacy perception on the privacy calculus, study IV was interested in the analysis of participants' perceptions and intentions in three different situations. Both studies found support for privacy decisions being situation specific. Study III showed that situational knowledge is crucial for a realistic perception of the situation which consequently affected the privacy calculus and self-disclosure. Study IV provided evidence that people engage in a

cognitive process of balancing positive and negative aspects of self-disclosure in every situation. Hence, privacy perceptions, intentions, and behaviors are inherently context and situation dependent. While contexts are a description of the environment, situations focus on both environmental and psychological factors (Masur, 2018; Nissenbaum, 2010). Both views, however, seem to be important to understand people's online privacy behaviors, with contexts adopting a more general view of stable circumstances that affect multiple situations and situations combining external factors and internal states and traits. In conclusion, self-disclosure seems to be depending on the respective situation (which also includes the context), but privacy protection intentions and behaviors are rather stable over multiple situations. For instance, a person has to decide to use a privacy protecting tool once and that tool keeps privacy protection up constantly (until one decides to stop using it). The decision to disclose personal information or not has to be made again and again. Hence, privacy protection would be driven by rather general perceptions whereas self-disclosure decisions are the result of situational perceptions. Nevertheless, stable factors like general beliefs or personality traits affect situational and contextual perceptions and privacy behaviors which can also be seen in Figures 6 and 7.

14 Interventions and transparency

Three studies tested privacy interventions or transparency enhancing measures. Study II examined effects of a fear appeal, study III focused on condensed privacy policies, and study IV investigated a privacy score. Whereas the fear appeal did not impact Facebook users' protection motivation, privacy threat perception, or self-disclosure intention, enhancing transparency was found to be an effective means to convey situational knowledge. In the manuscript of study II, it was argued that the fear appeal may have not worked because it was not based on participants' actual level of protection (to ensure equally large experimental groups). However, in general, fear appeals indicating a privacy threat and a protection possibility are likely to be helpful. This is because participants' privacy threat perception and perceived effectiveness of the privacy protection response were indicators of protection motivation. Hence, triggering these perceptions should generally lead to an increase in people's protection motivation. Study III found people who were confronted with highly condensed privacy policies to be more motivated to read the text compared to those who was shown a regular privacy policy. Those who read the privacy policies more carefully (i.e., especially those who saw the condensed policy) gained more situational knowledge and had a more realistic perception of the situation's level of privacy and a more realistic assessment of privacy risk likelihood. The study showed that users are indeed interested in collecting situational knowledge, however, conventional privacy policies are not designed to inform users but rather

to protect companies. Study IV investigated an even more condensed form of transparency enhancement, that is a nutrition label alike privacy score. The score displayed three categories (A, B, and C) implying different privacy levels in the colors of a traffic light. It was shown that participants' privacy risk perception was largely congruent with the implied privacy level. Hence, these two studies imply that providing users with condensed information in critical situations (e.g., when they are about to disclose information, download an app, or use a service) can greatly support them in their privacy decisions. However, transparency enhancement still shifts responsibility onto users while users are limited in their options to manage their online privacy (Baruh & Popescu, 2017).

15 Overview of the findings

This part describes the schematic overviews seen on the next pages. Both Figure 6 and Figure 7 make distinctions of stable, contextual, and situational factors. However, Figure 6 mainly focused on modelling the relationships of the different variables that were found in the studies, whereas Figure 7 aimed at a cleaner classification of stable, contextual, and situational factors. The model shown in Figure 6 separates the different dimensions of situation, context, and stable factors as well as the privacy calculus and the protection motivation theory. Self-disclosure is depicted to be a situational decision whereas privacy protection is rather cross-contextual. While it is conceivable that stable and contextual factors can affect situational factors, situational perceptions may also impact contextual or stable factors. For instance, the situational perception of perceived privacy costs and the rather stable desire for privacy protection were found to be highly related. Although the path was directed in the original study, a reciprocal relation seems more likely as, for example, a high desire for privacy protection could positively influence the situational perception of privacy threats. The model should be read in the way that factors placed within a box are primarily considered to take place in this box, for example, knowledge about current privacy is primarily situational. However, knowledge about current privacy is also within the contextual box because situations always take place within contexts. Another example is self-efficacy that is partly contextual and partly stable. It is conceivable that people exhibit a general privacy protection self-efficacy but also contextual skills. The model shows stimuli or paths that were not found significant in grey (e.g., fear appeal) and in grey dashed lines (e.g., privacy resignation), respectively. Figure 7 indicates that stable, contextual, and situational factors can equally contribute to people's privacy decisions. The factors were assigned to the categories based on theoretical considerations. Nevertheless, some variables are not unambiguously assignable to the categories (e.g., trust could be general trust, trust in a certain website, or increased situational trust).

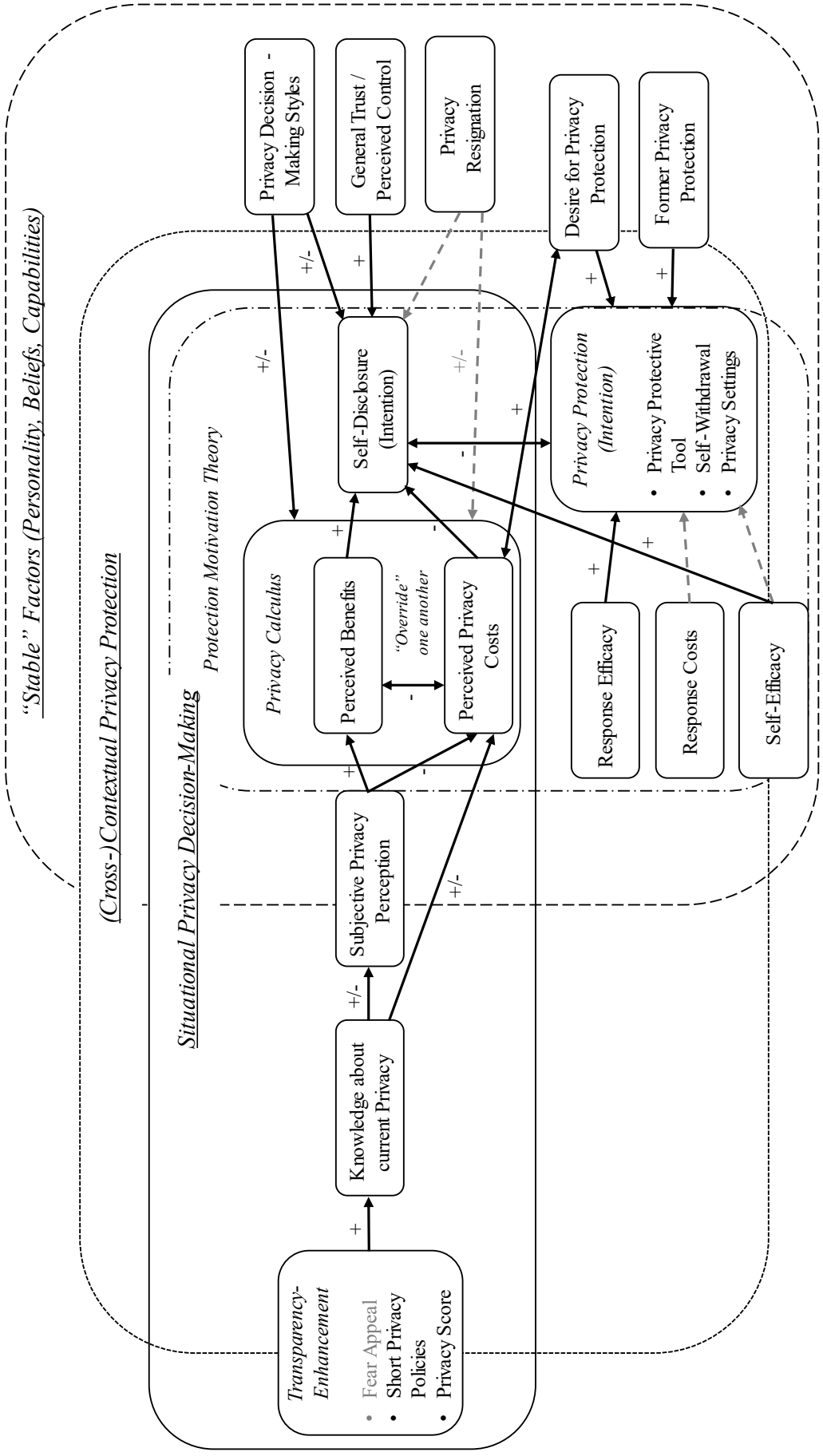

Figure 6. Schematic overview of the results. Dashed lines indicate non-significant paths.

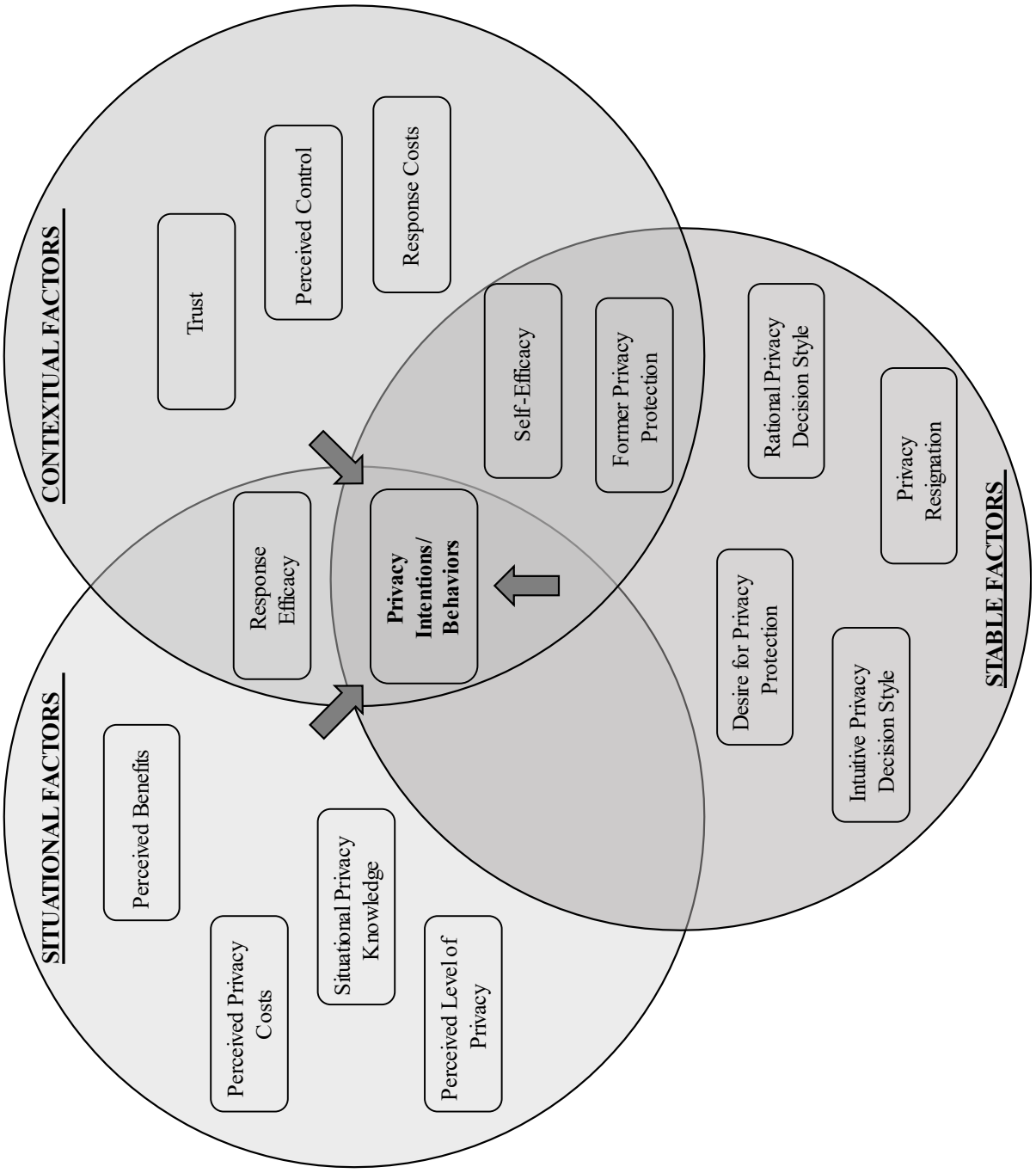

Figure 7. Attempt to sort the variables measured in the four studies into stable, contextual, and situational categories.

16 Theoretical Implications

The current dissertation applied two approaches to explain people's online privacy behaviors. These two approaches are the privacy calculus and the protection motivation theory. In the following sections, it will be summarized whether both approaches seemed applicable to the questions or whether they did not prove useful.

16.1 Privacy calculus

In studies I, III, and IV, the privacy calculus framework was applied. In study II, the privacy calculus was implicitly part of the protection motivation theory. Behavioral intentions were assessed in all studies but study III in which behavioral data were recorded. Study IV additionally separated between- from within-person variance. In general, privacy calculus notions were found when assessing self-disclosure intentions on both between- and within-subject levels. This means that persons who perceived higher privacy costs than others had a reduced self-disclosure intention and those who perceived higher benefits than others had an increased self-disclosure intention. In study IV, this between-person pattern was not shown when controlling for privacy decision-making styles and resignation. However, the study found striking results on the within-person level. The analyses revealed that people who currently perceive more benefits than in other situations have an increased self-disclosure intention and someone who perceives more privacy risks in the present situation has a decreased self-disclosure intention. Most interestingly, those who perceived higher benefits, simultaneously perceived reduced privacy risks which indicates that benefit and risk perceptions have the potential to override each other and are not independent of each other. These findings support the logic of the privacy calculus to a great extent (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Laufer & Wolfe, 1977). Recording behavioral data did not provide further support for the approach. Only the perception of benefits had a small positive effect on information sharing. Persons who found privacy risks more likely than others did not share less information on the networking site. In article III, it was argued that this result might be due to participants low privacy risk likelihood perception, due to their awareness of and trust in the artificial study situation, an unsuitableness of only the risk likelihood measure to predict self-disclosure, or the fact that participants felt an additional urge to disclose information as a part of the experiment. A combination of multiple explanations is not implausible. About 97% of variance were explained by factors other than the assessed ones which shows that in study III, self-disclosure was only weakly predicted by the privacy calculus. In sum, however, the privacy calculus approach was shown to have a high potential to predict Internet users' self-disclosure intentions.

Future studies could further focus on actual user behavior, possibly reducing the artificiality of experimental situations.

Additionally, the approach was found to predict privacy protection desires and protection motivation (studies I and II). Hence, the privacy calculus seems to be applicable to predict both self-disclosure and privacy protection (desires and intentions). However, as it has been argued in section 13, self-disclosure is a situationally repeated decision, whereas privacy protection oftentimes is a cross-contextual decision that is made once. Hence, it would seem that situational perceptions of privacy risks and benefits predict self-disclosure whereas more general perceptions of privacy online drive protective attempts. When this suggestion is considered when investigating both privacy protection and self-disclosure within the privacy calculus framework, the approach appears to work for predicting both variables.

16.2 Protection motivation theory

Study II utilized the protection motivation theory (Rogers, 1975, 1983). By and large, results found the cognitive processes of the theory to be suitable for the field of online privacy. The theory predicts that people need to have a high appraisal of a threat and a high appraisal of a coping response in order to develop protection motivation. Indeed, privacy threat perception and response efficacy were significant predictors of Facebook users' self-withdrawal. On the other side, the theory was also able to predict participants' self-disclosure intentions. Although not all variables predicted participants' protection intention, the theory can successfully explain why and why not Internet users self-disclose and protect their privacy. However, one central notion of the PMT was not found to have an impact on participants' threat perception and protection motivation: the fear appeal. It was argued that respondents might have perceived the appeal as not realistic or fitting to their actual protection levels. In previous studies, similar warning messages have been found to be effective (LaRose & Riffon, 2007). Moreover, there appear to be some contradictory findings. Whereas in the present study, self-efficacy was not positively related to protection motivation but even positively to a more revealing privacy behavior, it has also been found to be in accordance with the theory (Dienlin & Metzger, 2016). However, another study did not find a relation between self-efficacy and privacy protection behavior, too (Boerman et al., 2018). Hence, more research on online privacy and the protection motivation theory is needed to shed further light on open questions like under which circumstances warning messages are effective and why self-efficacy sometimes leads to increases in protection but sometimes even leads to increases in information sharing intentions. Nevertheless, the PMT appears to be a suitable approach to predict both people's privacy protection motivation and their self-disclosure intention. It contains more variables than the

privacy calculus that affect people's protection intention. However, the assumption of disclosure and protection happening on different situational and contextual levels also applies to the PMT. Thus, it seems that the privacy calculus would be an appropriate approach to investigate Internet users' self-disclosure behaviors whereas the PMT is best suited to study protection behaviors. Having said that, a combination of the privacy calculus (focusing on a specific situation) and the PMT (focusing on more general protection behavior) is conceivable and would be an interesting approach to examine.

17 Practical implications

Besides the theoretical implications of the four studies, practical implications can be derived that might help to improve people's privacy online. These practical implications result from the major or most surprising findings related to people's self-disclosure and privacy protection intentions or behaviors.

17.1 Users desire more online privacy

Sometimes, the question is asked whether people actually care for their online privacy (e.g., Hu & Ma, 2010). The studies of this dissertation can give a short and clear answer to this question: *yes*. People care for their privacy, many are aware of constant user tracking and surveillance techniques, and many wish to have much more online privacy. Hence, attempts are made to reach more private spheres. On the other side, people do not want to lose the benefits the online world provides which are sometimes not achievable when protection attempts are too strict (e.g., websites that do not allow for tracking-blockers). Thus, users experience a *privacy dilemma* (see section 18.1).

17.2 Users need additional information

Online privacy is an invisible good. In the physical world, we can sense if someone is around or if we are alone, if doors are closed or open, if we are in public places or in our private sphere. Online, such a sense for privacy is lacking. Hence, people cannot intuitively tell whether a website or app respects user privacy or is infiltrating it without, for instance, gathering information in privacy policies. Study III addressed this sense or subjective feeling for the current level of online privacy and results showed that this privacy feeling is very likely to be misleading when it is not based on hard evidence. Thus, I argue that providing Internet users with additional information about the current level of privacy is indispensable and mandatory. This information should clarify whether and which personal data websites automatically collect

and for what purposes. In this way, Internet users would be supported in developing realistic perceptions of online privacy.

17.3 Users need concise information

Privacy policies have been shown to be unpracticable not only by the current dissertation's study III, but by several empirical studies. The reasons for this are that they provide users with information that are not necessarily relevant for users and that they are way too long and cumbersome. Hence, either providing users with concise textual information about a website's privacy level or with pictorial information was found to greatly contribute to users' assessment of the current situation's actual privacy level. Hence, user would greatly benefit from the provision of additional concise and intuitive information about privacy risks such as privacy icons (Efroni et al., 2019), privacy seals (LaRose & Riffon, 2007), condensed privacy policies (study III), or privacy scores (study IV). So far, the GDPR allows and encourages but not requires the application of visualizations in addition to privacy policies (Efroni et al., 2019). The studies of the current dissertation suggest that Internet users would benefit immensely from receiving condensed information in critical situations. Providing additional information on privacy threats could alter users' decision to use certain services, download specific apps, or disclose personal information to particular websites and increase their online privacy. Moreover, some user groups (e.g., intuitive privacy decision-makers, children, or elderly people) might be especially vulnerable to privacy risks having a lower awareness for these threats. These user groups could particularly benefit from additional information.

17.4 Users need information on both risks and protection

One of the implications of study II was that information on both privacy threats and the protection response increase people's motivation to shield privacy risks. Hence, informing users solely about privacy risks that can arise in different situations might not be a sufficient means to motivate protection. In addition, users would also benefit from advices about if and how these risks can be avoided. This can additionally motivate users to engage in protective attempts as it might, for instance, override beliefs that online privacy protection is pointless. Thus, I recommend providing users with knowledge about both the potential situational privacy risks that can arise and knowledge about how to shield these risks to foster more cautious and aware privacy behaviors. Again, particularly vulnerable user groups, for instance, persons with low protection skills and knowledge are likely to benefit a lot.

17.5 Self-data protection or regulation?

Whereas Internet companies do their best to advertise their products (e.g., online services), they do not advertise the privacy risks associated with the usage of these products or means to avoid them because their business models rely on harvesting personal information (West, 2019; Zuboff, 2019). Logically, informing users about how a website invades their users' privacy and how one could possibly avoid the intrusion is not in the website provider's interest as it might reduce the company's sales. However, other practical examples exist where companies are obligated to inform about potential detrimental effects of their products (e.g., warning labels on cigarette packages). Hence, because self-data management and protection is limited (Baruh & Popescu, 2017) and because empirical findings show that users would greatly benefit from additional information, one possibility would be a stricter political regulation that may support Internet users on a larger scale.

18 Online privacy – general remarks

18.1 Paradox or dilemma?

Two views on online privacy have evolved: one stream views privacy behavior to be *paradoxical* whereas the second line argues that the paradox has been solved as privacy behavior is explainable. The general privacy paradox argument is that people often state to be very concerned about their online privacy, however, at the same time they disclose vast amount of personal information (Barnes, 2006; Norberg et al. 2007; Tufekci, 2008). Hence, their attitudes or intentions are said to be incompatible with their behaviors. Numerous empirical studies, however, have argued that there are plausible reasons for people's behavior like a lack of awareness (Pötzsch, 2008), lack of privacy literacy (Trepte et al., 2015), privacy cynicism and resignation (Hoffmann et al., 2016), or methodological problems (Dienlin & Trepte, 2015). Moreover, several review articles (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017) and a meta-analysis (Baruh et al., 2017) have dedicated themselves to the question whether Internet users' privacy behaviors are paradoxical or not. The tenor of these articles is that online perceptions, attitudes, and behaviors are not contradictory, but that research has identified a great number of reasons that explain why people behave the way they do. However, it also gets apparent that there are still some white spots that need to be explored before the map of online privacy can be completely painted.

Did the present dissertation find indicators that would support a privacy paradox? The majority of studies found people's self-disclosure intentions to be compatible with their perceptions of risks and benefits. Only the behavioral data did not fit into this scheme. However, the perception of benefits could insufficiently explain self-disclosure, too. Moreover, people's

protection intentions were higher than their disclosure intentions. Thus, I argue that the four studies of the present dissertation did not find evidence for a privacy paradox. Quite the contrary, participants who perceived high risks to their privacy online were less willing to disclose personal information and had higher protection intentions. It can be argued that people's behaviors do not represent a paradox, but that people are faced with a *privacy dilemma*. Brandtzæg and colleagues (2010) introduced this term in saying that users are trapped between social and privacy needs. This argument can be expanded to the Internet in general because in most cases people do not have the option to decide whether to disclose data or not when they want to use a certain service or website. Hence, they are trapped between not giving away personal information or between the obtainment of certain benefits. In conclusion, I argue that users often do not have a real choice in disregarding the benefits as this would lead to major disadvantages in several other areas (e.g., losing social connections, missing relevant information, being not able to buy certain products etc.). Hence, I propose that future research takes a closer look at the consequences that would arise from not receiving certain benefits.

18.2 Privacy calculus – the question of rationality

The main theoretical approach that has been examined by the studies of the present dissertation—the privacy calculus—has been subject to criticism due to its rational nature (Acquisti & Grossklags, 2003, 2005; Knijnenburg et al., 2017; Ostendorf et al., 2020; Wilson & Valaich, 2012). The original privacy calculus work is based on the rational choice theory (Simon, 1955) and partly the expectance theory (Vroom, 1964). Hence, the privacy calculus is generally understood as a theory of conscious and logic decision-making including the conception that people always attempt the best decision outcome (cf. Barth & de Jong, 2017). Acquisti and Grossklags (2005) argued that online privacy behaviors cannot be rational as people lack information and base their decisions on simplified mental models and heuristics. However, criticizing the notion of rationality does not mean that the privacy calculus is generally refuted. In contrast, those studies have often not tried to find alternative explanations for privacy behaviors, but they have extended the underlying logic of the approach (Acquisti & Grossklags, 2005) or proposed decision support (Knijnenburg et al., 2017). Moreover, the critics have pointed to sensitive misunderstandings of people's privacy choices. Viewing Internet users as completely rational agents would be an argument for companies and policy makers to shift responsibility completely onto users because people were able to always make optimal decisions. However, lots of studies with underlying views of both rational or irrational decision-making have found that several factors impact the privacy calculus variables and that benefit perceptions mostly outweigh risk perceptions. Moreover, whether behaviors are

rational, or irrational can only be comprehended by considering the environment in which decisions are embedded (Gigerenzer, 2008). Hence, lines of research that integrate contextual and situational factors to the privacy calculus as well as further factors such as heuristics, beliefs, and personality factors seem to be on the right track in approaching the nature of online privacy choices. Importantly, it would be a fallacy to speak of *the* nature of privacy decisions as there are empirical indices that point to inter-individual differences of online privacy decision-making (Dienlin et al., 2019; Ostendorf et al., 2020) among them study IV.

In conclusion, viewing online privacy choices as a merely rational process would be misleading and does not correspond to actual situations. This does, however, not mean that the privacy calculus framework should be refuted as a whole since it has been found to be a reliable framework for understanding people's online self-disclosure decisions by a plethora of empirical studies (Bol et al., 2018; Culnan & Armstrong, 1999; Dienlin & Metzger, 2016; Dinev & Hart, 2006; Meier & Schäwel, 2019; Krasnova et al., 2010; Trepte et al., 2017) including the studies of the current dissertation which also point to an internal weighing process. However, it is important to acknowledge that human choice is affected by cognitive distortions, personality traits that impede a rational weighing of several factors, and limited knowledge (Kahneman & Tversky, 1979). Moreover, behavior is always affected by the environmental and situational circumstances (Gigerenzer, 2008; Masur, 2018; Nissenbaum, 2010). When research considers these factors and acknowledges that most people are no optimal decision makers, the privacy calculus framework constitutes a very promising basis to investigate and understand people's online privacy choices.

18.3 Limited privacy protection

In parts of this dissertation, it was investigated how users could be motivated to better protect their privacy and which factors affect privacy protection. The topic is highly relevant because responsibility is frequently shifted onto users (Yao, 2011) and understanding why people protect their privacy online would be important to develop protective tools (Boerman et al., 2018). Researchers, however, argue that privacy protection performed by individuals has its limits. Some argue that protection attempts by users are rather difficult to apply (Bujlow et al., 2017), others even assume that self-data protection is very limited and therefore designed to fail (Baruh & Popescu, 2017; Matzner et al., 2016). Moreover, due to unequally distributed technical skills in the population, persons with higher expertise and literacy are more capable of protecting themselves compared to those with fewer skills and knowledge (Büchi et al., 2016; Matzner et al., 2016; Trepte et al., 2015). Due to power asymmetries between companies and users, users lack knowledge how to exactly protect personal information because actual data

collection techniques are often opaque (Almuhimedi et al., 2014; West, 2019). Hence, it seems that Internet users in general constitute a vulnerable group although there are large differences between individuals. Equipped with the right knowledge and skills (i.e., privacy literacy), many privacy risks could be avoided (Bujlow et al., 2017). However, this is not a universal solution as not all people are able or willing to protect themselves which is why functioning self-data protection is reserved to a small elite whereas the rest is still exposed to privacy threats. In conclusion, I argue that self-data protection is an important and indispensable first step for Internet users to protect their privacy online, but I also agree that this constitutes a limited approach leading to inequalities in privacy protection between differently skilled or literate groups. Hence, a system that is solely based on the idea of users that are fully capable of avoiding privacy threats, is rather utopian. Consequently, the need for alternative protection measures (e.g., privacy-by-design or privacy-by-default) comes to the fore.

19 Limitations

Although limitations for each of the studies have already been discussed in the respective articles, this section concedes general limitations.

One limitation concerns the application of hypothetical scenarios in three of the studies. Although all of these studies used visual stimuli in addition to the texts, findings may be limited due to these scenario-based approaches. In these scenario-based experiments, behavioral intentions but not behaviors were assessed. Hence, in the future, researchers could more frequently observe actual user behavior to overcome the potential hypothetical nature of the findings. Nevertheless, scenario-based studies are a good means to create high internal validity.

Another general limitation of all four studies is the utilization of convenience samples. The studies were generally promoted on social media, platforms for study distribution and participation, or panel providers (without controlling quotas). Thus, participants were generally younger, more female, and higher educated than the German average. These limitations are not insignificant in the realm of online privacy. For instance, younger persons tend to more intense Internet usage which is apparently related to higher privacy literacy (i.e., privacy skills and knowledge; Bartsch & Dienlin, 2016). At the same time, younger persons and men (on the vertical dimension) seem to protect their privacy to a higher extent (Park, 2013). Thus, participants of the current samples might have had a higher privacy literacy and therewith a higher awareness of privacy threats and higher protection skills (cf. Trepte et al., 2015). However, research on gender, education, and age effects on people's online privacy behaviors often shows mixed results (cf. Boerman et al., 2018). Hence, no general statements can be made at this point how the sample compositions may have impacted the results. In the future,

representative samples may be utilized more often, especially to be able to detect the most vulnerable groups.

The last general limitation involves the culture in which the studies were conducted, that is Germany. The findings are therefore valid for a nationwide spectrum and probably for the European population, but not across different cultures. Previously, privacy behaviors have been found to differ among western and eastern (i.e., individualistic and collectivistic) cultures (Trepte et al., 2017), but also among different western cultures (Dinev et al., 2006; Krasnova et al., 2012). Reasons for these differences might be distinct Internet usage behaviors but also differences in trust towards governmental institutions. Since May 2018, the EU has one of the strongest privacy regulations worldwide (i.e., the GDPR) which may also have affected people's privacy perceptions, intentions, and behaviors. This is why the results of the current dissertations' studies would apply to Germany and Europe, but it is unlikely that the results will retain their validity beyond the borders of the EU.

20 Next steps

Although a lot of research has been carried out in the realm of online privacy, there are lots of open questions. Due to the continuous development of platforms, tracking-mechanisms, and changing user behaviors, there is always the need for the conduct of further studies. Based on the findings of study I, it should be further examined whether the privacy calculus is context dependent and how different contexts might affect the weighing of risks and benefits. Moreover, studies could further focus on people's desire for privacy protection. Which factors other than perceived privacy risks, trust, and perceived control might impact this desire and which factors influence whether people engage in protective behaviors or not. In study II, the fear appeal did not lead to increases in perceptions and intentions. Hence, forthcoming investigations should examine under which circumstances fear appeals and warning messages might be useful and when they are useless. Further, interindividual differences can be targeted. How do fear appeals have to be built in order to persuade certain users with certain needs? Moreover, research on privacy and the protection motivation theory seems to be at its beginning. As stated earlier (section 16.2), a combination of PMT and privacy calculus would be thinkable whereby the PMT integrates rather general beliefs and perceptions to predict privacy protection motivation and the privacy calculus including situation-specific perceptions predicting self-disclosure. Hence, more research in this area is surely promising and the theory might be further developed to even more approach the field of online privacy protection. Concerning study III, it is very important to collect more behavioral user data. These behavioral data should be at best observed via a separate platform or website and not as direct part of an

experiment which could render user behavior unnatural. Moreover, users' subjective privacy perception could be further scrutinized. Which factors might lead to disadvantageous perceptions or which factors could be beneficial? Finally, based on the findings of study IV, I recommend examining the psychological processes that underly the privacy calculus approach in more detail. Is the weighing of risks and benefits a deliberate and conscious, or a heuristic and unconscious process (or both)? Under which circumstances are information rather processed deliberately or intuitively? Both differences between persons and processes within individuals should be further targeted. Finally, researchers may also generally turn towards different user groups, for instance, different privacy decision-makers, or children and elderly individuals to understand interindividual differences and to identify the most vulnerable groups. Moreover, studies could further concentrate on passive self-disclosure. Do people have awareness for being constantly tracked and does this awareness alter their behavior? How could more cautious privacy behaviors be learned and maintained? What would be long-term effects of using tools that provide transparency and increased online privacy? Would there be habituation effects when people are constantly informed about privacy threats? Thus, on one side, research has to go in more detail on the user side. On the other hand, findings must be used by both companies and politicians to build or enforce more user-friendly environments.

21 Conclusion

In the current dissertation, four quantitative online experiments were conducted that focused on the field of online self-disclosure and privacy protection. To conclude the dissertation, the following points are addressed. Generally, it was found that participants wished more privacy protection, perceived high privacy threats, and had higher intentions to protect their privacy than to share personal data. Hence, altogether the findings indicate that participants cared for their online privacy and were rather unsatisfied with the current situation in which companies collect, process, and disseminate personal data and constantly monitor users. Moreover, some ways of supporting users in their online privacy perceptions were investigated. Both short privacy policies and the privacy score were found to be beneficial for users. The short privacy policy was much easier to comprehend than long policies with heavily reduced cognitive and time effort leading to a much more realistic perception of the situation's privacy level. The privacy score seemed to be a good indicator of online privacy risks which may be even more beneficial than condensed privacy policies because it can be comprehended in even less time. These supportive means could lead to more risk aware and cautious privacy choices as it was also shown that people's perception of privacy risks and benefits can override each other. This finding that supports the general privacy calculus notion of weighing risks and

benefits on the within-person level indicates that more knowledge about privacy risks could effectively lead to a decrease of people's benefit perception and to less disclosure or to the search for alternatives (e.g., other websites that offer comparable benefits). In line with the protection motivation theory, it was found that Internet users value information about how to effectively protect their privacy. Hence, users would benefit from being equipped with both knowledge about privacy risks and how to protect one's online privacy. In general, both the privacy calculus approach as well as the PMT have been found to be good means to investigate people's online privacy behaviors. Whereas the privacy calculus focuses on situational perceptions of privacy risks and benefits affecting the situational decision to self-disclose, the PMT rather assesses general beliefs and perceptions because privacy protection is usually cross-situational. As both approaches are compatible, future studies could use theoretical frameworks that constitute a combination of both approaches.

To sum it up, the current dissertation found indicators of how Internet users can be supported in their online privacy behaviors. Providing information in critical situations could prevent users from being tricked into unwanted disclosures or unwanted consent. However, support mechanisms as well as transparency are not a panacea as they are unlikely to protect all individuals equally. Therefore, either personalized support mechanisms, or privacy-by-design and privacy-by-default standards could remedy the situation. In addition, companies and governments could also try to explore new paths on which either non-personalized advertisements are presented again, or on which attempts are made to further anonymize and pseudonymize data while maintaining ethical standards to protect the precious public good of individual privacy. To complete this work, I would like to cite Warren and Brandeis (1890) whose quote is probably more relevant than ever. They wrote "that the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection" (Warren & Brandeis, 1890, p. 193). Given the challenges to privacy the digital age has brought, the time seems to have come to redefine the extent of individual privacy protection.

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 Computing Surveys (CSUR), 50*(3), 1-41. http://dx.doi.org/10.1145/3054926

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *2nd Annual Workshop on Economics and Information Security-WEIS, 3*, 1-27.

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

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L., & Agarwal, Y. (2015, April). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 787-796.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Brooks/Cole.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191. https://psycnet.apa.org/doi/10.1037/0033-295X.84.2.191

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics, 34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

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

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society, 19*(4), 579-596. https://doi.org/10.1177%2F1461444815614001

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication, 67*(1), 26-53. https://doi.org/10.1111/jcom.12276

Bechara, A. (2005). Decision making, impulse control and loss of willpower to resist drugs: a neurocognitive perspective. *Nature neuroscience, 8*(11), 1458-1463. https://doi.org/10.1038/nn1584

Bechmann, A. (2015). Non-informed consent cultures: Privacy policies and app contracts on Facebook. *Journal of Media Business Studies, 11*(1), 21-38. https://doi.org/10.1080/16522354.2014.11073574

Berger, A. (1968). *Encyclopedic dictionary of Roman law (Vol. 43)*. American Philosophical Society.

Bilogrevic, I., Freudiger, J., De Cristofaro, E., & Uzun, E. (2014). What's the gist? Privacy-preserving aggregation of user profiles. *European Symposium on Research in Computer Security* (pp. 128-145). Springer. https://doi.org/10.1007/978-3-319-11212-1_8

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of advertising, 46*(3), 363-376. https://doi.org/10.1080/00913367.2017.1339368

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: insights from panel data. *Communication Research*. https://doi.org/10.1177%2F0093650218800915

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

Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4), 237-254. https://doi.org/10.1515/popets-2016-0038

boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, 15(5), 662-679. https://doi.org/10.1080/1369118X.2012.678878

boyd, d., & Marwick, A. E. (2011). Social privacy in networked publics: Teens' attitudes, practices, and strategies. *A decade in internet time: Symposium on the dynamics of the internet and society*. https://ssrn.com/abstract=1925128

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2012). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347. https://doi.org/10.1177%2F1948550612455931

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human–Computer Interaction*, *26*(11-12), 1006-1030. https://doi.org/10.1080/10447318.2010.516719

Bräunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., Seubert, S., & Gusy, C. (2020). Linking loose ends: An interdisciplinary privacy and communication model. *New Media & Society,* 1-22. https://doi.org/10.1177%2F1461444820905045

Büchi, M., Just, N., & Latzer, M. (2016). Caring is not enough: the importance of Internet skills for online privacy protection. Information, *Communication & Society, 20*(8), 1261-1278. https://doi.org/10.1080/1369118X.2016.1229001

Bujlow, T., Carela-Español, V., Sole-Pareta, J., & Barlet-Ros, P. (2017). A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE, 105*(8), 1476-1510. https://doi.org/10.1109/JPROC.2016.2637878

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

Cadwalladr, C. (2017). *The great British Brexit robbery: how our democracy was hijacked*. The Guardian. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81,* 42-51. https://doi.org/10.1016/j.chb.2017.12.001

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. https://doi.org/10.1089/cpb.2008.0226

Cozby, P. C. (1973). Self-disclosure: a literature review. *Psychological bulletin*, 79(2), 73. https://doi.org/10.1037/h0033950

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104 115. https://doi.org/10.1287/orsc.10.1.104

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47-60). Springer. https://doi.org/10.1007/978-3-642-21521-6_5

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763-781.

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J.-M. Mönig (Eds.), *Medien und Privatheit [Media and privacy]* (pp. 105–122). Stutz.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383. https://doi.org/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. https://doi.org/10.1002/ejsp.2049

Dienlin, T., Bräunlich, K., & Trepte, S. (2019). *How do like and dislike buttons affect communication? A privacy calculus approach to understanding self-disclosure online in a one-week field experiment.* Paper presented at the 69th Annual Conference of the ICA, Washington, DC, USA.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In A. Gupta, V. L. Patel, & R. A. Greenes (Eds.), *Advances in Healthcare Informatics and Analytics, Annals of Information Systems 19* (pp. 19–50). Springer publishing.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389-402. https://doi.org/10.1057/palgrave.ejis.3000590

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

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New media & society, 21*(8), 1824-1839. https://doi.org/10.1177%2F1461444819833331

Ebbers, F. (2019). How to Protect My Privacy? Classifying End-User Information Privacy Protection Behaviors. *IFIP International Summer School on Privacy and Identity Management*, 327-342. Springer. https://doi.org/10.1007/978-3-030-42504-3_21

Efroni, Z., Metzger, J., Mischau, L., & Schirmbeck, M. (2019). Privacy icons: a risk-based approach to visualisation of data processing. *European Data Protection Law Review, 5*, 352-366. https://doi.org/10.21552/edpl/2019/3/9

Egnell, M., Talati, Z., Pettigrew, S., Galan, P., Hercberg, S., & Julia, C. (2019). Comparison of front-of-pack labels to help German consumers understand the nutritional quality of food products. Color-coded labels outperform all other systems. *Ernährungs Umschau*, *66*(5), 76-84. https://doi.org/10.4455/eu.2019.020

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. https://doi.org/10.1177%2F1461444810385389

European Commission. (2019). *Special Eurobarometer 487a: The general data protection regulation. Brussels: European Commission*. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886

Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law, 7*(1), 36-47. https://doi.org/10.1093/idpl/ipw026

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

Gigerenzer, G. (2008). Why heuristics work. Perspectives on psychological science, *3*(1), 20-29. https://doi.org/10.1111%2Fj.1745-6916.2008.00058.x

Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. Boczkowski, and K Foot (Eds.), *Media technologies: Essays on communication, materiality, and society* (pp. 167-194). MIT Press.

Hamaker, E. L. (2012). Why researchers should think" within-person": A paradigmatic rationale. *Handbook of research methods for studying daily life*, 43-61. http://cds.web.unc.edu/files/2013/11/Hamaker_2012.pdf

Hamilton, K., Shih, S. I., & Mohammed, S. (2016). The development and validation of the rational and intuitive decision styles scale. *Journal of personality assessment*, *98*(5), 523-535. https://doi.org/10.1080/00223891.2015.1132426

Hannak, A., Soeller, G., Lazer, D., Mislove, A., & Wilson, C. (2014). Measuring price discrimination and steering on e-commerce web sites. *Proceedings of the 2014 conference on internet measurement conference*, 305-318. https://doi.org/10.1145/2663716.2663744

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International journal of communication, 10*, 21. https://doi.org/10.5167/UZH-148157

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/110.5817/CP2016-4-7

Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Review*, *25*(1), 84-88. https://doi.org/10.1016/j.clsr.2008.11.002

Hu, Q., & Ma, S. (2010). Does Privacy Still Matter in the Era of Web 2.0? A Qualitative Study of User Behavior towards Online Social Networking Activities. *PACIS, 2*. 591-602.

Janic, M., Wijbenga, J. P., & Veugen, T. (2013, June). Transparency enhancing tools (TETs): an overview. *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*, 18-25. https://doi.org/10.1109/STAST.2013.11

Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *The Journal of Abnormal and Social Psychology*, *56*(1), 91-98. https://psycnet.apa.org/doi/10.1037/h0043357

Julia, C., & Hercberg, S. (2017). Nutri-Score: Evidence of the effectiveness of the French front-of-pack nutrition label. *Ernährungs Umschau*, *64*(12), 181-187.

Kahneman, D. (2003). A perspective on judgment and choice: mapping bounded rationality. *American psychologist*, *58*(9), 697-720. https://doi.org/10.1037/0003-066X.58.9.697

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2). 263-292

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163-1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Khan, G. F., Swar, B., & Lee, S. K. (2014). Social media risks and benefits: A public sector perspective. *Social science computer review*, *32*(5), 606-627. https://doi.org/10.1177%2F0894439314524701

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death to the Privacy Calculus? *SSRN Electronic Journal*. https://dx.doi.org/10.2139/ssrn.2923806

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*, *110*(15), 5802-5805. https://doi.org/10.1073/pnas.1218772110

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* (pp. 127-141). Springer. https://doi.org/10.1007/978-3-642-21521-6_10

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

Krasnova, H., Kolesnikova, E., & Guenther, O. (2009). " It won't happen to me!": self-disclosure in online social networks. *Proceedings of the 15th Americas Conference on Information Systems* (pp. 1-10). https://doi.org/10.7892/boris.47460

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, *25*(2), 109-125. https://doi.org/10.1057%2Fjit.2010.6

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*(3), https://doi.org/127-135. 10.1007/s12599-012-0216-6

Kruikemeier, S., Sezgin, M., & Boerman, S. C. (2016). Political microtargeting: Relationship between personalized advertising on facebook and voters' responses. *Cyberpsychology, Behavior, and Social Networking*, *19*(6), 367-372. https://doi.org/10.1089/cyber.2015.0652

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

Lampinen, A., Lehtinen, V., Lehmuskallio, A., & Tamminen, S. (2011, May). We're in it together: interpersonal management of disclosure in social network services. *Proceedings of the SIGCHI conference on human factors in computing systems*, 3217-3226. https://doi.org/10.1145/1978942.1979420

Lang, A. (2000). The limited capacity model of mediated message processing. *Journal of Communication*, *50*(1), 46–70. https://doi.org/10.1111/j.1460-2466.2000.tb02833.x

Lang, A. (2017). Limited capacity model of motivated mediated message processing (LC4MP). In P. Rössler, C. A. Hoffner, & L. van Zoonen (Eds.), *The international encyclopedia*

of media effects (pp. 1–9). John Wiley & Sons. https://doi.org/10.1002/9781118783764.wbieme0077

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41*(1), 127-149. https://doi.org/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. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454. https://doi.org/10.1080/01449290600879344

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: growing up in a digital age: an evidence review. http://eprints.lse.ac.uk/101283/

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. N*ew Media & Society, 22*(7), 1168-1187. https://doi.org/10.1177%2F1461444820912544

Lutz, C., & Strathoff, P. (2014). Privacy concerns and online behavior–Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2425132

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

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5-21. https://doi.org/10.1111/j.1540-4560.1977.tb01879.x

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of social issues, 59*(2), 243-261. https://doi.org/10.1111/1540-4560.00063

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051-1067. https://doi.org/10.1177%2F1461444814543995

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

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication, 8*(2), 258-269. http://dx.doi.org/10.17645/mac.v8i2.2855

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, *2*(1), 1-13. https://doi.org/10.1177%2F2056305116634368

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

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society*, *12*(2), 93-106. https://doi.org/10.1108/JICES-08-2013-0030

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-It-Yourself Data Protection Empowerment or Burden? *Data protection on the move*, 277-305. Springer. https://doi.org/10.1007/978-94-017-7376-8_11

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Journal of Law and Policy for the Information Society*, *4*, 543-568. https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

Meier, Y. & Schäwel, J. (2019). No risk – no fun. The Role of Risk-Attitudes and the Need for Cognition in Online Privacy Decision-Making. *Paper presented at the 69th Conference of the International Communication Association, Washington, D.C., USA.*

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155-179. https://doi.org/10.1177%2F0093650206287076

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and engineering ethic*s, *24*(3), 831-852. https://doi.org/10.1007/s11948-015-9674-9

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

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media + Society*, *4*(3). https://doi.org/10.1177%2F2056305118784770

Ostendorf, S., Müller, S. M., & Brand, M. (2020). Neglecting long-term risks: Self-disclosure on social media and its relation to individual decision-making tendencies and

problematic social-networks-use. *Frontiers in Psychology, 11*, 1-17. https://doi.org/10.3389/fpsyg.2020.543388

Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday, 15*(8). https://journals.uic.edu/ojs/index.php/fm/article/download/3075/2581

Papadopoulos, P., Kourtellis, N., Rodriguez, P. R., & Laoutaris, N. (2017). If you are not paying for it, you are the product: How much do advertisers pay to reach you? *Proceedings of the 2017 Internet Measurement Conference*, 142-156. https://doi.org/10.1145/3131365.3131397

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236. https://doi.org/10.1177%2F0093650211418338

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

Petronio & Durham (2008). Communication Privacy Management Theory. In L. A. Baxter & D. O. Braithwait (Eds.) *Engaging Theories in Interpersonal Communication. Multiple Perspectives* (pp. 309-323). Sage.

Pötzsch, S. (2008, September). Privacy awareness: A means to solve the privacy paradox? *IFIP Summer School on the Future of Identity in the Information Society*, 226-236. Springer. https://doi.org/10.1007/978-3-642-03315-5_17

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

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

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*. https://doi.org/10.5210/fm.v15i1.2775

Reece, A. G., & Danforth, C. M. (2017). Instagram photos reveal predictive markers of depression. *EPJ Data Science*, *6*(1), 1-12. https://doi.org/10.1140/epjds/s13688-017-0110-z

Regulation 2016/679. *The protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation). European Parliament, Council of the European Union. http://data.europa.eu/eli/reg/2016/679/oj

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. https://doi.org/10.1111/j.1745-6606.2005.00018.x

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The journal of psychology*, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). Guilford Press.

Rohrmann, B. (2008). Risk perception, risk attitude, risk communication, risk management: A conceptual appraisal. *15th Internaional Emergency Management Society (TIEMS) Annual Conference*.

Rossi, A., & Palmirani, M. (2019). DaPIS: An Ontology-Based Data Protection Icon Set. In G. Peruginelli and S. Faro (Eds.) *Knowledge of the Law in the Big Data Age* (pp. 181-195). https://doi.org/10.3233/FAIA190020

Schäwel, J. (2019). *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*. Doctoral dissertation, Universität Duisburg-Essen. https://doi.org/10.17185/duepublico/70691

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement, 55*(5), 818-831. https://doi.org/10.1177%2F0013164495055005017

Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, *69*(1), 99-118. https://doi.org/10.2307/1884852

Solove, D. (2008). *Understanding privacy*. Harvard University Press

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880-1903. https://ssrn.com/abstract=2171018

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer Mediated Communication*, *22*(2), 55-70. https://doi.org/10.1111/jcc4.12182

Strack, F., & Deutsch, R. (2004). Reflective and impulsive determinants of social behavior. *Personality and social psychology review, 8*(3), 220-247. https://doi.org/10.1207%2Fs15327957pspr0803_1

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review, 8*(2). https://doi.org/10.14763/2019.2.1410

Taddicken, M. (2011). Selbstoffenbarung im Social Web. Ergebnisse einer Internet-repräsentativen Analyse des Nutzerverhaltens in Deutschland. *Publizistik, 56*(3), 281-303. https://doi.org/10.1007/s11616-011-0123-8

Tamir, D. I., & Mitchell, J. P. (2012). Disclosing information about the self is intrinsically rewarding. *Proceedings of the National Academy of Sciences, 109*(21), 8038-8043. https://doi.org/10.1073/pnas.1202129109

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*, *4*(2). https://doi.org/10.1177%2F2056305118767134

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media + Society*, *1*(1). https://doi.org/10.1177%2F2056305115578681

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory 00*, 1-22. https://doi.org/10.1093/ct/qtz035

Trepte, S., & Dienlin, T. (2014). Privatsphäre im Internet. *Neue Medien und deren Schatten. Mediennutzung, Medienwirkung und Medienkompetenz*, 53-79.

Trepte, S. & Masur, P. (2020). Need for privacy. *Encyclopedia of personality and individual differences*. Springer. https://doi.org/10.1007/978-3-319-24612-3_540

Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 61-73). Springer. https://doi.org/10.1007/978-3-642-21521-6_6

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), 1-13. https://doi.org/10.1177%2F2056305116688035

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). *Reforming European data protection law*; 333-365. Springer. https://doi.org/10.1007/978-94-017-9385-8_14

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological review*, *117*(2), 440. https://dx.doi.org/10.1037%2Fa0018963

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. https://doi.org/10.1177%2F0270467607311484

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). https://cyberpsychology.eu/article/view/4223/3265

Vroom, V. H. (1964). *Work and motivation*. Wiley.

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

Wang, Y., Leon, P. G., Chen, X., & Komanduri, S. (2013). From Facebook Regrets to Facebook Privacy Nudges. *Ohio State Law Journal, 74*, 1307-1335.

Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology, 114*(2), 246. https://psycnet.apa.org/doi/10.1037/pspa0000098

Warner, R., & Sloan, R. (2013). Beyond Notice and Choice: Privacy, Norms, and Consent. *Suffolk University Journal of High Technology Law*. https://doi.org/10.2139/SSRN.2239099

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & society*, *58*(1), 20-41. https://doi.org/10.1177%2F0007650317718185

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

Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B, 89*(1), 1-12. https://doi.org/10.1140/epjb/e2015-60754-4

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision making within the privacy calculus. *Proceedings of the 33rd international conference on information systems (ICIS2012)*, 1-11.

Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 111-125). Springer. https://doi.org/10.1007/978-3-642-21521-6_9

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500. https://doi.org/10.1080/1369118X.2013.777757

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75-89. https://doi.org/10.1057%2Fjit.2015.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Public Affairs.

Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodó, B., & de Vreese, C. H. (2018). Online political microtargeting: promises and threats for democracy. *Utrecht Law Review,* 14(1), 82-96. https://doi.org/10.18352/ulr.420

DOI: 10.17185/duepublico/73985
URN: urn:nbn:de:hbz:464-20210205-075438-1