University of Hohenheim

Doctoral Thesis

The psychology of privacy: Analyzing processes of media use and interpersonal communication

Tobias Dienlin

Fakultät Wirtschafts- und Sozialwissenschaften
Institut für Kommunikationswissenschaft
Fachgebiet für Kommunikationswissenschaft insb. Medienpsychologie

2017

First advisor: Prof. Dr. Sabine Trepte
Second advisor: Prof. Dr. Nicole Krämer
Chair of the committee : Prof. Dr. Jens Vogelgesang
Dean: Prof. Dr. Dirk Hachmeister
Day of defense: 05.12.2016

The psychology of privacy: Analyzing processes of media use and interpersonal communication
Tobias Dienlin
Dissertation
University of Hohenheim
2017

Contents

Abstract

What is the psychology of privacy? How do we perceive privacy? Why do we disclose personal information about ourselves on the Internet, and what does this reveal about our own personalities? In six chapters, this dissertation discusses potential answers to these questions. Chapter 1 provides a general introduction to the overarching research question, Chapters 2-5 include the four main studies that either have already been published (Study 1, 2, and 3) or have been submitted for publication (Study 4), and Chapter 6 summarizes the dissertation and offers a concluding privacy synthesis.

In Study 1, I propose a new privacy theory, the so-called *Privacy Process Model* (PPM). The PPM states that privacy consists of three major elements: the privacy context, the privacy perception, and the privacy behavior. In order to balance the three elements people constantly engage in a privacy regulation process, which can be either explicit / conscious or implicit / subconscious. Through concrete examples of new digital media, several implications of the PPM are demonstrated.

In Study 2 and 3, I analyze aspects of privacy that pertain to the Internet in particular. Both studies explain and predict concrete online privacy behaviors on social network sites (SNSs). An observation known as *privacy paradox* states that privacy behaviors cannot be predicted sufficiently by means of psychological antecedents such as privacy concerns. In Study 2 (*Is the Privacy Paradox a Relic of the Past?*), which is co-authored by Prof. Dr. Sabine Trepte, we analyze this observation through the results of an online questionnaire with 579 respondents from Germany. By adopting a theory of planned behavior-based approach, the results showed that self-disclosure could be explained by privacy intentions, privacy attitudes, and privacy concerns. These findings could be generalized for three different privacy dimensions: informational, social, and psychological privacy behaviors. Altogether, Study 2 therefore suggests that the privacy paradox does not exist.

Study 3 (*An Extended Privacy Calculus Model for SNSs*), co-authored by Prof. Dr. Miriam J. Metzger, builds upon the results of Study 2 and investigates whether psychological antecedents can explain not only online self-disclosure but also online self-withdrawal, all within one single theoretical and empirical framework. Using a privacy calculus-based approach, the study analyzes data from a U.S.-representative online sample with 1,156 respondents. The results showed that self-disclosure could be explained both by privacy concerns and expected benefits. In addition, self-withdrawal could also be predicted by both privacy concerns and privacy self-efficacy. In conclusion, Study 3 demonstrates that perceived benefits, privacy self-efficacy, and privacy concerns together predict both online self-disclosure and online self-withdrawal.

Study 4 (*Predicting the Desire for Privacy*), also co-authored by Miriam J. Metzger, then again broadens the perspective and analyzes the relationship between the desire for privacy and different facets of personality, with a focus on aspects of personal integrity. Building on Altman's privacy regulation theory, we tested our hypotheses with a 2-study approach: First, we conducted an online questionnaire with 296 respondents and second, we ran a laboratory experiment with 87 participants. The results of the questionnaire showed several significant relationships: For example, respondents who reported lacking integrity and being more shy, less anxious, and more risk averse were all more likely to desire privacy. The experiment, for example, showed a statistical trend that participants who had written an essay about past negative behaviors were more likely to express an increased desire for privacy from other people. In addition, an implicit association test (IAT) showed that participants whose IAT results implied higher lack of integrity also desired more privacy from government surveillance. In conclusion, the results evidence that the desire for privacy relates with several aspects of personality and, notably, also with personal integrity.

In the overarching discussion, I combine the aforementioned results in order to draw a novel and updated picture of privacy. This picture suggests that online self-disclosure is not paradoxical but explainable. Being able to understand online privacy behaviors is important; however, this is not only because the Internet has paramount importance in social and professional contexts, but also because our desire for privacy can even reveal central aspects of personality, such as our own personal integrity. Finally, I integrate the results with the aim to contribute to a new privacy synthesis. This privacy synthesis argues that modern societies should try to design new cultural artifacts about privacy, update old and obsolete social privacy cybernetics, foster a better understanding of the conceptual nature of privacy, work toward new and more protective privacy laws, and, above all, aim to leverage overall privacy literacy.

Introduction

1 Introduction

1.1 A brave new privacy?

In his novel *Brave New World*, Aldous Huxley (1932) describes a fictitious society of the future, one that is full of technological and societal revolutions. In this new world, people can learn while they are sleeping, have promiscuous relationships, benefit from optimized genes, reproduce artificially, and enjoy perennial instant gratification (through a drug called "soma"). On the one hand, this enabled some significant societal improvements, such as stability, peace, and freedom (according to the totalitarian government); on the other hand, however, these changes also curtailed several important socio-psychological aspects, such as eudemonic growth or individual self-realization (according to the main protagonist Bernard Marx). In the end, the negative consequences prevailed — this brave new world was not positive but negative, Huxley designed a dystopia and not a utopia.

Since Huxley's novel in 1932, the real world has changed substantially as well, and several sweeping technological and societal revolutions took place. Interestingly, some of these changes are similar to those described by Huxley: People nowadays google in order to attain all the information they need, find their romantic partners online through apps such as tinder, optimize their physique by counting and tracking every single step they make, talk with their friends and family at any time and at any place, and overall just never seem to be bored. But what do these technological and societal changes imply, are they positive or negative?

Notably, almost all of the aforementioned changes have one thing in common: They affect peoples' privacy. When, what, and how much do we want to disclose about ourselves? Information systems now record, store, and make accessible a large part of things that had not been documented before, had been forgotten, or had not been accessible. What once was private can now become public. There is no doubt that the recent technological and societal changes have both changed and challenged the foundations of privacy — with no end in sight.[1] Hence, even though it remains somewhat controversial and polemic to say, there seems to be some truth to the claim that with the end of the 20th century, society changed so significantly that indeed a brave new world was born, a world with eminent effects on everyone's privacy.

1.2 Thesis: Our privacy has decreased

In order to discuss how the socio-technological changes affected privacy exactly, it is useful to have a look at the general mechanisms of change. To this end, Georg Wilhelm Friedrich Hegel offered a most prominent and helpful template, the so-called "Hegel's dialectic" (Hegel, 1807/2011). According to Hegel, societal change often takes place as follows: A status quo (thesis) causes an extreme reaction (antithesis), which eventually leads to a more moderate solution (synthesis). Change is a social process and always messy and cumbersome: A difficult situation will provoke an extreme reaction, which will entail both important improvements but also grave new errors (Hegel, 1807/2011). Only gradually, and after much to and fro, a more moderate solution can manifest.

As illustration, consider the following prominent example from history, the French Revolution (The Philosophers Mail, 2015): The regal decadency during times of absolutism in France in the 18th century was a strong provocation for the impoverished French people (thesis). Eventually, this provocation paved the way for the French revolution, with the aim to empower the people (antithesis). The code civil, a cornerstone of personal freedom and civil rights, was passed; but, at the same time, Robespierre's reign of terror also started to devastate society. Only gradually and several decades later, modern democracies were able to manifest (synthesis). Hegel's tripar-

[1] Interestingly, the rate of technological progress seems to increase steadily: According to the law of accelerating returns, technological progress does increase not only linearly but even exponentially (Kurzweil, 2005). According to Moore's law, components per computer chip double each year, a hypothesis that is by now well supported by empirical data (Mack, 2011). Hence, the future will very likely provide even more technological devices that collect personal data.

tite observation of thesis, antithesis, and synthesis thus offers a promising framework to analyze current phenomena of privacy, which is why I will adopt it in this introduction and also later in the overarching discussion.

Thesis: In the course of the past years, our privacy has decreased significantly. It has decreased because the status quo, from an intrapersonal perspective, encompasses an unprecedented *intrusion into personality*. Others can attain very sensible information about us, sometimes even information that we do not know ourselves — for example, our shopping habits, our color preferences, or our social network structure. Others can acquire pieces of information about us that accurately describe our personality, our inner selves. Second, the status quo epitomizes a *loss of control*. Companies have the capabilities to precisely predict our personality, and users have no chances to prevent them from doing so (Matzner, 2014). Moreover, even if we deliberately allow Facebook to access our information, we cannot prevent Facebook from passing on that information to others.[2] Latent profiles are construed with information drawn from several sources, a process that is beyond our control (Matzner, 2014). Third, the status quo undermines the human *ability to forget*. The characteristic of humans brains to forget information is oftentimes considered a blessing (e.g., Smithstein, 2010-07-25): Forgetting eventually helps to forgive, one might consider it the brain's inherent capacity to "wipe the slate clean". As instant messengers today record and store the content of verbal communication, this capacity is undercut. Fourth, the status quo is a challenge for *cross-contextual integrity* (Nissenbaum, 2010). Whereas before it was possible to represent different personas in different contexts, this possibility gets lost due to a so-called context collapse (boyd, 2008). Context collapse describes the characteristic of SNSs to combine several distinct social groups into one meta group. Hence, one's partner, family, friends, colleagues, and acquaintances are suddenly merged into one single audience. And this can pose a significant threat, as it increases the need to communicate very coherently. The Internet is full of anecdotes in which communication went awry, entire websites are dedicated to privacy mistakes.[3]

[2] for example, all pieces of information that fall under Facebook's IP-License; see section 6.4.4, p. 179

[3] e.g., www.en.webfail.com/

One could argue that before, it was easier to get away with not telling the entire truth. Today, the need for integrity increases and, thus, interferes with aspects of self-disclosure and privacy.

Privacy also decreases from a societal perspective. First, because corporate companies such as Facebook, Google, or Amazon have exhibited a substantial *increase in private power*. By now, they have become entities that provide a worldwide infrastructure. Apple, for example, determines for billions of people how to communicate, how to buy, and what information to attain. Never before had organizations existed with such knowledge and such power. The individual loses some of his or her autonomy, as social conventions and processes compel individuals to use very specific proprietary services. And second, because the lack of privacy is continuously increasing (especially due to big data), this can curtail political deliberation and become a *threat for democracy*. In the book *Privacy, Publicity, and Democratic Decision-Making in Times of Big Data*, edited by Philipp Richter, eight scholars coming from eight different research disciplines warn of this risk. Several notions are presented suggesting that democratic deliberation is currently thwarted — for example, because of the fact that statistical algorithms derived from big data analyses are capable of precisely predicting users' voting behavior (Nebel, 2015). Eventually, this might undermine the anonymity of the voting process, a prerequisite for democracies.

This novel intrusion into personality by means of computer generated predictive algorithms, the loss of control, the challenge of cross-contextual integrity, the increase in corporate power, and the new threat to democracy hence converge to the following thesis: In the course of the past years, our privacy has decreased significantly.

1.3 Antitheses: Post privacy or total privacy?

What is the reaction, what is the antithesis? So far, two major antitheses emerged: First, the *post privacy* antithesis. The post privacy antithesis is most vividly represented by Gordon Bell, a researcher emeritus at Microsoft Research (e.g., Wilkinson, 28.05.2007). Gordon Bell is one of the founding fathers of lifelogging, which stands for the continual capturing of each and every personal and interpersonal action (Bell & Gemmell, 2009). Later, others followed his lead — for example Jeff Jarvis (Jarvis, 2011) and Christian Heller (Heller, 2011) — and proclaimed that the time of privacy is finally over. The antithesis of the post privacy movement is: Privacy might have decreased, but privacy was never important in the first place, which is why we should abandon the concept altogether.

The second and very diametrical reaction is the *total privacy* antithesis. This antithesis is most prominently spearheaded by Edward Snowden, who is a former NSA contractor and who revealed the mass surveillance activities by the NSA (Greenwald, 2013.06.06). Other prominent advocates of the total privacy movement include Jacob Appelbaum (Brooke, 2011.10.11) or Max Schrems (Gibbs, 2015.12.03). The total privacy antithesis proclaims that by using privacy enhancing technology (for example, sending PGP encrypted e-mail, surfing in the deep web, or using air-gapped computers) everyone should protect any communication from third parties. The antithesis of the total privacy reaction is: If privacy continues to decrease, our freedom, social life, and democracy will eventually cease to exist, which is why we have to safeguard our privacy under all circumstances.

I argue that both antitheses will not be the solution to the thesis that privacy has decreased significantly: Post privacy as a solution can only be feasible for a fraction of the population, as it would ridicule in the long run the convention to wear clothes, to shut bathroom doors, or to close the curtains when having sexual intercourse — conventions that only few would be willing to abandon. Similarly, total privacy cannot be the solution as well: First, total privacy is also only feasible for a fraction of the population, as a very high technical expertise is needed to employ all means necessary to use anonymous and encrypted technology. Second, legal authorities need to have at least some capability of limiting privacy in order to enforce the law: For example, identification is necessary for imposing traffic penalties, stopping tax evasion, or prosecuting criminal activities. Hence, total privacy or complete anonymity for everyone and at all times does not seem to be an adequate solution either.

1.4 Toward a privacy synthesis

Ultimately, this dissertation aims to offer some helpful thoughts regarding a potential synthesis of privacy. I aim to achieve this primarily by trying to contribute to our general understanding of privacy. To this end, this dissertation features four separate studies, including a theoretical analysis of privacy as a psychological concept (Chapter 2), two empirical studies on specific online privacy behaviors (Chapter 3 and Chapter 4), and an empirical study on which aspects of personality make people desire more or less privacy (Chapter 5).

What is the exact nature of privacy? Even among experts, the notion is widespread that "privacy is a messy and complex subject" (Nissenbaum, 2010, p. 67). For example, what is the difference between privacy, freedom, autonomy, control, or self-disclosure? Interestingly, especially for the context of SNSs is has been argued that because users have a lot of control over their in- and outputs they have the illusion of privacy, feel free, and experience a "shelter for ... authentic living" (Trepte & Reinecke, 2011, p. 61). Ultimately, this shows that aspects of control, privacy, and even authenticity are closely related to one another. At the same time, one could argue that if privacy was *only* about being in control of one's accessibility (a position that is, for example, supported by Burgoon, 1982) than a prisoner who is currently sitting in his cell, not being able to decide when to leave his or her compartment, accordingly would have no privacy at all. But can that be true? Does he really have no privacy, given that he is remote, alone, and just by himself? Overall, it is apparent that the theoretical configuration of privacy is still challenging, which is why I argue that first of all we have to advance our conceptual understanding of privacy, and especially our understanding of privacy in online contexts. To this end, I hold that it is not so much important to develop a decidedly new model of privacy. Instead, given the large number of already existing theories on privacy (e.g., Altman, 1975; Burgoon, 1982; Gavison, 1980; Petronio, 2002; Warren & Brandeis, 1890; Westin, 1967), which all comprise numerous valuable insights, I propose that it will be more profitable to integrate the aforementioned theories into one encompassing theory of privacy.

With this aim, I have developed the privacy process model (PPM), which I present in Chapter 2 of this dissertation. Throughout the entire dissertation, the PPM provides the theoretical framework for the empirical studies.

Next to improving our general comprehension of privacy theory, I argue that it is equally important to leverage our specific understanding of privacy behaviors. Especially on the Internet, several controversial privacy behaviors can be found. Consider the following example: In general, people are most willing to self-disclose in situations when they feel private, withdrawn, and in control of their environment (e.g., Westin, 1967). On the Internet, however, there are several contexts in which there is almost no privacy whatsoever, given that Google is analyzing its users' personal mail, that Facebook is scanning its members' social conversations, and that the NSA is generally intercepting as much computer traffic as possible (e.g., The Guardian, 2014). And still, people are self-disclosing vividly on these sites. How can that be? With the aim of answering these questions, I subsequently present two empirical studies that analyze concrete privacy behaviors and their corresponding psychological correlates for SNSs. Besides the example mentioned above, a number of other studies have also suggested that online privacy behaviors are somewhat paradoxical — most of all, because people with more privacy concerns had not been found to disclose less personal information on SNSs (e.g., Taddicken, 2014; Tan, Qin, Kim, & Hsu, 2012; Tufekci, 2008). As a result, in Chapter 3, I first analyze the privacy paradox by using a specific behavior explanation paradigm, the theory of planned behavior (Ajzen, 1985), aiming to find significant relations between psychological concepts of privacy and online self-disclosure. Second, in Chapter 4, I refer to a different strand of privacy research, the so-called privacy calculus (e.g., Krasnova, Veltri, & Günther, 2012), in order to provide a more comprehensive analysis of online privacy behaviors. Whereas the theory of planned behavior-based approach addresses privacy concerns as predictors of privacy behaviors, the privacy calculus states that next to privacy concerns also expected benefits can explain privacy behaviors. In addition, literature on the privacy calculus so far analyzed only self-disclosure as behavioral criterion, which is somewhat incomplete given that privacy behaviors also include acts of self-withdrawal (i.e., the deliberate deletion, obfuscation, or withholding of information; e.g., Debatin, 2011). As a result, I developed the extended privacy calculus model for SNSs, which extends the scope of prior research by including self-withdrawal behaviors as additional dependent variable.

Whereas the first three studies focus on a better understanding and explanation of privacy, the last empirical study targets the relevance and the implications of privacy. In Chapter 5, I hence explore the relation between privacy and specific facets of personality, focusing on the question of whether people who lack integrity might desire more privacy. So far, this question has not been analyzed in an empirical study, although there are several plausible theoretical reasons why this relationship might exist. For example, according to Altman (1976) people reinforce their social boundaries in situations of imminent risk, and subsequently withdraw from social interactions (thereby increasing their privacy). People who have done something dishonorable or even illegal indeed face a higher risk, because others would disapprove of their behavior, which is why they have a good reason to conceal that information. Or in more technical terms, it seems plausible that people who lack integrity have an increased desire for privacy. On the other hand, it seems equally possible that people desire privacy because they are generally more withdrawn, shy, or risk-averse. Pedersen (1982), for example, found that people who described themselves as "introverted thinkers" were more likely to prefer social isolation. Hence, it could be that several different facets of personality affect peoples' desire for privacy, including aspects that can be considered negative, neutral, or positive. Analyzing this relationship seems relevant given that there are very distinct and conflicting positions regarding the inherent value of privacy. Some say that it is important to limit privacy in order to prevent crime (e.g., the mayor of Chicago, Rahm Emanuel; Dellimore, 2013), others hold that everyone should generally have the basic right to be let alone (Warren & Brandeis, 1890); some argue that privacy hinders social participation (e.g., the CEO of Facebook, Mark Zuckerberg; Kirkpatrick, 2010), others claim that privacy fosters personal growth (Westin, 1967). Hence, what does it reveal about someone's personality if he or she desires more privacy? Might he or she indeed lack integrity or, by contrast, is that person simply more shy? And what are the potential societal implications?

In Chapter 6, I combine the results of the aforementioned studies in one overarching general discussion. First of all, I evaluate the studies' results in light of the extant literature, highlighting some novel aspects that this dissertation affords and addressing some problematic positions that future research might want to resolve. Eventually, I discuss the societal and practical implications of this dissertation. What does it mean that our privacy is decreasing, how does it affect the world we are living in? Is this "brave new privacy" good or bad, do the positive or do the negative aspects prevail? How do we have to react to the changes introduced by new information technologies, and, overall, what is a potential privacy synthesis? These questions are of a very general nature, broad, and maybe even philosophical. Can one dissertation answer these questions? No, of course not. However, it becomes increasingly apparent that psychology and communication research play a major role in answering these questions, given that they offer convenient theoretical and methodological frameworks to analyzing these questions. In his 2015 article *Communication and the good life*, former president of the International Communication Association (ICA) Peter Vorderer discussed the challenges of the digital revolution and ended with the following conclusion: "What a mess, what a wonderful challenge for a discipline like ours, because it is this field that 'literally studies ways in which the world is made' (Calhoun, 2011, p. 1495)" (p. 8). Therefore, in the final chapter, I also aim to provide some practical and societal implications that can be drawn based on the results of this dissertation.

Privacy is a broad meta concept that reverberates in various areas of social life. At the same time, privacy is a very specific process that unfolds in concrete behavioral manifestations. Privacy is not neutral, it is often considered a value, it is deemed important for democracies, and it might be related to personality, maybe even to integrity. That is the point where this dissertation starts. The aim is to develop a better understanding of the psychology of privacy and, eventually, to contribute to a new privacy synthesis. The research question of this dissertation, in short, might thus be described best as follows: What happens in each one of us when we provide information about ourselves, for example on SNSs, and what could this process reveal about our personality? Overall, what is the psychology of privacy?

Literature

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control* (pp. 11–39). Berlin, Germany: Springer. doi:10.1007/978-3-642-69746-3{_}2

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, *8*(1), 7–29. doi:10.1177/001391657600800102

Bell, C. G. & Gemmell, J. (2009). *Total recall: How the e-memory revolution will change everything*. New York, NY: Dutton.

boyd, d. m. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13–20. doi:10.1177/1354856507084416

Brooke, H. (2011.10.11). How the US government secretly reads your email. *The Guardian*. Retrieved from www.theguardian.com

Burgoon, M. (Ed.). (1982). *Communication yearbook 6*. Beverly Hills, CA: Routledge.

Calhoun, C. (2011). Communication as social science (and more). *International Journal of Communication*, *5*, 1479–1496.

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47–60). Berlin, Germany: Springer.

Dellimore, C. (2013). Emanuel stresses value of surveillance cameras in probe of Boston bombings. Retrieved from http://chicago.cbslocal.com/2013/04/17/emanuel-stresses-value-of-surviellance-cameras-in-probe-of-boston-bombings/

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*(3), 421–471.

Gibbs, S. (2015.12.03). Max Schrems demands Facebook stop EU to US data transfer due to snooping. Retrieved from www.theguardian.com

Greenwald, G. (2013.06.06). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from www.theguardian.com

Hegel, G. W. F. (1807/2011). *Phänomenologie des Geistes*. Paderborn, Germany: Salzwasser Verlag.

Heller, C. (2011). *Post Privacy: Prima leben ohne Privatsphäre*. Munich, Germany: Beck.

Huxley, A. (1932). *Brave new world*. London, UK: Chatto & Windus.

Jarvis, J. (2011). *Public parts: How sharing in the digital age improves the way we work and live*. New York, NY: Simon & Schuster.

Kirkpatrick, M. (2010). Facebook's Zuckerberg says the age of privacy is over. Retrieved from http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

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), 127–135. doi:10.1007/s12599-012-0216-6

Kurzweil, R. (2005). *The singularity is near: When humans transcend biology*. New York, NY: Viking.

Mack, C. A. (2011). Fifty years of Moore's law. *IEEE Transactions on Semiconductor Manufacturing*, *24*(2), 202–207. doi:10.1109/TSM.2010.2096437

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. doi:10.1108/JICES-08-2013-0030

Nebel, M. (2015). Facebook knows your vote! – Big Data und der Schutz politischer Meinung in sozialen Netzwerken. In P. Richter (Ed.), *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data*. Baden-Baden, Germany: Nomos.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Pedersen, D. M. (1982). Personality correlates of privacy. *The Journal of Psychology*, *112*(1), 11–14. doi:10.1080/00223980.1982.9923528

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Smithstein, S. (2010-07-25). The importance of forgetting (or not). Retrieved from www.psychologytoday.com/blog/what-the-wild-things-are/201007/the-importance-forgetting-or-not

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. doi:10.1111/jcc4.12052

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research*, *22*(2), 211–233. doi:10.1108/10662241211214575

The Guardian. (2014). Microsoft, Facebook, Google and Yahoo release US surveillance requests. Retrieved from https://www.theguardian.com

The Philosophers Mail. (2015). The great philosophers: Hegel. Retrieved from www.thephilosophersmail.com/perspective/the-great-philosophers-6-hegel/

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). Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6{_}6

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36. doi:10.1177/0270467607311484

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

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Wilkinson, A. (28.05.2007). Remember this? A project to record everything we do in life. *New Yorker*. Retrieved from www.newyorker.com/magazine/2007/05/28/remember-this

Study 1

2 The privacy process model

Preamble

Abstract

The following article develops a new model of privacy referred to as the privacy process model (PPM). Drawing on extant literature on privacy, the PPM analyzes the distinct conditions, mechanisms, and regulations of privacy. First, it identifies an objective privacy context, which is subdivided into informational, social, psychological, and physical dimensions. Second, it examines subjective privacy perceptions, which are divided into the same dimensions. Third, it observes privacy behavior, which is the amount of self-disclosure people show. If either privacy perception or privacy behavior differ from a desired status, people will engage in a privacy regulation, meaning that they will try to alter their privacy context or their privacy behavior. Able to account for online as well as offline contexts, the PPM offers a novel and universal approach to understanding privacy.

Keywords: privacy process model, context, perception, regulation, social network site, SNS, Facebook

Status of publication

The following study has already been published. Please cite as follows: Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

The content of the text has not been altered. For reasons of consistency, the language and the formatting have been changed from British English to American English.

2.1 Introduction

In recent years, privacy has become one of the most prevalent topics in public discourse. Individuals, political parties, and private companies alike all ponder questions relating to the phenomenon privacy. The more people analyze privacy, the more approaches to privacy there are. These approaches can vary substantially — for example, some concentrate on technical issues such as the security of data online, others to psycho-social aspects such as the seemingly preposterous acts of self-disclosure on Social Network Sites (SNSs).

Because privacy is often talked about, the impression arises that the meaning of the term is established. But this is not the case — even in scientific contexts, people display very distinct understandings of privacy. Numerous definitions of privacy have been developed (see, e.g., Altman, 1975; Burgoon, 1982; Gavison, 1980; Petronio, 2002; Warren & Brandeis, 1890; Westin, 1967). Yet, as Helen Nissenbaum (2010) argues, none seems to be capable of grasping the entire truth. In the following, I address this problem by developing a new model of privacy, the privacy process model (PPM). The PPM is conceptualized on the basis of a theoretical analysis of extant literature on privacy and privacy models, and on recent empirical studies. The PPM is designed to arrange existing definitions, mechanisms, and effects in a single model. It thereby aims to integrate privacy's most important aspects, but also takes into account that all variables are interdependent. I start by giving an overview of already existing models and definitions of privacy; afterwards, I outline the PPM. I then present a possible application of the PPM in the field of new media in order to illustrate the use of the PPM and conclude by discussing the strengths and limitations of the PPM.

2.2 Theories of privacy

The fact that so many publications explicitly deal with privacy shows at least one thing: The definition of privacy is not self-evident. Extant definitions lead to a heterogeneous and sometimes inconsistent scientific depiction of privacy (Margulis, 2011). Nissenbaum describes the situation with the following words: "One point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject" (Nissenbaum, 2010, p. 67). I will therefore start with addressing the literal meaning of the term privacy. Subsequently, I will present the core elements of three essential works on privacy. These are Alan Westin's *Privacy and Freedom* (1967), which argues that privacy must be treated as a particular condition or status; Irwin Altman's *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (1975), which highlights the importance of the regulatory aspects of privacy; and Judee Burgoon's *Privacy and Communication* (1982), which elaborates different dimensions of privacy.

When dealing with privacy and the different depictions of it, it is helpful to look at its original meaning. The word "private" derives from the Latin word privatus, which literally means "deprived", and more extensively "robbed, free, personal". A private thing thus reflects something that is separate, not attainable for everybody and belonging to a particular person. The term privacy accordingly measures the extent to which somebody or something is detached from the influence of others. Though this might seem trivial, it is important to note — in some definitions, privacy is defined as the control over the degree of detachment (see, e.g., Burgoon, 1982). If this was the case, however, a lonely wanderer would be as private as a person on the dance floor of a nightclub: Both are in equal control of all possible aspects of their privacy. Hence, in order to be able to account for this apparent difference, privacy should always be a measure of the degree of a certain type of detachment.

According to Westin, privacy can be defined as "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" (Westin, 1967, p. 7). Four different conditions arise as a result: solitude (freedom from presence and surveillance of others); intimacy (freedom to be able to hold relationships); anonymity (freedom from identification); and reserve (limitation of self-disclosure). Westin thus follows an approach that classifies different states of privacy. Altogether, it is important to note that privacy is understood as a proportionate withdrawal from social interactions.

Altman's definition mirrors Westin's to a great extent, but adds an important notion: Taking a socio-psychological approach, Altman places more emphasis on the constant dialectic and dynamic regulation of privacy. He therefore stresses that there is no paramount condition of privacy that one should generally try to attain. On the contrary, desired levels of privacy fluctuate depending on the specific situation and the interaction that takes place. In order to achieve a desired level of privacy, people constantly adjust interpersonal boundaries. Privacy thus resembles a thermostat: First, the current level of privacy is perceived. If the perceived level differs from the desired level, the current status is appraised negatively. This negative appraisal results in an attempt to regulate the current status. If people perceive themselves as having too little or too much privacy, they will try to change their behavior. Altman's assumptions have been tested in various studies. Vinsel, Brown, Altman, and Foss (1980) were able to show that students who engaged in various forms of privacy boundary adjustments — for example, closing doors when they need to study or consciously seeking company in the dorm when appropriate — showed an increased likelihood to successfully pass the first year and to advance to the next.e

The next important progress in the definition of privacy was made by Judee Burgoon in 1982. In an analysis of the literature available at the time, Burgoon proposed that privacy and all associated regulations take place in four different dimensions: informational privacy, social privacy, psychological privacy, and physical privacy. Informational privacy measures how far people can decide what information is collected about themselves. Is behavior recorded on a video-tape? Can the person be clearly identified? How much information about biography and personality is accessible? Social privacy reflects the extent to which people can decide whom they interact with, whom they share personal information with and who has access to them. Psychological privacy captures the degree to which people can control mental in- and outputs, what kind of information they are confronted with and what kind of information they are free to voice. Physical privacy defines the adjustment of factual physical boarders: How close people are to one another or how thoroughly people are separated, for example by windows, fences or walls. According to Burgoon, privacy is very much about the controllability of these dimensions. Again, no general desirable condition of privacy is stated. Burgoon argues that when people are capable of adjusting the dimensions, privacy is high; when people are not in the position to do so, privacy is low. Burgoon's approach is empirically supported by the fact that people display different kinds of behaviors in each dimension. A longitudinal study has investigated whether people changed their privacy behavior on Facebook after experiencing negative interactions after somebody left a hostile post on their Facebook wall (Trepte, Dienlin, & Reinecke, 2014b). It was found that after such negative experiences, people did increase their informational privacy — for example by disguising their authentic names. Nevertheless, respondents did not change their social or psychological privacy behavior.

In their attempt to define privacy, the aforementioned theories more or less claim to be comprehensive. Yet, each takes a different but at the same time viable viewpoint on privacy, leading to a somewhat diffuse and unsatisfactory theoretical definition. With the PPM, outlined below, I aim to conceptualize a model that integrates the presented definitions and adds important new aspects.

2.3 The privacy process model

If one regards the literal meaning of privacy together with the aforementioned theories, a broader picture of privacy can be seen. Privacy emerges as the degree of separation from others (the literal definition); as a separation that can be characterized by different conditions (Westin, 1967); as being about a continuous adjustment of individual boundaries (Altman, 1975); and as taking place in four different dimensions, namely the informational, the social, the psychological and the physical (Burgoon, 1982).

2.3.1 Privacy context

The literal translation of the word privacy and the work by Westin (1967) suggest that privacy is first and foremost an objective condition people find themselves in: People are either alone or in company. The degree of privacy should thus be objectively measurable. This notion comprises the first factor of the PPM and shall be called the *privacy context*. It seems reasonable to further adhere to Burgoon (1982), who argues that there are four dimensions of privacy. Unlike Burgoon, I do not consider the dimensions as a degree of control over privacy, but — bearing in mind the literal translation of privacy — as a degree of individual detachment. The informational privacy context thus measures the amount of information collection taking place in a given situation. Are cameras in use? Is another person taking notes? Is there an active voice recorder? The social privacy context refers to the number and the kind of people present. The fewer people there are in one room and the more one is acquainted with them, the higher the social privacy context becomes. For the PPM, I propose measuring the dimension of psychological privacy somewhat differently to Burgoon (1982). Burgoon defines psychological privacy as the freedom of thought, a condition that in most cases can be regarded as warranted and as a whole somewhat difficult to operationalize. I thus propose that psychological privacy be taken as a measure of the extent to which people present in a situation engage in intimate and personal, or trivial and impersonal conversations. The more that people disclose intimate information, the higher the psychological privacy context. If people elaborate on mundane topics like the weather, psychological privacy is regarded as low. Defining psychological privacy this way offers one benefit: It accounts for all the situations in which people are able to think as they please, but not speak as they like. Finally, the physical privacy context concerns the extent of the proximity of others. How close are other people? Can or are they touching me? Can they see me?

All four dimensions of the privacy context are independent and can differ from each other. For example, on the Christmas party of a large company, informational privacy is high (no observation and collection of personal data); social privacy is low (presence of several personally distant colleagues); psychological privacy might be high (a lot of personal, non-business related talk); and physical privacy moderate (for example, when being seated together at a table in a restaurant). Furthermore, the privacy context can be defined for different kinds of situations, ranging from offline contexts such as business meetings, cocktail parties, or even confessions in a church to online contexts such as Facebook groups / wallposts, YouTube channels, or public Internet platforms.

2.3.2 Privacy perception

The privacy context is the given situation that can be assessed and described objectively. That being said, it can be argued that the privacy context also needs to be perceived — research shows that people differ greatly in their perception of particular situations (see, e.g., Haber, Cohen, Lucas, & Baltes, 2007). Especially in the case of online media use, people often perceive greater privacy than there actually is (Trepte & Reinecke, 2011b). Barnes (2006) raises the point that users of SNSs are often not aware of the fact that a substantial part of their conversations are not private but accessible for other users. In order to account for this difference, the factor *privacy perception* is included in the PPM. Again, the privacy perception is defined in the four dimensions regarding Burgoon (1982).

The following examples of the four dimensions of privacy perception show the importance of these distinctions. In terms of informational privacy, people tend to feel anonymous and unobserved in public spaces. Yet this assumption is not true: In Britain, on a busy day in an urban environment, a person will have their image captured by approximately 300 cameras on thirty different CCTV systems (Norris & Armstrong, 1999). In the entire country, more than 50,000 cameras monitor public places in 500 cities (Hempel & Töpfer, 2004). Because of the discrepancy of context and perception, it is mandatory to install signs with notifications when CCTV is in use (see, e.g., Hempel & Töpfer, 2004). Facebook, on the other hand, serves as a perfect example of false social privacy perception. It can be shown that people are not fully aware of their entire audience when posting messages on their timeline (boyd, 2008a). This phenomenon has been termed the context collapse — meaning that users address several distinct groups of persons at once, without being able to find the appropriate level of self-disclosure (boyd, 2008a). Hence, it can be stated that the people's perception of their social privacy exceeds the factual social privacy context.

The same discrepancy can be assumed for psychological privacy perception: Again, some Facebook users perceive a very pronounced psychological privacy and assume that a lot of private information is being shared online and that it is generally appropriate to behave similarly (Trepte & Reinecke, 2011b). All the same, studies show that a substantial part of SNS users do not disclose information online and remain so-called lurkers (Metzger, Wilson, Pure, & Zhao, 2012). People generally seem to overestimate the amount and the intimacy of information being shared online. The discrepancy between physical privacy perception and context is probably the least pronounced. Only in few situations are people incapable of assessing who shares their presence and who is how close. This being said, people differ in their estimate of physical privacy: For some people, being touched by somebody during a conversation might be very usual and not be considered to reduce physical privacy. People in other cultures, however, would consider this as an intrusion and as a significant reduction of their physical privacy (see, e.g., Hall, 1990). Again, all four dimensions are distinct and hence judged independently. At this point in the discussion, the most important aspects of privacy have been covered. Yet, arguably the most intriguing question regarding privacy has been omitted: How does privacy influence human behavior?

2.3.3 Privacy behavior

Depending on contexts and privacy perceptions, people will engage in different kind of privacy behaviors (see, e.g., Margulis, 2003). If people feel they are in a private situation, they are willing to talk about different things compared to less private contexts (Westin, 1967; Trepte, 2012). I therefore include the factor *privacy behavior* as the third major element of the PPM. One question remains: What exactly is privacy behavior? In the PPM, I define it as any behavior that involves acts of self-disclosure. According to Wheeless (1976, p. 338), a self-disclosure is "any message about the self that a person communicates to another. Consequently, any messages or message unit may potentially vary in the degree of self-disclosure present depending upon the perception of the message by those involved". In line with Wheeless and Grotz, numerous behaviors can be regarded as privacy-related: postings on Facebook, conversations among friends, talks in front of audiences, etc. For privacy behaviors, the four dimensions of Burgoon (1982) are not applicable. Instead, I will implement the approach by Taddicken (2011), which differentiates self-disclosure into the dimensions of facts, thoughts, feelings and experiences. Depending on how people perceive their privacy, they are more or less willing to engage in acts of self-disclosure. If people feel that they are in a private situation, they are more willing to expose personal information and to share intimate beliefs; they can be authentic, creative, or imaginative (Margulis, 2003; Trepte, 2012). Derlega and Chaikin (1977) have pointed out that self-disclosure is a function of privacy. Thus, it can be concluded that people are best able to self-disclose in situations of high perceived privacy.

2.3.4 The privacy regulation process and controllability

Altman (1975) makes the important point that people are constantly regulating their privacy. This finding appears to be a pivotal aspect of privacy, which is also implemented in the PPM. I propose that people cannot regulate their privacy perception. Nevertheless, people can obviously change their contexts as well as their behavior. As a result, the current status of privacy perception and privacy behavior are constantly compared to a corresponding desired state of privacy perception and a desired state of privacy behavior. If the current and the desired state do not correspond with each other, people will feel dissatisfied and want to alter this imbalance — in order to do so, they will engage in a privacy regulation. Privacy regulation can be established by two means: either by changing the context or by changing the behavior. Which route people will chose depends on the controllability: If it is more convenient to change the context, people will do this — and vice versa.

In order to illustrate the process of privacy regulation, let us consider the following example: A man comes home from work and sits down to have dinner with his family. Since his oldest son is away, a seat next to his younger son is free. Due to the distance, the current status of the physical privacy perception is increased. Because he wants to be close to his family at this moment, his desired physical privacy perception is low. He might change the privacy context: He decides to leave his usual seat in order to sit next to his son. He thereby engages in a privacy regulation by deliberately reducing his own physical privacy context. Additionally, people also always monitor their privacy behavior, that is the intimacy of their self-disclosure. Going back to our example, the man is now alone with his wife at the table. His desired level of self-disclosure is high, because he wants to talk about his bad feelings resulting from the difficult day at work. All the same, he realizes that they are still just talking about trivial things. Consequently, he shifts the topic and starts talking about his day and explains why he was not able to cope with the situation. He alters his privacy behavior by augmenting the amount of self-disclosure.

In order to be able to regulate, people need to be actually capable of doing so. The more people are in control of their privacy context and privacy behavior, the more they are able to adjust. This notion is not new; Burgoon (1982) was one of the first who stressed the importance of control for understanding privacy. Thus, in order for privacy regulation to take place, controllability needs to be granted. A prisoner, for example, is unable to determine whether he is being videotaped, whom to meet, or when to leave his cell. The mere presence of privacy is not the problem for him but the fact that he is unable to adjust it. A prisoner does not have controllability over his privacy. *Controllability* must therefore be the last factor in the PPM.

2.3.5 Integration of the privacy process model

The aforementioned elements of the privacy context, the privacy perception and the privacy behavior constitute the main frame of the PPM. Furthermore, the mechanism of privacy regulation and the factor of controllability complement the PPM. The entire model can be seen in Figure 2.1. The PPM is called a process model because it incorporates several sequential steps: People have a privacy perception, because they find themselves in a privacy context. People disclose certain pieces of information, because they feel private. First comes the situation, second its perception, and third the behavior. The fact that people constantly regulate their privacy context and privacy behavior further exemplifies the dynamic features of privacy, which are considered in the PPM.

The PPM builds on another important premise: All the different states of privacy context, privacy perception, and privacy behavior need to be regarded in a descriptive, that is in a neutral and value-free way. As Ruth Gavison (1980) writes:

> First, we must have a neutral concept of privacy that will enable us to identify when a loss of privacy has occurred so that discussions of privacy and claims of privacy can be intelligible. Second, privacy must have coherence as a value, for claims of legal protection

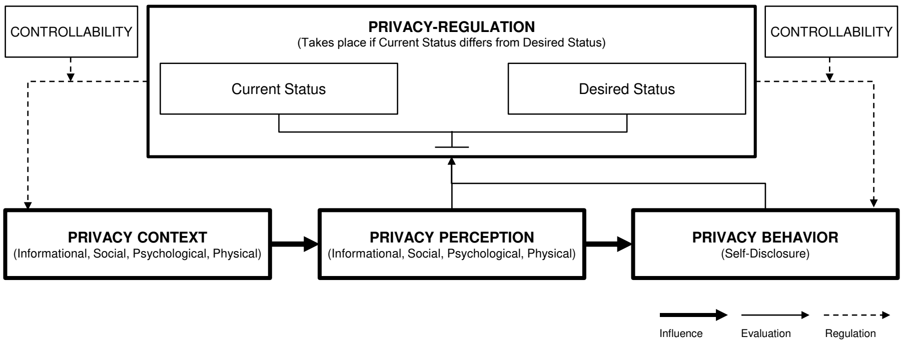

Figure 2.1: The privacy process model

> of privacy are compelling only if losses of privacy are sometimes undesirable and if those losses are undesirable for similar reasons. (p. 423)

Two viewpoints — for example, on the desired status of the privacy context — are therefore possible. The descriptive viewpoint would be: "On Facebook, privacy decreases." The normative one would be: "On Facebook, privacy is endangered!" In the prevailing media coverage a normative viewpoint is often adopted (Lindner, 2013). Generally, more privacy is deemed to equal better privacy. Margulis (2003) makes a strong point in saying that it is important to have privacy in order to reflect upon oneself, to promote creativity, and to foster relationships. However, this does not imply that a constant state of privacy is desirable. On the contrary, studies show that people in constant need of privacy are less satisfied with their lifes and show more negative affect (Trepte, Dienlin, & Reinecke, 2013). Furthermore, in the media, demands are often made for restrained and moderate behavior online. Nevertheless, increased amounts of self-disclosure on SNSs can be shown to be associated with higher degrees of life satisfaction and positive affect. Also, in a 2-year longitudinal study with 327 respondents it was found that people get more informational support online than offline (Trepte, Dienlin, & Reinecke, 2014a). In order to take advantage of that support, people necessarily need to open their privacy context to a certain extent.

Taken together, this shows that privacy first needs to be regarded descriptively. Only afterwards, with support by scientific research, should normative assumptions be made. Since research on these aspects is still sparse, more work on how to find absolute criteria of advisable behaviors needs to be conducted. First studies show that the results might contradict public opinion. To summarize the core implications of the PPM in seven axioms:

1. Any given situation (privacy context) leads to a particular sense of intimacy and confidentiality (privacy perception).
2. The higher the level of privacy perception, the more people will engage in a subsequent act of self-disclosure (privacy behavior).
3. For the privacy context as well as for the privacy perception, the dimensions of informational, social, psychological, and physical privacy can be differentiated.
4. For the privacy perception as well as for the privacy behavior, people perceive a current status of privacy, which they compare with a desired status of privacy.
5. If there is a discrepancy between current status and desired status, people engage automatically in a privacy regulation process. In the privacy regulation process, people aim to change either the privacy context or the privacy behavior.
6. In order for a privacy regulation to be able to take place, the controllability of either privacy context or privacy behavior needs to be warranted.
7. All elements shall be assessed not in a normative but in a descriptive heuristic.

2.4 The privacy process model in the context of the media

Numerous social interactions — like the purchase of goods, the handling of financial transactions, or the fostering of social relationships — have been shifted into the Internet. Therefore, these interactions now take place in a different context with different characteristics. These new characteristics are defined by (boyd, 2008b) as follows: The Internet is persistent, searchable, replicable, and scalable. This means that information will last longer, can be found more easily, can be recontextualized, and can be distributed and assessed on a large scale. All these points influence our own privacy: On account of the digital representation of ourselves, the form and the extent of access we grant to ourselves have been changed substantially. Because of this change, privacy in online contexts has become such an important topic. Even so, it is important to note that mechanisms pertaining to privacy establishment and regulation have not changed. Arguably, there is no such thing as *online privacy* that entails a new and different kind of privacy. On the contrary, the same mechanisms of privacy unfold, only in a substantially different context. Therefore, it is preferable instead to talk of *privacy in online contexts* (cf. Trepte et al., 2014a). The PPM considers this notion — that is, the privacy context can be defined for all possible situations. In the following, I advance a detailed, fictional example of how the PPM can be applied to a very common Internet process: communication on Facebook.

Stefan Mayer, 26 years old, is just about to finish his degree in medicine at a German university. If we regard the four different dimensions of his privacy context in Facebook, the following conditions can be found: (1) On Facebook, Stefan does not use his full name. Instead of naming his account *Stefan Mayer*, he calls himself *Ste Fan*. For his profile picture, Stefan uses a photo that clearly shows himself. He indicates his birthday, but not his postal address. Stefan does not have a public profile. For people who do not know Stefan, just a few pieces of information can be found. Nevertheless, friends of Stefan can access a lot of personal information about him online. Because Stefan also uses Facebook on his smartphone, Facebook can regularly retrieve his location. As a result, Stefan's informational privacy on Facebook might be considered low to medium. Evidently, this evaluation is volitional from his standpoint. In order to be able to assess the absolute magnitude of privacy contexts, such evaluations would need to be compared with averages of representative samples. (2) Stefan has 350 friends and uses no friend lists. Among Stefan's friends are his family, fellow students, current and old friends, people he used to go to school with, teammates of his football club, colleagues of his part-time job, and a few acquaintances. He is not befriended with any professors or lecturers from university, nor with his boss. As a result, Stefan's social privacy context can be regarded as being low. (3) Stefan's Facebook friends most of the time post things like links to videos and music on the Internet, share photos, or ask for ideas on what to do in the evening. The psychological privacy can be considered medium: His friends talk about interesting and relevant things, but not on Facebook. (4) Using Facebook does not affect his physical privacy, which is therefore high.

Let us now look at Stefan's own privacy perception. (1) Stefan knows that Facebook collects various kind of data. He is aware of the fact that without any precautions, unacquainted people would be able to find a lot of personal information. He therefore decides to use a nickname and set the status of his profile to private. He now thinks that his informational privacy is somewhat guaranteed, therefore probably medium. (2) Stefan knows that many people with whom he does not interact on a regular basis can read his messages. He tried to regulate the audience of his posts by not befriending any supervisors. People whom Stefan does not know cannot access his profile. All in all, he knows that he is not completely private, but thinks that his audience is familiar enough for him to be able to share some information with them without having to worry about being compromised. Hence, he estimates his social privacy as medium. (3) Stefan has the impression that on Facebook people sometimes post very intimate things, things he does not want to know. Nonetheless, he knows that for more sensitive issues, friends tend to send him a personal message. So he thinks that overall there is generally a medium to high level of psychological privacy on Facebook.

Moving on to different kind of privacy behaviors Stefan displays during the completion of his degree in medicine: (1) After he gets his exam results — he passes successfully — he leaves a happy status post saying that he is now officially a doctor and that it is the best feeling he has ever had. This post can be considered of medium intimacy: He informs people of an important event in his life, which is nothing trivial, yet does not include anything very intimate or self-revealing. (2) The day after he went to the graduation party, Stefan sends his best friend a picture of a girl he got to know, tells him about their evening, and that he likes her very much. This behavior can be regarded as being of high self-disclosure: He reveals to his friend very personal and intimate information, and asks for his opinion.

It is often argued that people perceive SNSs as more private than they actually are (Trepte & Reinecke, 2011b), and that not the factual but the perceived privacy context determines one's subsequent behavior. How, then, does the privacy context differ from the privacy perception in this fictional example? Whereas the informational context can be considered low to medium, Stefan perceives it to be medium. Whereas his social privacy can be estimated as low, Stefan regards it as medium. Again, the psychological privacy context was medium, whereas Stefan perceives it to be medium or even high. In our example, the privacy behavior was first a status update and second a personal message. The status update mirrors Stefan's perceived privacy: He estimates his audience as sufficiently familiar to be willing to inform them that he obtained his university degree. One day later, he wants to share another piece of information: That he got to know an interesting woman. This self-disclosure embodies much more intimacy, which he is not willing to share in the context of a public wall post. This shows that the current level of perceived privacy does not amount to his desired level of privacy. As a result, he engages in a privacy regulation by changing the privacy context: This information he shares privately with his best friend, thereby altering his social and psychological privacy context.

All different communication mechanisms available on Facebook enable privacy regulations: By choosing specific channels for particular self-disclosures, people regularly change their privacy context. Again, this shows that it is very important for people to be able to regulate contexts — some information is simply not meant for everybody. If this changing of contexts is not possible, people will need to change their privacy behavior, meaning that they will disclose less personal information than desired. Since self-disclosure is an important socio-psychological factor for people (Trepte & Reinecke, 2013), environments that provide a secure background for privacy behaviors are all the more important.

2.5 Discussion of the privacy process model

2.5.1 Implications

In this article, I have developed a new privacy model, the privacy process model. Several positive aspects are brought forward by the PPM. One of its major benefits is that the PPM includes the most important aspects of privacy in a single model. If one looks at existing definitions alone, the phenomenon of privacy cannot be fully understood. Privacy is not just a condition (Westin, 1967), it is not just the readjustment of interpersonal boundaries (Altman, 1975) and it is not just about being in control of these boundaries (Burgoon, 1982) — it contains all these aspects and more. For example, until now, no model for capturing privacy has distinguished between factual privacy contexts and subjective privacy perceptions. Since this distinction is relevant for both offline and online contexts, its incorporation in a privacy model seems viable. Moreover, the notion of self-disclosure has not been conceptualized in existing privacy related models. In the PPM, people are considered to engage in self-disclosure depending on the level of privacy they perceive. Additionally, the PPM sets the aforementioned variables in a contingent order: People first encounter a privacy context, out of this context a privacy perception arises, which then determines the extent of people's self-disclosure. Also, in everyday contexts, people constantly regulate aspects of privacy (Altman, 1975). The PPM is the first model that takes this notion into account: When the desired privacy differs from the desired privacy, people change either their privacy context or their level of self-disclosure.

The model's distinction between the four dimensions of privacy (Burgoon, 1982) is also useful. It is often claimed that privacy is over in the era of the Internet (Heller, 2011; Jarvis, 2011). With the more specified model of the PPM, however, it becomes apparent that even though the informational privacy is reduced online (Trepte & Reinecke, 2011b), this does not transfer to aspects of social, psychological, and physical privacy. Here, users can decide with whom they want to share information and how intimate this information is. Besides, in Trepte's and Reinecke's book *Privacy Online*, none of the thirty-one researchers claim that the time of privacy is over (Trepte & Reinecke, 2011a). Finally, the PPM is not limited to online contexts. Every context can be assessed by the PPM in terms of the four dimensions of informational, social, psychological, and physical privacy. Thus, privacy behaviors relating to situations such as business meetings can be regarded as well as mechanisms taking place when users leave a post on their Facebook wall. Consequently, there is no need to refer to different models when trying to understand, replicate, or predict privacy related behaviors.

2.5.2 Limitations

The PPM results from analyzes of extant literature and new empirical findings — at this point, the model has not been validated empirically. Hence, the PPM is still a hypothesized model that needs to be examined in further empirical studies. The PPM builds upon a selection of theories and definitions of privacy. Other elaborate definitions — for example the communication privacy management theory by Petronio (2002) or the privacy in context approach by Nissenbaum (2010) — are not addressed explicitly here and encompass potential additional insights. Moreover, the four privacy dimensions need to be validated. Based on a theoretical analysis by Burgoon in 1982, their empirical foundation seems moderate. The first study trying to reproduce the four factor structure was unable to perfectly reproduce the four dimensions (Ruddigkeit, Penzel, & Schneider, 2013). Other variables such as cross-contextual consistency, familiarity of context members, or context replicability might be worth integrating. Regarding the privacy perception, it seems possible that people assess their own privacy according to a much more basic and simple heuristic. Thus, further empirical research needs to be conducted in order to establish what dimensions have to be included.

Finally, the aim of the PPM is not to explain self-disclosure behaviors as comprehensively as possible. If it was, variables such as the need to belong, impression managament, anticipated self-disclosure gratifications, or extraversion would have to be included (see, e.g., Christofides, Muise, & Desmarais, 2009; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010).

2.5.3 Conclusion

The phenomenon of privacy cannot be regarded in a simplistic, uni-dimensional way. Because of the thorough changes induced by the rise of the Internet, it becomes all the more important to understand the dynamics inherent to privacy. The privacy process model has been designed to capture the core variables and mechanisms of privacy in a model applicable to both offline and online contexts. With its reference to established definitions of privacy and the inclusion of current empirical studies, the PPM offers a comprehensive overview of the most pivotal aspects pertaining to privacy.

Literature

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from www.firstmonday.org/issues/issue11_9/barnes/index.html

boyd, d. m. (2008a). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13–20. doi:10.1177/1354856507084416

boyd, d. m. (2008b). *Taken out of context. American teen sociality in networked publics: Doctoral dissertation*. Berkeley, CA: University of California.

Burgoon, M. (Ed.). (1982). *Communication yearbook 6*. Beverly Hills, CA: Routledge.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*(3), 341–345. doi:10.1089/cpb.2008.0226

Derlega, V. J. & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, *33*(3), 102–115. doi:10.1111/j.1540-4560.1977.tb01885.x

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*(3), 421–471.

Haber, M. G., Cohen, J. L., Lucas, T., & Baltes, B. B. (2007). The relationship between self-reported received and perceived social support: A meta-analytic review. *American Journal of Community Psychology*, *39*(1-2), 133–144. doi:10.1007/s10464-007-9100-9

Hall, E. T. (1990). *The hidden dimension*. New York, NY: Anchor Books.

Heller, C. (2011). *Post Privacy: Prima leben ohne Privatsphäre*. Munich, Germany: Beck.

Hempel, L. & Töpfer, E. (2004). On the threshold to urban panopticon? Analysing the employment of CCTV in european cities and assessing its social and political impacts - final report to the European Union. Berlin.

Jarvis, J. (2011). *Public parts: How sharing in the digital age improves the way we work and live*. New York, NY: Simon & Schuster.

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

Lindner, R. (2013). Datenschutz: Umstrittene Privatsphäre à la Facebook - Unternehmen - FAZ. Frankfurt a.M. Retrieved from www.faz.net/aktuell/wirtschaft/unternehmen/datenschutz-umstrittene-privatsphaere-a-la-facebook-1983538.html

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

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 9–17). Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6{_}2

Metzger, M. J., Wilson, C., Pure, R. A., & Zhao, B. Y. (2012). Invisible interactions: What latent social interaction can tell us about social relationships in social networking sites: Paper presented at the Annual Meeting of the International Communication Association. Phoenix, AZ. Retrieved from www.cs.ucsb.edu/~ravenben/publications/pdf/interactions-ica12.pdf

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Norris, C. & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Oxford, UK: Berg.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Ruddigkeit, A., Penzel, J., & Schneider, J. (2013). Dinge, die meine Eltern nicht sehen sollten. *Publizistik*, *58*(3), 305–325. doi:10.1007/s11616-013-0183-z

Taddicken, M. (2011). Selbstoffenbarung im Social Web. *Publizistik*, *56*(3), 281–303. doi:10.1007/s11616-011-0123-8

Trepte, S. (2012). Privatsphäre aus psychologischer Sicht. In J.-H. Schmidt (Ed.), *Datenschutz* (Vol. 1190, pp. 59–66). Schriftenreihe Bundeszentrale für Politische Bildung. Bonn, Germany: Bundeszentrale für politische Bildung.

Trepte, S., Dienlin, T., & Reinecke, L. (2013). Privacy, self-disclosure, social support, and social network site use. Research report of a three-year panel study. Retrieved from University of Hohenheim website: http://opus.uni-hohenheim.de/volltexte/2013/889/.

Trepte, S., Dienlin, T., & Reinecke, L. (2014a). Influence of social support received in online and offline contexts on satisfaction with social support and satisfaction with life: A longitudinal study. *Media Psychology*, *18*(1), 74–105. doi:10.1080/15213269.2013.838904

Trepte, S., Dienlin, T., & Reinecke, L. (2014b). Risky behaviors. How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis* (Vol. 41, pp. 225–244). Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft. Konstanz, Germany: UVK.

Trepte, S. & Reinecke, L. (Eds.). (2011a). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6{_}6

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

Trepte, S. & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior*, *29*(3), 1102–1112. doi:10.1016/j.chb.2012.10.002

Vinsel, A., Brown, B. B., Altman, I., & Foss, C. (1980). Privacy regulation, territorial displays, and effectiveness of individual functioning. *Journal of Personality and Social Psychology*, *39*(6), 1104–1115. doi:10.1037/h0077718

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

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Wheeless, L. R. (1976). Self-disclosure and interpersonal solidarity: Measurement, validation, and relationships. *Human Communication Research*, *3*(1), 47–61. doi:10.1111/j.1468-2958.1976.tb00503.x

Study 2

3 Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors

Preamble

Abstract

The privacy paradox states that online privacy concerns do not sufficiently explain online privacy behaviors on Social Network Sites (SNSs). In this study, it was first asked whether the privacy paradox would still exist when analyzed as in prior research. Second, it was hypothesized that the privacy paradox would disappear when analyzed in a new approach. The new approach featured a multidimensional operationalization of privacy by differentiating between informational, social, and psychological privacy. Next to privacy concerns, also privacy attitudes and privacy intentions were analyzed. With the aim to improve methodological aspects, all items were designed based on the theory of planned behavior (TPB). In an online questionnaire with $N = 595$ respondents, it was found that online privacy concerns were not significantly related to specific privacy behaviors, such as the frequency or content of disclosures on SNSs (e.g., name, cell-phone number, or religious views). This demonstrated that the privacy paradox still exists when it is operationalized as in prior research. With regard to the new approach, all hypotheses were confirmed: Results showed both a direct and an indirect relation between privacy attitudes and privacy behaviors, the latter mediated by privacy intentions. In addition, also an indirect relation between privacy concerns and privacy behaviors was found, mediated by privacy attitudes and privacy intentions. Therefore, privacy behaviors can be explained sufficiently when using both privacy attitudes and privacy concerns within the TPB. The behaviors of users on SNSs are not as paradoxical as was once believed.

Keywords: privacy paradox, privacy, theory of planned behavior, social network site, SNS, Facebook, privacy concerns, attitudes, intentions, behaviors, structural equation modeling

Status of publication

The following study has already been published. Please cite as follows: Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. doi:10.1002he/sheejsp.2049.

The content of the text has not been altered. For reasons of consistency, some minor changes in formatting have been carried out.

3.1 Introduction

Many social network site (SNS) users have pronounced privacy concerns and are afraid that their privacy might be violated online (European Commission, 2011; Hoy & Milne, 2010; Yao, Rice, & Wallis, 2007). However, these concerns and fears rarely impact actual SNS use (Gross & Acquisti, 2005; Nosko, Wood, & Molema, 2010). In prior research, this phenomenon of contradicting privacy attitudes and behaviors was referred to as the privacy paradox (Barnes, 2006). Now, several years after its detection in 2006, it seems fruitful to ask: Does the privacy paradox still exist?

This study has three aims: First, to replicate prior research — to see if the privacy paradox still occurs. Second, to develop a new and optimized approach that reflects the widely shared understanding of privacy as a multi-dimensional construct. Third, to find a way to connect both privacy attitudes and privacy behaviors with privacy concerns — to determine if privacy concerns are relevant or not.

3.2 Theory

3.2.1 The privacy paradox

The privacy paradox was first mentioned in an essay by Barnes (2006): "Herein lies the privacy paradox. Adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the Internet" (para. 15). More specifically, Barnes observed four controversial phenomena of SNS use: (a) the large quantity of information disclosed online, (b) the illusion of privacy on SNSs, (c) the discrepancy between context and behavior (indicating that even when people realize that SNSs are a public realm they still behave as if it was a private place), and (d) the users' poor understanding of data processing actions by online enterprises (Barnes, 2006). The privacy paradox was debated in many disciplines (Trepte & Reinecke, 2011a) and has been investigated in a number of studies (Trepte, Dienlin, & Reinecke, 2014; Utz & Kramer, 2009). It can be defined as follows: People's concerns toward privacy are unrelated to the privacy behaviors. Even when users have substantial concerns with regard to their online privacy (European Commission, 2011) they engage in self-disclosing behaviors that do not adequately reflect their concerns.

Since that time, several studies have investigated the privacy paradox also empirically. A considerable number of studies have found support for the privacy paradox (e.g., Acquisti & Gross, 2006; Ellison, Lampe, & Vitak, 2011; Gross & Acquisti, 2005; Nosko et al., 2012; Stutzman & Kramer-Duffield, 2010; Taddei & Contena, 2013; Tufekci, 2008). For example, Tufekci (2008) demonstrated that "Findings show little to no relationship between online privacy concerns and information disclosure on online social network sites" (p. 20). Tufekci reported that privacy concerns did not relate to the disclosure of the users' authentic names, their political / religious views, and addresses. Similarly, Acquisti and Gross (2006) showed that there was no relation between privacy concerns and posting of cell-phone number on SNSs. Also, Taddei and Contena (2013) found that privacy concerns did not correspond to the posting behavior on Facebook.

However, results on the privacy paradox are manifold and some studies did not support the privacy paradox (Debatin, Lovejoy, Horn, & Hughes, 2009; Joinson, Reips, Buchanan, & Schofield, 2010; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010; Mohamed & Ahmad, 2012; Stutzman, Vitak, Ellison, Gray, & Lampe, 2012). Krasnova et al. (2010) found that the perceived privacy risk — a construct that closely resembles privacy concerns — was associated significantly with the respondents' amount of self-disclosure on SNSs. Mohamed and Ahmad (2012) came to the conclusion that "Information privacy concerns explain privacy measure use in social networking sites" (p. 2366). The study of Trepte et al. (2014) on negative online experiences found that even when users were insulted online they changed only their informational but not their social or psychological privacy behavior. The empirical findings of the privacy paradox thus can be considered inconsistent in nature. As a consequence, it seems important to first replicate previous research.

Research question: Will privacy concerns be related to specific online privacy behaviors such as the indication of (a) the authentic first name, (b) the authentic last name, (c) the personal address, (d) the cell-phone number, (e) political or religious views, and (f) the frequency of posts on SNSs?

3.2.2 The privacy paradox explicated

In the following, we explicate the privacy paradox in more detail. First, we start with the definitions of privacy behaviors and privacy concerns. Afterward, we aim to unveil the privacy paradox by elaborating on the relation between privacy concerns and privacy behaviors. As a final point, we suggest a new approach to analyze the privacy paradox.

Privacy behaviors and privacy concerns

Behaviors are usually referred to as any observable actions that are taken by individuals. Privacy behaviors are generally referred to as any behaviors that are intended to optimize the relationship with others by either limiting self-disclosure or by withdrawing from interactions with others (e.g., Altman, 1975; Burgoon, 1982; Dienlin, 2014; Petronio, 2002; Warren & Brandeis, 1890; Westin, 1967). Burgoon (1982), for example, defines privacy based on the following four dimensions: Informational privacy, which captures the individual control over the processing and transferring of personal information. Social privacy, which captures the dialectic process of regulating proximity and distance toward others (Burgoon, 1982). Psychological privacy, which captures the perceived control over emotional and cognitive inputs and outputs. Physical privacy, which captures the personal freedom from surveillance and unwanted intrusions upon one's territorial space.

Privacy concerns have been described as "the desire to keep personal information out of the hands of others" (Buchanan, Paine, Joinson, & Reips, 2007, p. 158). Privacy concerns capture the negatively valenced emotional attitude that people feel when personal rights, information, or behaviors are being regressed by others. Privacy concerns can be related to the concept of attitudes. An attitude is "an evaluative integration of cognitions and affects experienced in relation to an object" (Crano & Prislin, 2006, p. 347). Attitudes are studied on two dimensions: instrumental (cognitive) attitudes and experiential (affective) attitudes (Courneya & Bobick, 2000). Generally, attitudes can be both positive and negative. Privacy attitudes and privacy concerns have two major differences with regard to polarity and scope: Concerning polarity, privacy concerns are unipolar, whereas privacy attitudes are bipolar. Privacy concerns measure, for example, if people are afraid that their bank account would be compromised — which can be only a negative feeling. Privacy attitudes measure if, for example, people think that it is either advantageous or disadvantageous to use online banking — which can either be a positive or a negative feeling. Concerning scope, the potential application area of privacy attitudes is larger. Privacy attitudes can be specified for every single online privacy action, such as having a Facebook account, indicating one's authentic name, or posting family pictures. Privacy concerns, by contrast, refer to online phenomena that are considered only negative: For example, online identity theft, misuse of personal data, or willful deception in communication processes.

Unveiling the privacy paradox

To answer the question of why users engage in paradoxical behavior we suggest three approaches that are interconnected with each other. First, we reconsider the definitions of privacy concerns and privacy behaviors. Second, we refer to socio-psychological research and to the general finding of the attitude-behavior gap (Fazio & Roskos-Ewoldsen, 1994; LaPiere, 1934). Third, we critically ask how well previous methodological operationalizations are able to reflect the influence of users' privacy attitudes on behaviors.

With regard to the definition of privacy behaviors, we suggest the following: Burgoon's approach toward privacy was largely acknowledged in the field of online privacy research (Peter & Valkenburg, 2011; Trepte & Reinecke, 2011a). However, so far only Ruddigkeit, Penzel, and Schneider (2013) used Burgoon's approach in an empirical work. In the majority of studies, a multitude of singular behaviors were used that did not consider the multidimensional nature of privacy (Acquisti & Gross, 2006; Ellison et al., 2011; Gross & Acquisti, 2005; Nosko et al., 2012; Stutzman & Kramer-Duffield, 2010; Taddei & Contena, 2013; Tufekci, 2008). We suggest that a multidimensional approach toward privacy by referring to Burgoon's (1982) definition seems worthwhile. With regard to the definition of privacy concerns, we suggest that it is important to also empirically distinguish between privacy concerns on the one hand and privacy attitudes on the other hand. From a methodological viewpoint, the aforementioned considerations imply a limitation of variance when looking at privacy concerns only. Generally, a limitation of variance decreases the likelihood to detect significant relations (Schmidt, Hunter, & Urry, 1976). This might partly explain why, so far, it has not been possible to find significant correlations between privacy behaviors and privacy concerns. Integrating privacy attitudes might account for more variance and thus statistical power. We therefore suggest that it is important to consider both privacy concerns and privacy attitudes when analyzing the privacy paradox.

A second answer to the question of why users engage in paradoxical behavior might be found in socio-psychological research, which has identified the attitude-behavior gap (Fazio & Roskos-Ewoldsen, 1994; LaPiere, 1934). The attitude-behavior gap indicates that attitudes and behaviors are oftentimes unrelated (Kaiser, Byrka, & Hartig, 2010). A number of boundary conditions have been proposed with regard to why and when this gap occurs (Trepte et al., 2014). The first condition addresses the situations in which respondents are asked to express their attitudes (Fazio & Roskos-Ewoldsen, 1994). It has been shown that subjective norms, peer pressure, and situational constraints can have a substantial influence on respondent answering behavior. Respondents might withhold their true opinions or even provide false answers if they perceive strong situational constraints and norms forcing them to do so. Especially with regard to online privacy, users might be aware of contemporary reports in the mass media that often focus on prevailing privacy risks (Teutsch & Niemann, 26.05.2014). As a consequence, respondents' answers might largely reflect the public's opinion rather than their own. Another boundary condition states that the strength of the association between attitudes and behaviors largely depends on the strength of the attitude. When attitudes are pronounced or extreme, they are more likely to determine behavior (Kaiser et al., 2010; Petty & Krosnick, 1995). The last condition addresses personal experiences, which determine whether attitudes allow for adequately predicting behaviors. The societal threat posed by online privacy intrusions remains rather obscure, because only a few users have actually experienced privacy violations (European Commission, 2012; Trepte, Dienlin, & Reinecke, 2013). Thus, it seems that privacy attitudes are largely built on heuristics and secondhand experiences. However, firsthand personal experiences are important when it comes to building sustainable attitudes (Tormala, Petty, & Brinol, 2002). A lack of personal experiences with online privacy issues might have the effect that respondents are authentic when indicating that they are afraid of privacy violations; at the same time, this aspect is not relevant and consolidated enough to influence subsequent behavior significantly. In sum, social-psychological research suggests taking into consideration the situational constraints, the prevailing peer pressure, and to refer to both personal experiences and attitude strength when operationalizing privacy attitudes.

A third reason why users may seem to engage in paradoxical behavior comes from a methodological viewpoint. Presumably, privacy behaviors and attitudes have not significantly been related in previous research, because of the ways that they were operationalized. For example, Lewis (2011) operationalized privacy behaviors by asking respondents if they had an open or a public profile, which is a dichotomous measure. Similarly, Acquisti and Gross (2006) asked if their respondents had a Facebook account or not. These measures were then related to metric scales of privacy attitudes. The dichotomy of the dependent variables again implies a possible limitation of variance (Schmidt et al., 1976), which might lead to lower statistical power. In conclusion, methodological considerations suggest operationalizing both privacy attitudes and privacy behaviors on at least ordinal scales.

A new approach toward the privacy paradox

To carefully consider and combine the aforementioned points in a new approach, it seems important to adopt a theory based approach that is explicitly configured to explain privacy behaviors by privacy attitudes. For this study, we use the theory of planned behavior (TPB; Ajzen, 1985; Fishbein & Ajzen, 2010) due to four reasons: First, the TPB's variables are conceptualized according to the principle of compatibility (Fishbein & Ajzen, 2010). Questions operationalizing attitudes and behaviors comply in terms of action, target, context, and time (Fishbein & Ajzen, 2010). Broad and abstract attitudes such as privacy concerns are less likely to predict narrow behaviors such as the use of public versus private profile on SNSs. Questions that share the same content as the behavior — for example attitudes regarding the use of friend lists on Facebook as a predictor for the factual use of friend lists — are more likely to reflect the reality of users. Second, in the TPB specific behaviors (e.g., "How often do you go running?") as well as categorical behaviors (e.g., "How often do you exercise?") can be analyzed (Fishbein & Ajzen, 2010). Third, the TPB introduces a third variable to bridge the attitude behavior gap, the behavioral intention. For example, some smokers have the attitude that smoking is bad, nonetheless they continue to smoke. This discrepancy can be explained partly by means of the intention: Although some smokers disapprove of smoking, they simply do not want to stop — because, for example, they think that they are not capable of doing so. Fourth, the TPB was already successfully used to predict diverse behaviors, including physical activities (Hagger, Chatzisarantis, & Biddle, 2002) or sexual intercourse (Terry, Gallois, & McCamish, 1993). For online contexts, Yao (2011) advised an application of the TPB and Burns and Roberts (2013) used the TPB in a more general study on online privacy behaviors.

Taking into account the findings from the groundwork of psychological research on privacy, it seems important to furthermore consider the different dimensions of privacy (informational, social, psychological, and physical) as suggested by Burgoon (1982). Because physical privacy is not particularly relevant for online contexts and also problematic to operationalize,[1] it is not addressed in this study. Also, privacy attitudes and privacy concerns are distinguished; privacy attitudes are used as main predictor for privacy behaviors. The theory of planned behavior is thus applied three times: for linking informational privacy attitudes with informational privacy behaviors, for linking social privacy attitudes with social privacy behaviors, and for linking psychological privacy attitudes with psychological privacy behaviors.

[1] Trepte and Reinecke (2011b) as well as Krämer and Haferkamp (2011) stated that transferring physical privacy to SNSs does not seem to be feasible; Ruddigkeit et al. (2013) also reported difficulties in their empirical attempt to measure physical privacy with regard to digital behaviors. As SNSs deal with the digital representations of people, no physical points of contact are possible.

In conclusion, in Hypothesis 1 it is assumed that privacy attitudes and privacy behaviors are related with each other based on an application of the TPB and a multidimensional understanding of privacy attitudes and behaviors.

> *Hypothesis 1*: (a) Informational, (b) social, and (c) psychological privacy attitudes will be related significantly to (a) informational, (b) social, and (c) psychological privacy behaviors.

As advanced before, the TPB also integrates the behavioral intentions as a mediator between attitudes and behaviors. It has been demonstrated previously that attitudes do not always influence behaviors directly (Fazio & Roskos-Ewoldsen, 1994). Although people might hold a positive attitude, they do not necessarily express this attitude in overt behaviors. The TPB emphasizes that peoples' behavioral intentions are not only determined by their attitudes, but also by their subjective norms or their perceived control over changing a behavior (Ajzen, 1991). For aspects of online privacy, looking at behavioral intentions for linking privacy attitudes with privacy behaviors seems fruitful also. Some users might be of the opinion that it is advantageous to use a nickname on Facebook; however, it could well be that all of their friends use their authentic names, which might refrain them from choosing a nickname (subjective norms; c.f., Lewis, 2011). Furthermore, some users might want to employ a friend list on Facebook to restrict access to their profile, but at the same time cannot handle the complex technical infrastructure of Facebook (perceived control). As a result, in Hypothesis 2 the privacy paradox is addressed accordingly: Intentions are used as a mediator between privacy attitudes and privacy behaviors, because they include additional information referring to subjective norms and the perceived behavioral control.

> *Hypothesis 2*: (a) Informational, (b) social, and (c) psychological privacy attitudes positively influence (a) informational, (b) social, and (c) psychological privacy intentions, which in turn positively influence (a) informational, (b) social, and (c) psychological privacy behaviors.

The question remains: What is the relation between privacy behaviors and privacy concerns? As shown above, privacy concerns differ from privacy attitudes in terms of polarity and scope. Both capture people's opinions toward various aspects in online contexts, but privacy concerns tend to be less specific. For example, one item of the scale used by Buchanan et al. (2007) is: "How concerned are you about your privacy online?" By contrast, privacy attitudes are more specific. For example, one item could be: "I think that communicating personal information on Facebook is disadvantageous / advantageous." Prior research has shown that privacy concerns do not determine privacy behaviors (Acquisti & Gross, 2006; Tufekci, 2008). However, it can be suggested that privacy concerns might determine privacy attitudes: The general skepticism people have toward actions on the Internet presumably influences their more differentiated attitudes toward diverse privacy behaviors. Although there is not a direct relation of privacy concerns with privacy behaviors, there might be an indirect one. As final assumption, in Hypothesis 3 we thus suggest that privacy concerns first influence privacy attitudes, which then affect privacy behaviors both directly (Hypothesis 1) and indirectly (Hypothesis 2).

> *Hypothesis 3*: Privacy concerns will positively influence (a) informational, (b) social, and (c) psychological privacy attitudes, which will in turn positively influence (a) informational, (b) social, and (c) psychological privacy intentions and (a) informational, (b) social, and (c) psychological privacy behaviors.

3.3 Methods

3.3.1 Procedure and participants

The study was designed as an online questionnaire with the online tool Sosci Scientific Survey (Leiner, 2014). Participants were recruited from the Socio-Scientific Panel (soscisurvey, 2014). At the time of the study, the panel consisted of 97,199 persons. The panel is noncommercial and based on voluntary participation. Each year, panel members receive on average three e-mails with invitations to take part in selected studies. In order for a study to be picked for the panel, a formal application and review process takes place. The soscisurvey panel is used regularly for both German and international studies. For example, Gottschalk and Kirn (2013) used the panel in a study on analyzing cloud computing by means of the theory of reasoned action (Fishbein & Ajzen, 1975). For further information about the Socio Scientific Panel itself see, for example, Leiner (2012, March) or soscisurvey (2014).

5000 invitation e-mails were sent to members of the panel. The contact rate was 98.2%; 88 e-mails could not be delivered successfully. The cooperation rate was 16.3%; 800 people started filling out the questionnaire. The completion rate was 74.5%; 595 respondents finished the questionnaire. Overall, the response rate was 11.9%. The panel's average cooperation rate is 17% (soscisurvey, 2014), the response rate of a similar survey 8–10% (Pew Research Center, 2014). Considering the panel objectives and comparable studies, the response rate can be considered satisfactory. The data for this study consists of $N = 595$ respondents who finished the questionnaire (66.67% women, 33.33% men, $\text{M}_{\text{age}} = 29.75$ years, age range: 15–78 years, $SD = 10.43$ years). The sample is a convenience sample, as participation was on a voluntary basis.

3.3.2 Measures

The guidelines of Fishbein and Ajzen (2010) were used for designing the TPB items. Categorical behaviors were conceptualized according to the principle of compatibility (Fishbein & Ajzen, 2010). For example, the item measuring informational privacy behavior was: "How much identifying information (content) have you now (time) posted (action) on Facebook (context)?" All items were designed and presented in German. The items that were used for this study can be found translated into English in Table 3.1. Back and forward translation was done in order to guarantee translation accuracy. For each variable's mean, standard deviation, internal consistency, range, and skewness see Table 3.2.

Privacy behaviors

Informational privacy behaviors measured how many identifying pieces of information people shared on their Facebook profile. Participants answered three items on 7-point Likert scales, ranging from (for example) 1 = *none* to 7 = *very much*. The scale was recoded for analyses with lower values expressing lesser extent as opposed to higher values expressing a higher extent

Table 3.1: Item pool used for H1, H2, and H3

	Informational Privacy	Social Privacy	Psychological Privacy
Behaviors	How much identifying information have you now posted on FB?	Do you right now restrict access to your FB profile?	How many personal things do you communicate on FB?
	How much identifying information can generally be found on your FB profile?	How strongly is the visibility of content on your FB profile restricted?	How exactly is your personality resembled by your FB profile?
	How precisely can you be identified on FB by strangers?	How strongly is your FB profile restricted regarding the accessibility for particular persons?	How personal is your FB profile?
Intentions	How much identifying information do you currently want to provide on FB?	How strongly do you want to restrict your FB profile right now?	How much personal information do you want to communicate on FB?
	How much identifying information about yourself do you generally want to have on your FB profile?	How strongly do you want that the visibility of content on your FB profile is restricted?	How exactly do you want your FB profile to resemble your entire personality?
	How precisely do you want to be identifiable for strangers on FB?	How strongly restricted do you want your FB profile to be for certain persons?	How personal do you want your FB profile to be?
Attitudes	I think that giving information on FB that identifies me is:	I think that restricting access to one's FB profile is:	I think that communicating personal information on FB is:
	1. not useful - very useful	1. not useful - very useful	1. not useful - very useful
	2. disadvantageous - advantageous	2. disadvantageous - advantageous	2. disadvantageous - advantageous
	3. worrying - not worrying	3. worrying - not worrying	3. worrying - not worrying
	4. very dangerous - not dangerous	4. unpleasant - not unpleasant	4. very dangerous - not dangerous
	5. careless - not careless	5. very mean - very fair	5. not pleasant - very pleasant
	6. very bad - very good	6. very bad - very good	6. very bad - very good
Concerns	1. In general, how concerned are you about your privacy while you are using the Internet?		
	Are you concerned		
	2. about online organizations not being who they claim they are?		
	3. that you are asked for too much personal information when you register or make online purchases?		
	4. about online identity theft?		
	5. about people online not being who they say they are?		
	6. that information about you could be found on an old computer?		
	7. about people you do not know obtaining personal inform. about you from your online activities?		
	8. that a message you send online may be read by someone else besides the person you sent it to?		
	9. that a message you send someone online may be inappropriately forwarded to others?		
	10. about messages you receive online not being from whom they say they are?		

Table 3.2: Psychometric Properties of the Study Variables

				Range		
Variable	*M*	*SD*	α	Potential	Actual	Skew
Privacy behaviors (specific)						
Indication of						
First name	85%	36%		0 - 1	0 - 1	-1.43
Last name	72%	45%		0 - 1	0 - 1	-0.96
Address	6%	24%		0 - 1	0 - 1	3.49
Phone number	3%	16%		0 - 1	0 - 1	5.84
Religious / political views	39%	49%		0 - 1	0 - 1	0.42
Frequency of posts	4.98	1.35		1 - 7	1 - 7	-0.56
Privacy behaviors (categorical)						
Informational	4.83	1.33	0.77	1 - 7	1.0 - 7.0	-0.51
Social	5.28	1.48	0.85	1 - 7	1.0 - 7.0	-1.07
Psychological	4.96	1.28	0.82	1 - 7	1.0 - 7.0	-0.45
Privacy intentions						
Informational	5.42	1.21	0.81	1 - 7	1.3 - 7.0	-0.70
Social	5.50	1.26	0.78	1 - 7	1.0 - 7.0	-1.02
Psychological	4.98	1.36	0.85	1 - 7	1.0 - 7.0	-0.50
Privacy attitudes						
Informational	4.50	1.10	0.87	1 - 7	1.0 - 7.0	0.11
Social	5.85	0.93	0.81	1 - 7	2.5 - 7.0	-0.58
Psychological	4.72	1.11	0.89	1 - 7	1.3 - 7.0	0.22
Privacy concerns	3.22	0.76	0.84	1 - 5	1.2 - 5.0	-0.11

of privacy behavior. Social privacy behaviors captured whether people restricted access to their Facebook profile. Participants answered three items on 7-point Likert scales, ranging from (for example) 1 = *not at all* to 7 = *very much*. No recoding was applied. Psychological privacy captured the degree to which people had an intimate and personal Facebook profile. Participants answered three items on 7-point Likert scales, ranging from (for example) 1 = *very impersonal* to 7 = *very personal*. For psychological privacy, the scale was recoded with lower scale values expressing a lower and higher values expressing a higher level of psychological privacy.

Privacy intentions

Adhering to the principle of compatibility (Fishbein & Ajzen, 2010), three corresponding privacy intention items were modeled that paralleled items for privacy behavior in terms of action, target, context, and time. Three informational privacy intention items measured how many identifying pieces of information people currently wanted to share on their Facebook profile. Three social privacy intention items comprised how strongly people wanted to restrict access to their Facebook profile. Three psychological privacy intention items encompassed the degree to which people wanted to have an intimate and personal Facebook profile.

Privacy attitudes

Privacy attitudes were operationalized by items that measured the general appraisal of each particular privacy behavior (Fishbein & Ajzen, 2010). Informational privacy attitudes measured respondents' appraisal of posting identifying information on Facebook. For each dimension, items consisted of an introduction, which was followed by six different semantic differentials. Semantic differentials work both for uni-dimensional (*dangerous* versus *not dangerous*) and for bidimensional (*bad* versus *good*) pairs (Fishbein & Ajzen, 2010). For the informational privacy attitude, the introduction was "I think that providing information on FB that identifies me is: . . . " The following semantic differentials were answered on a 7-point scale and ranged, for example, from 1 = *useful* to 7 = *not useful*. Social privacy attitude comprised respondents' appraisal of restricting access to a Facebook profile. The introduction was "I think that restricting access to one's FB profile is: . . . " The semantic differentials were answered on a 7-point scale ranging from, for example, 1 = *very mean* to 7 = *very fair*. Psychological privacy attitude captured respondents' appraisal of sharing personal pieces of information on Facebook. The introduction was "I think that communicating personal information on FB is: . . . " Again, respondents indicated their answers on a 7-point semantic differential, ranging from, for example, 1 = *very dangerous* to 7 = *not dangerous*.

Online privacy concerns

Online privacy concerns measure the degree to which people are worried regarding their online privacy. 10 items from the 18-item scale by Buchanan et al. (2007) were used (see Table 3.1). For reasons of parsimony only 10 items that fit the study's needs best were chosen. One example item was "Are you concerned about people online not being who they say they are?" Respondents answered all items on a 5-point Likert Scale, ranging from 1 = *not at all* to 5 = *very strongly*.

Specific privacy behaviors

In order to answer the research questions, respondents were asked several questions that captured specific privacy behaviors. Items were chosen with the aim to replicate those studies that found evidence in favor of the privacy paradox. Thus, all items resembled the ones used by Tufekci (2008), Acquisti and Gross (2006), and Taddei and Contena (2013). For all items, possible answers were 0 = *no*, 1 = *yes*. Respondents were asked the following questions: (a) "On Facebook, I use my authentic first name (that is, the exact way it is written in my passport)." (b) "On Facebook, I use my authentic second name (that is, the exact way it is written in my passport)." (c) "On Facebook, I indicate my current address." (d) "On Facebook, I indicate my telephone number." (e) "On Facebook, have you ever posted a religious, political, or ethical statement?" (f) "How often do you leave a post on Facebook?" This time, possible answers were 1 = *never*, 2 = *every other month*, 3 = *on a monthly basis*, 4 = *several times a month*, 5 = *several times a week*, 6 = *once a day*, 7 = *several times a day*.

3.3.3 Data analysis

The results of Cronbach's Alpha tests showed that all variables had at least satisfactory internal consistencies (Table 3.2). All variables were tested for normal distribution with Kolmogorov-Smirnov tests. With large sample sizes, Kolmogorov-Smirnov tests overestimate significant differences from the normal distribution (Field, 2009). Hence, random subsamples of $n = 30$ were drawn. The tests did not produce significant results, thus the results did not imply that the data were not distributed normally.

One of the aims of the study was to replicate already existing research. In those studies, regression analyses were used (e.g., Utz & Kramer, 2009). As a result, RQ1 was answered via bivariate regressions. The hypotheses were analyzed with structural equation models (SEMs). H1, H2, and H3 were analyzed together in one single SEM. As the hypotheses were tested along three dimensions — informational, social, and psychological privacy — , three different SEMs were computed: In SEM_{INF}, H1, H2, and H3 were tested for the dimension of informational privacy; in SEM_{SOC}, H1, H2, and H3 were tested for the dimension of social privacy; in the SEM_{PSY}, H1, H2, and H3 were tested for the dimension of psychological privacy. The structure of the SEMs was configured a priori. For the design of the SEMs, see Figure 3.1.

Missing values were considered missing at random and were replaced with the full information maximum likelihood Arbuckle (1996). To estimate effect sizes, the correlation coefficient r was used as suggested by Field (2009). Values exceeding $r = .10$ were considered small effects, $r = .30$ medium effects, and $r = .50$ large effects. For structural equation modeling, beta-coefficients can be interpreted as r-values (e.g., Durlak, 2009). Hypotheses were tested with a two-tailed .05 level of significance. The data were analyzed with the Software R, version 3.0.1 (R Core Team, 2016). To conduct the SEMs, the package lavaan, version 0.5–14 (2012) was used (Rosseel, 2012). Furthermore, the packages QuantPsyc, moments, boot, psych, and memisc were used.

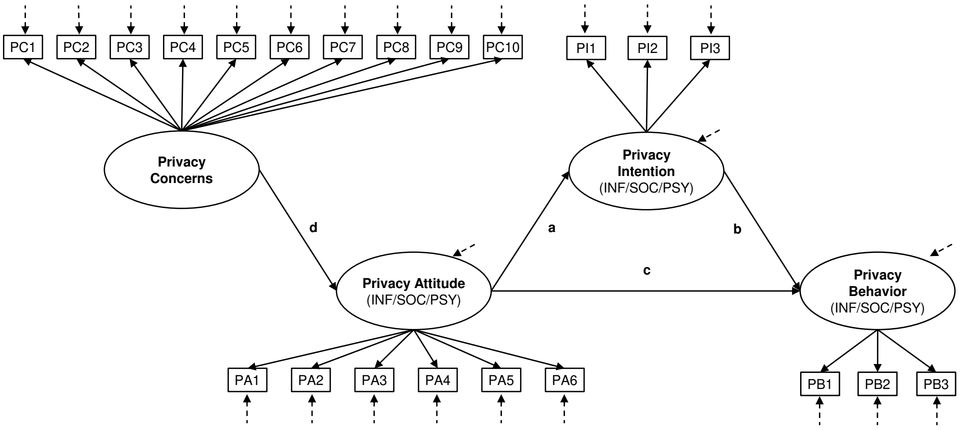
PC1
PC2
PC3
PC4
PC5
PC6
PC7
PC8
PC9
PC10
PI1
PI2
PI3
Privacy Concerns
Privacy Intention (INF/SOC/PSY)
d
a
b
c
Privacy Attitude (INF/SOC/PSY)
Privacy Behavior (INF/SOC/PSY)
PA1
PA2
PA3
PA4
PA5
PA6
PB1
PB2
PB3

Figure 3.1: SEMs with the direct and indirect influences of privacy attitudes and privacy concerns on privacy behaviors. Latent variables are represented by ovals, and observed variables by rectangles. Dashed arrows represent error terms / residuals. The model was designed for informational privacy (SEM_{INF}), social privacy (SEM_{SOC}), and psychological privacy (SEM_{PSY})

3.4 Results

3.4.1 Research questions: Replicating previous research on the privacy paradox

RQ1 asked if privacy concerns were related to specific privacy behaviors, such as the indication of (a) the authentic first name, (b) the authentic second name, (c) the personal address, (d) the cell-phone number, (e) political or religious views, and (f) the frequency of posts on SNSs. The results indicated the following:

- RQ1a: Regression analyses showed privacy concerns to be unrelated to the online disclosure of the authentic first name ($F(1, 586) = 0.51$, $p = .478$, $b < -0.01$, $\beta = -.03$).
- RQ1b: Privacy concerns were again unrelated to the online disclosure of the authentic second name ($F(1, 586) = 3.00$, $p = .084$, $b < -0.01$, $\beta = -.07$).

- RQ1c: Here, privacy concerns were related to the online disclosure of the personal address (F(1, 586) = 9.40, p = .002, b = -0.03, β = -.13). This implies that people who are more concerned about their privacy are less likely to disclose their personal address online. The size of the effect of privacy concerns on the online disclosure of the personal address was small.
- RQ1d: Privacy concerns were unrelated to the disclosure of the cell-phone number (F(1, 582) = 0.35, p = .552, b < -0.01, β = -.02).
- RQ1e: Privacy concerns were not associated with postings of political or religious views on Facebook (F(1, 585) = 2.32, p = .128, b < -0.01, β = -.063).
- RQ1f: Privacy concerns were not related to the frequency of posts on SNSs (F(1, 585) = 2.25, p = .134, b < 0.01, β = .06).

In sum, with the exception of the minor correlation with address disclosure, the results are consistent with previous research. The results indicate that online privacy concerns remain unrelated to specific privacy behaviors such as the frequency and contents of online disclosures.

3.4.2 Hypotheses: A multidimensional perspective on the privacy paradox

Model fit

H1, H2, and H3 were tested for the three dimensions informational, social, and psychological privacy. Thus, three different SEMs were computed. The three SEMs were first tested regarding model fit. The following guidelines for testing model fit criteria were applied: χ^2 divided by degrees of freedom was not to exceed a value of 5 (e.g., Marsh & Hocevar, 1985); as a combined rule, together with an SRMR of .06, the CFI, TLI, and RNI were not to fall below .90 (Hu & Bentler, 1999); the RMSEA were not exceed values of .08 (Browne & Cudeck, 1992).

SEM$_{\text{INF}}$ showed adequate model fit (χ^2 / df = 3.57, p < .001, CFI = .91, TLI = .90, RNI = .91, RMSEA = .07, 90% CI [.06, .07], SRMR = .06). SEM$_{\text{SOC}}$ also showed adequate model fit (χ^2 / df = 3.35, p < .001, CFI = .90, TLI = .89, RNI = .90, RMSEA = .06, 90% CI [.06, .07], SRMR = .06). However, the

Table 3.3: Fit Indices for the Three SEMs of Informational (SEM_{INF}), Social (SEM_{SOC}), and Psychological (SEM_{PSY}) Privacy

		SEM_{INF}		SEM_{SOC}		SEM_{PSY}	
Fit indices	Criteria	A priori	Post hoc	A priori	Post hoc	A priori	Post hoc
χ^2		720.34	534.38	677.26	443.5	634.68	449.07
df		202	179	202	178	202	179
χ^2 / *df*	<5[a]	3.57	2.99	3.35	2.49	3.14	2.51
CFI	>.90[b]	0.91	0.94	0.90	0.94	0.93	0.96
TLI	>.90[b]	0.90	0.93	0.89	0.93	0.92	0.95
RNI	>.90[b]	0.91	0.94	0.90	0.94	0.93	0.96
RMSEA	<.08[c]	.07	.06	.06	.05	.06	.05
SRMR	<.08[d]	.06	.06	.06	.05	.05	.05

Note: Note. [a]Marsh and Hocevar, 1985; [b]Hu and Bentler, 1999; [c]Browne and Cudeck, 1992; ' [d]Hu and Bentler, 1999

TLI did not reach the expected .90. SEM_{PSY} showed good model fit (χ^2 / df = 3.14, $p < .001$, CFI = .93, TLI = .92, RNI = .93, RMSEA = .06, 90% CI [.06, .07], SRMR = .05). For a comprehensive overview, see Table 3.3. In conclusion, the a priori models showed adequate model fit. However, further analyses suggested model adjustments, which are explained below.

Factorial validity

Table 3.4 shows the SEMs' measurement model. Except item $ATT_{SOC}3$, all items exceeded a threshold of .50, implying adequate overall model fit. Two items were removed: Item $ATT_{SOC}3$ ("I think that restricting access to one's FB profile is: worrying – not worrying") was removed for inadequate fit ($\gamma = .46$). Item PC5 ("Are you concerned that information about you could be found on an old computer?") was removed because it is not necessarily associated with privacy concerns in online contexts and was thus deemed theoretically irrelevant. To check for individual cross-loadings and error covariances, modification indices were computed. No significant cross-loadings were found that warranted inclusion in the model. With respect to error covariances, indices showed that some items ($ATT_{SOC}5$, $ATT_{SOC}6$; PC4, PC5;

PC8, PC9, PC10) were correlated substantially. As the items' formulations were especially parallel (see Table 3.1), the correlations seemed plausible and were integrated into the new model.

To further check for factorial validity, the average variance extracted (AVE) was computed. Except for the privacy concerns, the values for all variables were above the minimum of AVE = .50 (Fornell & Larcker, 1981, see Table 3.4). To analyze factor reliability, the composite reliability REL(ξ) was computed. All variables were above the minimum of REL(ξ) = .60 (Bagozzi & Yi, 1988). In general, analyses showed that the privacy concern scale did not perform well. However, it was maintained due to its importance in answering research questions. The removal of the two items (ATT$_{soc}$3 and PC5) and the inclusion of the item error covariances improved model fit significantly. The three new models showed good fit (Table 3.3).

Hypothesis 1 Hypothesis 1 stated that (a) informational, (b) social, and (c) psychological privacy attitudes would have a direct positive effect on corresponding privacy behaviors.

Results indicated that informational privacy attitudes did have a positive direct effect on informational privacy behavior ($b = 0.12$, 95% CI [0.05, 0.19], $\beta = .11$, $p = .04$, $SE = .06$). This implies that people who favor disguising their identity on Facebook are also less identifiable on Facebook. The effect is small.

For social privacy, results showed that social privacy attitudes also did have a positive direct effect on social privacy behavior ($b = 0.36$, 95% CI [0.16, 0.56], $\beta = .20$, $p = .001$, $SE = .10$) demonstrating that people who have a positive opinion toward restricting access to their profiles on Facebook also employ more profile restrictions on Facebook. The effect is also small.

In terms of psychological privacy, results showed that psychological privacy attitudes did have a positive direct effect on psychological privacy behavior ($b = 0.05$, 95% CI [0.01, 0.10], $\beta = .08$, $p = .030$, $SE = .02$). This implies that people who hold the belief that it is not good to have a Facebook profile full of personal information also have a Facebook profile that is less personal. Again, the effect is small.

Table 3.4: Indices for Measurement Models: Factor Loadings (γ), Composite Reliability (Rel (ξ)), and Average Variance Extracted (AVE) of the SEMs

	SEM_{INF}			SEM_{SOC}			SEM_{PSY}		
	γ	Rel (ξ)	AVE	γ	Rel (ξ)	AVE	γ	Rel (ξ)	AVE
P. Behaviors		0.79	0.57		0.85	0.66		0.83	0.62
PB1	.88*			.83*			.62*		
PB2	.83*			.88*			.83*		
PB3	.51*			.72*			.89*		
P. Intentions		0.85	0.66		0.95	0.60		0.86	0.68
PI1	.92*			.57*			.65*		
PI2	.91*			.85*			.88*		
PI3	.54*			.83*			.92*		
P. Attitudes		0.93	0.55		0.93	0.54		0.95	0.60
PA1	.77*			.77*			.86*		
PA2	.77*			.70*			.82*		
PA3	.67*			.46^{*a}			.62*		
PA4	.63*			.69*			.63*		
PA5	.71*			.56*			.77*		
PA6	.81*			.71*			.85*		
P. Concerns		0.83	0.35		0.83	0.35		0.83	0.35
PC1	.58*			.57*			.56*		
PC2	.61*			.62*			.62*		
PC3	.62*			.61*			.61*		
PC4	.56*			.56*			.57*		
PC5	.57*			.58*			.58*		
PC6	.51^{*a}			.52^{*a}			.51^{*a}		
PC7	.63*			.64*			.62*		
PC8	.61*			.61*			.61*		
PC9	.50*			.50*			.50*		
PC10	.61*			.61*			.62*		

Note: $^{*}p < .001$. ^{a}Item was deleted post hoc.

Hypothesis 2 Hypothesis 2 stated that (a) informational, (b) social, and (c) psychological privacy attitudes would positively influence (a) informational, (b) social, and (c) psychological privacy intentions, which in turn would positively influence (a) informational, (b) social, and (c) psychological privacy behaviors.

Results showed that informational privacy attitudes did have a positive indirect effect on informational privacy behaviors, mediated by informational privacy intentions ($b = 0.47$, 95% CI [0.38, 0.57], $\beta = .44$, $p < .001$, $SE = .05$). This implies that people who have a positive opinion on disguising their identity on Facebook also report an increased intention to do so, which finally leads to the fact that they are less identifiable on Facebook. The effect can be considered medium to large.

For social privacy, it was revealed that social privacy attitudes also had a positive indirect effect on social privacy behaviors, mediated by social privacy intentions ($b = 0.49$, 95% CI [0.34, 0.63], $\beta = .28$, $p < .001$, $SE = .07$). This indicates that people who have a positive opinion on restricting access to their profiles on Facebook also have an increased intention to do so, which in turn leads to the fact that they employ more profile restrictions on Facebook. The effect is to be considered small to medium.

Regarding psychological privacy, results demonstrated that attitudes also had a positive indirect effect on psychological privacy behaviors mediated by psychological privacy intentions ($b = 0.29$, 95% CI [0.23, 0.35], $\beta = .46$, $p < .001$, $SE = 0.03$). People who disapprove of having a Facebook profile showing personal information also have the intention to withhold personal information and therefore have a Facebook profile that is less personal. The effect can be considered medium to large.

In technical terms, the three significant direct effects of H1 and the three significant indirect effects of H2 demonstrate partial mediation. To assess mediation size, the proportion of mediation was computed (e.g., Iacobucci, Saldanha, & Deng, 2007). For all three dimensions, the proportion of the indirect effect on the total effect was large (informational = .80, social = .59, psychological = .84). Hence, mediation analyses also confirmed the importance of using intentions as mediator between privacy attitudes and privacy behaviors.

Hypothesis 3 Hypothesis 3 posited that privacy concerns would positively influence (a) informational, (b) social, and (c) psychological privacy attitudes, which in turn would positively influence (a) informational, (b) social, and (c) psychological privacy intentions and the (a) informational, (b) social, and (c) psychological privacy behaviors.

Results showed that privacy concerns did have an indirect effect on informational privacy behaviors ($b = 0.54$, 95% CI [0.39, 0.70], $\beta = .23$, $p < .001$, $SE = .08$). First, privacy concerns were related to informational privacy attitudes; informational privacy attitudes in turn had both a direct effect on informational privacy behaviors (as was already shown in H1) and an indirect effect (as already shown in H2). This implies that respondents who have pronounced privacy concerns are also more skeptical regarding the posting of identifiable information on Facebook, which in turn is both directly and indirectly associated with a profile that features less identifiable information online. The effect is small.

The effect also was shown for social privacy behaviors ($b = 0.38$, 95% CI [0.24, 0.51], $\beta = .16$, $p < .001$, $SE = .07$). This indicates that people who have pronounced privacy concerns also think that it is good to restrict access to their Facebook profile, which in turn is directly and indirectly associated with a more restricted Facebook profile. The effect is small.

Finally, the effect also existed for psychological privacy behaviors ($b = 0.22$, $\beta = .12$, $p < .001$, $SE = 0.05$). This implies that respondents who have increased privacy concerns also believe that it is good not to post too much personal information on Facebook. This attitude is then both directly and indirectly accompanied with a less personal Facebook profile. The effect is small.

Additional analyses and modification indices showed that no direct effect of privacy concerns on privacy behavior existed, which is why no proportion of mediation was computed. For an overview of all effects, see Table 3.5. For a visual representation of the results of H1–H3, see Figure 3.2.

Table 3.5: Estimates of Effects for Privacy Concerns and Privacy Attitudes on Privacy Behaviors for the Three SEMs of Informational (SEM_{INF}), Social (SEM_{SOC}), and Psychological (SEM_{PSY}) Privacy

	SEM_{INF}			SEM_{SOC}			SEM_{PSY}		
Effects	*b*	95% CI	β	*b*	95% CI	β	*b*	95% CI	β
Direct effects									
a	0.67	[0.59, 0.76]	.68***	0.72	[0.58, 0.86]	.61***	0.40	[0.34, 0.47]	.58***
b	0.70	[0.59, 0.82]	.65***	0.68	[0.49, 0.86]	.45***	0.73	[0.63, 0.82]	.79***
c [H1]	0.12	[0.01, 0.23]	.11*	0.36	[0.16, 0.56]	.20***	0.05	[0.01, 0.10]	.08*
d	0.92	[0.69, 1.15]	.42***	0.44	[0.30, 0.59]	.33***	0.63	[0.39, 0.88]	.25***
Indirect effects									
a x b [H2]	0.47	[0.38, 0.57]	.44***	0.49	[0.34, 0.63]	.28***	0.29	[0.23, 0.35]	.46***
d x a x b	0.43	[0.30, 0.57]	.18***	0.22	[0.13, 0.31]	.09***	0.19	[0.10, 0.27]	.11***
d x c	0.11	[0.01, 0.21]	.05*	0.16	[0.06, 0.26]	.07**	0.03	[0.01, 0.07]	.02*
Total effects									
(a x b) + c	0.59	[0.49, 0.69]	.55***	0.85	[0.68, 1.02]	.48***	0.35	[0.28, 0.41]	.55***
(d x c) + (d x a x b) [H3]	0.54	[0.39, 0.70]	.23***	0.38	[0.24, 0.51]	.16***	0.22	[0.13, 0.31]	.14***

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

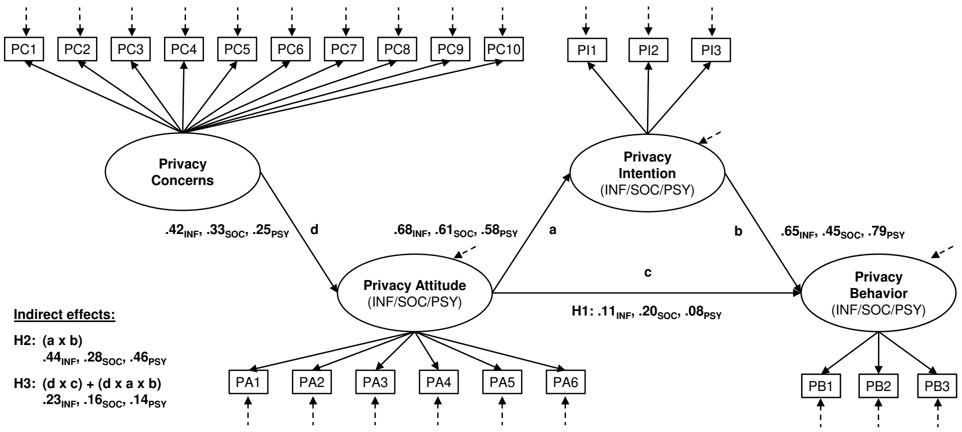

Figure 3.2: Visualization of effects for the three SEMs of informational privacy (SEM_{INF}), social privacy (SEM_{SOC}), and psychological privacy (SEM_{PSY}). Path c represents Hypothesis 1, path $a \text{x} b$ represents Hypothesis 2, and path $(d \text{x} c)$ + $(d \text{x} a \text{x} b)$ represents Hypothesis 3. All effects are significant on the basis of a level of significance of $p < .05$

3.5 Discussion

3.5.1 Implications

The privacy paradox The first aim of this study was to replicate former studies that investigated the privacy paradox. Results of prior research were twofold: Some studies showed that privacy concerns were not associated with specific privacy behaviors (Acquisti & Gross, 2006; Trepte et al., 2014; Ellison et al., 2011; Gross & Acquisti, 2005; Nosko et al., 2012; Stutzman & Kramer-Duffield, 2010; Taddei & Contena, 2013; Tufekci, 2008); others found that by using variables that closely refer to privacy concerns (e.g., perceived privacy risks; Mohamed & Ahmad, 2012) privacy behaviors can be explained to a certain degree (Debatin et al., 2009; Joinson et al., 2010; Krasnova et al., 2010; Mohamed & Ahmad, 2012; Stutzman et al., 2012).

The results of this study showed that privacy concerns were mostly unrelated to specific privacy behaviors on SNSs. People who were concerned about their privacy were not less likely to indicate their authentic first name, their authentic second name, their cell-phone number, or their political views on Facebook. Also, privacy concerns were demonstrated to be unrelated to the frequency of status posts on Facebook. However, one inconsistent observation was made: Privacy concerns were negatively associated with the disclosure of the personal address on Facebook. Taken together, the results suggest the following: Privacy concerns do not sufficiently predict specific privacy behaviors, and even when they do the effects are small. This shows that privacy concerns do not play a major part when it comes to explaining specific actions on SNSs. Thus, it can be summarized that also after several years the privacy paradox can still be found — as long as it is investigated as suggested and outlined above.

Advances to the privacy paradox In a second aim of the research, a new approach toward the privacy paradox was suggested. This new approach was based on the TPB and a fine-grained definition of privacy as referring to informational, psychological, and social aspects.

It was demonstrated that informational, social, and psychological privacy attitudes were significantly related to informational, social, and psychological privacy behaviors. It does make a difference if people think that it is for example (a) useful to indicate one's authentic name on Facebook (informational privacy dimension), that it is (b) good to use friend lists to restrict access to one's profile (social privacy dimension), or that it is (c) dangerous to disclose personal pieces of information on Facebook (psychological privacy dimension). If users of SNSs are of these opinions, their attitudes do affect their corresponding privacy behaviors. In addition to the direct effect, attitudes were found to also indirectly affect behavior through intentions: Attitudes are associated with an increased intention to show these behaviors, which in turn is associated with an increased privacy behavior. More important, effect sizes indicate that these associations are substantial: Privacy attitudes are decisive when it comes to understanding people's privacy behaviors.

In addition, results showed that privacy concerns were indirectly associated with privacy behaviors on all three dimensions. Although privacy concerns are not directly related to privacy behaviors, they nonetheless affect privacy behaviors indirectly. Thus when operationalized adequately, it can be shown that privacy concerns play a significant role when it comes to explaining privacy behaviors. The results correspond with the findings of Taddei and Contena (2013): In their study, privacy concerns also did not relate directly to privacy behaviors. The authors nevertheless found that privacy concerns interacted with the general trust users had toward webpages, which was then associated directly with self-disclosure behaviors.

Arguably, the methodological alterations have proven to be worthwhile. The significant effects showed that applying the principle of compatibility to measures (Fishbein & Ajzen, 2010) generally narrowed and even bridged the attitude-behavior gap (Kaiser et al., 2010). Also, the differentiation between the three dimensions of privacy can be considered worthwhile: The three SEMs differed regarding the coefficients' estimates. For example, the relation between intentions and behaviors was the strongest in SEM_{PSY}. The coefficient $\beta = .79$ implies that people are capable of disclosing almost exactly as much information as they want to disclose. By contrast, the coefficient $\beta = .47$ for the same relation in the SEM_{SOC} indicates that even when people intend to restrict access to their Facebook profile, they are not equally capable of showing that behavior.

3.5.2 Limitations and future perspective

First, the results are based on cross-sectional data. Thus, the direction or causality of effects cannot be demonstrated statistically. It appears that attitudes influence behaviors; however, as has been shown for cognitive dissonance (Festinger, 1957), actions can also influence attitudes. Second, participation was voluntary, self-selective, and resulted in a convenience sample. This implies that the sample cannot be considered statistically representative. Third, the data are based on respondents' self-reports. This is especially relevant when it comes to measuring behavior; an objective procedure is to be preferred here. All the same, it has been shown for behaviors on SNSs that self-reports correspond closely to objective data (Hampton, Goulet, Marlow, & Rainie, 2012). Fourth, with respect to the SEM's quality, though adequate, the factorial validity and the model fit could have been better: Of the 58 items in use, 1 item performed poorly and 8 only just adequately. Also, the privacy concern scale needs to be reconsidered regarding the just acceptable internal factorial validity. It might prove worthwhile to update the scale as to better correspond to contemporary online contexts. As a final note, the TPB was designed to measure repeated behavior from a longitudinal perspective (Fishbein & Ajzen, 2010). This suggests an experimental or panel study with multiple measurements. Behaviors that were used in this study cannot be regarded as repeated; most people choose their profile name only once. Even so, it has been shown that a substantial part of users do change their privacy settings at some point — Utz and Kramer (2009) found that 90% of all users already did so.

The present study can be further analyzed regarding the three dimensions' distinct characteristics; for reasons of parsimony, those analyses were not included here. In addition, to corroborate the findings, future studies might want to develop alternative ways to measure overt behaviors. For example, the current results could be validated in experimental settings: Do observable privacy behaviors change when privacy attitudes are manipulated by, for example, exposure to news stories of online data fraud?

3.5.3 Conclusion

The findings of our study suggest the following: First, the privacy paradox is still a phenomenon to be detected in empirical data when analyzed exactly as it was done in prior research. Second, and more important, the privacy paradox disappears when (1) distinguishing between privacy concerns and privacy attitudes, by (2) using the TPB as a theory driven framework to operationalize the research design, and by (3) differentiating privacy dimensions (informational, social, and psychological) as proposed by Burgoon (1982). In conclusion, the privacy paradox can be dissolved: The results of our study clearly show that online privacy behaviors are not paradoxical in nature, but that they are based on distinct privacy attitudes. The privacy paradox can be considered a relic of the past.

Literature

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Proceedings of 6th Workshop on Privacy Enhancing Technologies* (pp. 36–58). Cambridge, UK: Robinson College.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control* (pp. 11–39). Berlin, Germany: Springer. doi:10.1007/978-3-642-69746-3{_}2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:10.1016/0749-5978(91)900 20-T

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Arbuckle, J. L. (1996). Full information estimation in the presence of incomplete data. In G. A. Marcoulides & R. E. Schumacker (Eds.), *Advanced structural equation modeling* (pp. 243–277). Mahwah, NJ: Lawrence Erlbaum Associates.

Bagozzi, R. P. & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. doi:10.1007/BF0 2723327

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from www.firstmonday.org/issues/issue11_9/barnes/index.html

Browne, M. W. & Cudeck, R. (1992). Alternative ways of assessing model fit. *Sociological Methods & Research*, *21*(2), 230–258. doi:10.1177/0049124192 021002005

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. doi:10.1002/asi.20459

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook 6* (pp. 206–249). Beverly Hills, CA: Routledge.

Burns, S. & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48–64. doi:10.1057/cpcs.2012.13

Courneya, K. S. & Bobick, T. M. (2000). Integrating the theory of planned behavior with the processes and stages of change in the exercise domain. *Psychology of Sport and Exercise*, *1*(1), 41–56. doi:10.1016/S1469-0292(00)00006-6

Crano, W. D. & Prislin, R. (2006). Attitudes and persuasion. *Annual Review of Psychology*, *57*(1), 345–374. doi:10.1146/annurev.psych.57.102904.190034

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

Durlak, J. A. (2009). How to select, calculate, and interpret effect sizes. *Journal of Pediatric Psychology*, *34*(9), 917–928. doi:10.1093/jpepsy/jsp004

Ellison, N. B., Lampe, C., & Vitak, J. (2011). With a little help from my friends: Social network sites and social capital. In Z. Papacharissi (Ed.), *A networked self* (pp. 124–145). New York, NY: Routledge.

European Commission. (2011). Attitudes on data protection and electronic identity in the European Union. Retrieved from www.ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Commission. (2012). Pan-European survey of practices, attitudes and policy preferences as regards personal identity data management. Brussels: European Commission. Retrieved from http://is.jrc.ec.europa.eu/pages/TFS/documents/EIDSURVEY_Web_001.pdf

Fazio, R. H. & Roskos-Ewoldsen, D. R. (1994). Acting as we feel: When and how attitudes guide behavior. In S. Havitt & T. C. Brock (Eds.), *Persuasion* (pp. 71–93). Boston, MA: Allyn & Bacon.

Field, A. P. (2009). *Discovering statistics using SPSS* (3rd ed.). Los Angeles, CA: Sage Publications.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Fishbein, M. & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. New York, NY: Psychology Press.

Fornell, C. & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*(3), 382. doi:10.2307/3150980

Gottschalk, I. & Kirn, S. (2013). Cloud computing as a tool for enhancing ecological goals? *Business & Information Systems Engineering*, *5*(5), 299–313. doi:10.1007/s12599-013-0284-2

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks: ACM Workshop on Privacy in the Electronic Society. Alexandria, VA.

Hagger, M. S., Chatzisarantis, N. L., & Biddle, S. J. (2002). A meta-analytic review of the theories of reasoned action and planned behavior in physical activity: Predictive validity and the contribution of additional variables. *Journal of Sport & Exercise Psychology*, *24*(1), 3–32.

Hampton, K. N., Goulet, L. S., Marlow, C., & Rainie, L. (2012). Why most Facebook users get more than they give. Washington, D.C. Retrieved from www.pewinternet.org/~/media/Files/Reports/2012/PIP_Facebook%20users_2.3.12.pdf

Hoy, M. G. & Milne, G. R. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. doi:10.1080/15252019.2010.10722168

Hu, L.-T. & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, *6*(1), 1–55. doi:10.1080/10705519909540118

Iacobucci, D., Saldanha, N., & Deng, X. (2007). A meditation on mediation: Evidence that structural equations models perform better than regressions. *Journal of Consumer Psychology*, *17*(2), 139–153. doi:10.1016/S1057-7408(07)70020-7

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, *25*(1), 1–24. doi:10.1080/07370020903586662

Kaiser, F. G., Byrka, K., & Hartig, T. (2010). Reviving Campbell's paradigm for attitude research. *Personality and Social Psychology Review*, *14*(4), 351–367. doi:10.1177/1088868310366452

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). Berlin, Germany: Springer.

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

LaPiere, R. T. (1934). Attitudes vs. actions. *Social Forces*, *13*(2), 230–237. doi:10.2307/2570339

Leiner, D. J. (2012, March). SoSci panel: The noncommercial online access panel. Poster presented at the GOR 2012, 6th March, Mannheim. Zugriff unter www.soscisurvey.de/panel/download/SoSciPanel.GOR2012.pdf.

Leiner, D. J. (2014). SoSci survey (Version 2.4.00-i) [Computer Software]. Retrieved from www.soscisurvey.de

Lewis, K. (2011). The co-evolution of social network ties and online privacy behavior. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (Vol. 2011, pp. 91–109). Berlin, Germany: Springer.

Marsh, H. W. & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First- and higher order factor models and their invariance across groups. *Psychological Bulletin*, *97*(3), 562–582. doi:10.1037/0033-2909.97.3.562

Mohamed, N. & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. doi:10.1016/j.chb.2012.07.008

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. *Computers in Human Behavior*, *26*(3), 406–418. doi:10.1016/j.chb.2009.11.012

Nosko, A., Wood, E., Kenney, M., Archer, K., de Pasquale, D., Molema, S., & Zivcakova, L. (2012). Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed? *Computers in Human Behavior*, *28*(6), 2067–2074. doi:10.1016/j.chb.2012.06.010

Peter, J. & Valkenburg, P. M. (2011). Adolescents' online privacy: Toward a developmental perspective. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 221–234). Berlin, Germany: Springer.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Petty, R. E. & Krosnick, J. A. (Eds.). (1995). *Attitudes strength: Antecedents and consequences* (4th ed.). Hillsdale, NJ: Erlbaum.

Pew Research Center. (2014). Survey questions. Retrieved from www.pewresearch.org/files/2014/01/Survey-Questions_Facebook.pdf

R Core Team. (2016). R: A language and environment for statistical computing [Computer Software]. Vienna, Austria: R Foundation for Statistical. Retrieved from www.R-project.org

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(2). Retrieved from www.jstatsoft.org/v48/i02/paper

Ruddigkeit, A., Penzel, J., & Schneider, J. (2013). Dinge, die meine Eltern nicht sehen sollten. *Publizistik*, *58*(3), 305–325. doi:10.1007/s11616-013-0183-z

Schmidt, F. L., Hunter, J. E., & Urry, V. W. (1976). Statistical power in criterion-related validation studies. *Journal of Applied Psychology*, *61*(4), 473–485. doi:10.1037/0021-9010.61.4.473

soscisurvey. (2014). SoSci Panel für Wissenschaftler. Retrieved from www.soscisurvey.de/panel/researchers.php

Stutzman, F. & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (pp. 1553–1562). New York, NY: ACM.

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). Privacy in interactions: Exploring disclosure and social capital in Facebook. In *Proceedings of International Conference on Weblogs and Social Media (ICWSM '12)*. Dublin, IE.

Taddei, S. & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. doi:10.1016/j.chb.2012.11.022

Terry, D., Gallois, C., & McCamish, M. (Eds.). (1993). *The theory of reasoned action: Its application to AIDS-preventive behaviour*. Oxford, UK: Pergamon Press.

Teutsch, D. & Niemann, J. (26.05.2014). Social network sites as a threat to users' self-determination and security: A framing analysis of German newspapers. Paper presented at the 64th annual conference of the International Communication Association. Seattle, WA.

Tormala, Z. L., Petty, R. E., & Brinol, P. (2002). Ease of retrieval effects in persuasion: A self-validation analysis. *Personality and Social Psychology Bulletin*, *28*(12), 1700–1712. doi:10.1177/014616702237651

Trepte, S., Dienlin, T., & Reinecke, L. (2013). Privacy, self-disclosure, social support, and social network site use. Research report of a three-year panel study. Retrieved from University of Hohenheim website: http://opus.uni-hohenheim.de/volltexte/2013/889/.

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors. How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis* (Vol. 41, pp. 225–244). Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft. Konstanz, Germany: UVK.

Trepte, S. & Reinecke, L. (Eds.). (2011a). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6{_}6

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

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36. doi:10.1177/0270467607311484

Utz, S. & Kramer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2). Retrieved from www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2

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

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 111–125). Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6{_}9

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722. doi:10.1002/asi.20530

Study 3

4 An extended privacy calculus model for SNSs — Analyzing self-disclosure and self-withdrawal in a representative U.S. sample

Preamble

Abstract

The privacy calculus established that online self-disclosures are based on a cost-benefit tradeoff. For the context of SNSs, however, the privacy calculus still needs further support as most studies consist of small student samples and analyze self-disclosure only, excluding self-withdrawal (e.g., the deletion of posts), which is essential in SNS contexts. Thus, this study used a U.S. representative sample to test the privacy calculus' generalizability and extend its theoretical framework by including both self-withdrawal behaviors and privacy self-efficacy. Results confirmed the extended privacy calculus model. Moreover, both privacy concerns and privacy self-efficacy positively predicted use of self-withdrawal. With regard to predicting self-disclosure in SNSs, benefits outweighed privacy concerns; regarding self-withdrawal, privacy concerns outweighed both privacy self-efficacy and benefits.

Keywords: privacy calculus, privacy paradox, self-efficacy, Facebook, structural equation modeling, representative sample

Status of publication

The following study has already been published. Please cite as follows: Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs — Analyzing self-disclosure and privacy behaviors in a representative U.S. sample. *Journal of Computer-Mediated Communication, 21*, 368–383. doi:10.1111/jcc4.12163

The content of the text has not been altered. For reasons of consistency, some minor changes in formatting have been carried out.

4.1 Introduction

With literally billions of users today, social network sites (SNSs) play a central role in everyday life. This is because SNSs offer several benefits such as helping users initiate or maintain social relationships, share information, or provide entertainment (e.g., Choi & Bazarova, 2015). However, SNSs also pose risks, for example, users can become victims of cyberbullying, surveillance by government agencies and private companies, and information can be accessed by unintended audiences (e.g., Marwick & boyd, 2011). Most of the risks relate to aspects of privacy, which helps explain why a lot of people have strong concerns when it comes to having control over the information they provide online (Pew Research Center, 2015).

Nonetheless understanding why, how, and to what effect people use SNSs despite the risks to privacy remains a major challenge for researchers (Zhang & Leung, 2015). Given that SNSs introduced a completely new infrastructure of communication, changed interpersonal processes in a way that can be compared only to the effect of the telephone, and enticed people to provide personal information to private companies on a scale never before seen, it is crucial to further our understanding of SNS behavior. And Facebook, despite the fact that other SNSs such as Instagram or Snapchat are becoming increasingly popular, is an important center of focus when it comes to privacy issues with more than one billion users worldwide.

As shown by Krasnova, Spiekermann, Koroleva, and Hildebrand (2010), the best explanation of SNS use despite privacy fears is that of the "privacy calculus" theory, which states that people will self-disclose personal information when perceived benefits exceed perceived negative consequences. Although this makes intuitive sense, in practice using the privacy calculus to explain self-disclosure on SNSs has proved to be difficult. According to the privacy calculus, people should disclose information on SNSs only when they perceive the benefits of doing so outweigh the perceived costs. Yet, some studies found that people disclosed information in SNSs even when they felt the risks were high (e.g., Taddicken, 2014), which has been called the "privacy paradox." This sparked a great deal of research, which sometimes did find significant statistical relations between privacy concerns (or perceived risks) and self-disclosure behavior in SNSs (e.g., Dienlin & Trepte, 2015; Zlatolas, Welzer, Heričko, & Hölbl, 2015). Hence, our first aim is to replicate earlier findings of the privacy calculus suggesting that both perceived benefits and potential risks affect self-disclosure.

Though prior research has applied the privacy calculus to SNSs, the generalizability of this finding needs to be substantiated. Altogether, we found 7 published studies that have analyzed the privacy calculus specifically, of which 5 focused on youth (e.g, Krasnova et al., 2010; Krasnova, Veltri, & Günther, 2012), 5 had small sample sizes ($N < 300$; e.g., Shibchurn & Yan, 2015; F. Xu, Michael, & Chen, 2013), and 6 used convenience samples (e.g., Sun, Wang, Shen, & Zhang, 2015). Moreover, even though SNSs initially came from the U.S., an extensive study on the privacy calculus using a large sample in the U.S. is still missing — so far, large-scale studies have only been conducted in China (Cheung, Lee, & Chan, 2015) and Korea (Min & Kim, 2015), or have focused on similar but distinct notions such as the privacy paradox (e.g., Taddicken, 2014).[1] Even these studies yield conflicting findings, as some report no relationship between perceived privacy risks and self-disclosure (Cheung et al., 2015; Taddicken, 2014) and others a negative relationship (Min & Kim, 2015). Hence, the second aim of this study is to improve the generalizability of the privacy calculus by analyzing it in a U.S. representative sample.

The third aim of this research is to elaborate the privacy calculus theory. One central finding of research that has not been addressed adequately in the theory is the concept of self-withdrawal. Unlike self-disclosure, which is the typical focus within this literature, self-withdrawal refers to the active retention of information (Altman, 1975). Yong Jin Park (2015) and others have demonstrated the importance of considering both self-disclosure and self-withdrawal in privacy research. And both aspects of privacy behavior are particularly salient for research on SNSs, as privacy behavior in SNSs is not limited to self-disclosure but also includes self-protection via withholding information. This is true for many reasons: For example, because of the

[1] Unlike the other studies cited here that focused on the privacy calculus within SNSs only, Taddicken (2014) examined privacy behavior across SNSs, blogs, wikis, discussion forums, photo and video sharing sites. While her study does not explicitly examine the privacy calculus, it does analyze the relationship between privacy concern and self-disclosure.

collapse of formerly distinct social contexts into a single audience on SNSs (Marwick & boyd, 2011), users need to be able to make some information inaccessible to particular people.

4.2 Theory

4.2.1 Privacy theory

Theorists disagree about how to define privacy as well as what it includes. According to Burgoon (1982), it is possible to distinguish physical privacy (freedom from surveillance and unwanted intrusions upon one's physical space), social privacy (control over social encounters), psychological privacy (protects from intrusions upon one's thoughts, feelings, attitudes, and values) and informational privacy (the ability to control the aggregation and dissemination of information). As privacy in SNSs is largely about the dissemination and retention of personal information, we hence focus on aspects of informational privacy.

According to Westin (1967), "privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means" (p. 7). This definition is pivotal in the privacy literature and shows the two major components of privacy theory: Privacy is, first of all, a withdrawal from others (e.g., Westin, 1967) that, second, must happen voluntarily by people who are in control of their withdrawal (e.g., Altman, 1975). 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). People withdraw from others for many reasons, for example, to make autonomous decisions, to foster intimate relationships, or to regulate emotions (Westin, 1967). Self-withdrawal is largely about trying to avoid negative outcomes of communication; which is why it can be considered a form of self-protection behavior (see Rogers, 1983).

On the other hand, people need to interact with one another to foster social relationships, and interacting with others always requires some form of self-disclosure—which in turn reduces privacy (Altman, 1975). Hence, people regulate their privacy most prominently by either self-withdrawing or self-disclosing (see also Petronio, 2012). But when do people withdraw from social interactions and when do they partake? Referring to the "calculus of behavior" (p. 35), Laufer and Wolfe (1977) were one of the first to analyze this question.

4.2.2 The privacy calculus

The answer provided by Laufer and Wolfe (1977) is that people weigh the potential risks and benefits in terms of the consequences for them in the future. Of course, people cannot know in advance what those risks and benefits might be, so they rely on past experience, intuition, or perception to assess them. Applying this perspective to SNSs, when users weigh perceived benefits more heavily than the risks to privacy — which are often nebulous and uncertain — disclosure is likely to occur. Indeed, some research suggests that disclosure behavior may be primarily motivated by the more proximate social benefits of SNS use rather than by the more distal risks to privacy (Krasnova et al., 2010).

The notion that expected risks and benefits influence peoples' behavior originally comes from economic literature (hence the term "homo economicus"), and stresses that human decision-making is often based on mathematical calculations. Later, social sciences adopted the calculus perspective in order to explain interpersonal behavior, often with a stronger focus on affect: Social exchange theory, for example, posits that when people expect to get more rewards than punishments they will engage in interpersonal interactions (Homans, 1974). Estimating the consequences of behaviors is difficult, as people cannot calculate the risks and benefits rationally, but rather have to perceive them psychologically (Rogers, 1983). Regarding the negative consequences of behavior, protection motivation theory hence argues that subjective, rather than objective, threat appraisals are the driving factor that determines behavior (Rogers, 1983). Empirical studies on SNSs support this theoretical reasoning; for example, F. Xu et al. (2013) found that the perceived privacy risk strongly predicted privacy concern in SNSs.

In an e-commerce setting, Culnan and Armstrong (1999) found that when people were not explicitly told that their personal data would be handled with care, people with greater privacy concerns were less willing to provide personal data. Culnan and Armstrong were the first to call this tradeoff the "privacy calculus" (p. 106). Building on behavior calculus theory (Laufer & Wolfe, 1977), the privacy calculus posits that people will disclose personal information when the perceived benefits exceed the potential costs. The privacy calculus has now been used to explain self-disclosure behaviors in various online contexts, but Krasnova et al. (2010) were the first to analyze the privacy calculus in the context of SNSs. The authors found that users who reported having higher perceived privacy risks had a less comprehensive Facebook profile and users who reported getting more benefits had a more comprehensive profile.

4.3 A new privacy calculus model

4.3.1 Distinction of self-disclosure and self-withdrawal

As stated earlier, one objective of this study is to integrate important tenets of privacy theory in an extended privacy calculus model. This is because prior research on the privacy calculus arguably has failed to integrate an important finding. That is, to date, most studies involving the privacy calculus have focused on self-disclosure only (e.g., Cheung et al., 2015). However, using SNSs does not only involve the *dispersion* of information (i.e., self-disclosure), but also the active *retention* of information (i.e., self-withdrawal; for example, limiting the audience for one's posts). Although related, SNS self-disclosure and self-withdrawal are not simple mirror-images of one another, but rather are distinct concepts (see Christofides, Muise, & Desmarais, 2009). For example, high self-disclosure does not necessitate low self-withdrawal (e.g., it is possible to disclose extensively on one topic while talking to a small group of people). For this reason, both concepts should be considered in the privacy calculus.

The basic tenet of communication privacy management theory (CPM, Petronio, 2012) is that disclosure and withdrawal stand in dialectical tension with one another. This means that people feel competing simultaneous needs to be both social (by disclosing information) and private (by withholding information). CPM differs from other theories in its view that in order to understand how people navigate privacy disclosure must always be considered in relation to the desire to protect information. People handle these competing needs by making decisions about the extent of privacy and publicness they want to have in a given interaction (Petronio, 2012). People hence establish privacy rules for both information disclosure and information withholding (for example, not to reveal one's medical history to a stranger).

Although CPM theory was developed for interpersonal interactions, the notion of competing desires for disclosure and privacy is also relevant in SNSs. For example, while most attention has been directed toward disclosure, SNS users can and do enact rules about untagging themselves in particular photos, posting only certain types of content, or being selective about whom they 'friend' as a means to protect their privacy. In accordance, Marwick and boyd (2011) posited that in order to leverage the benefits of SNSs, users have to make some information available to certain groups of users but not to others. We argue that such mechanisms can be considered self-withdrawal behaviors and are central facets of privacy-related behavior in SNSs. If self-disclosure is one side of the privacy coin, self-withdrawal is the other; and so far, whereas research on similar online phenomena has included this differentiation (Yong Jin Park, 2015), research on the privacy calculus has tended to focus on only one side.

4.3.2 Privacy concerns as costs

In privacy calculus research to date, "costs" of SNS use have been measured by either perceived privacy risks or privacy concerns. Privacy risks are "the expectation of losses associated with the release of personal information" (H. Xu, Luo, Carroll, & Rosson, 2011, p. 46), and privacy concerns are "the degree to which an Internet user is concerned about website practices related to the collection and use of his or her personal information" (Hong & Thong, 2013, p. 276). These definitions show that both privacy risks and privacy concerns involve fear concerning potential losses due to the disclosure of, or lack of control over, personal information. Protection motivation theory (Rogers, 1983) shows that fear is a strong driving factor in why people employ preventive measures, which may include self-withdrawal (i.e., withholding information) in SNS contexts. Most research on SNSs has operationalized costs as concerns (e.g., Min & Kim, 2015). Moreover, F. Xu et al. (2013) found that privacy risks predicted privacy concerns, which in turn determined self-disclosure. As a result, we focus on privacy concerns as a mitigating cost factor for self-disclosure and as a reinforcing factor for self-withdrawal.

4.3.3 Integrating privacy self-efficacy

Establishing self-protective behaviors can be difficult in any context (Rogers, 1983), and this may be especially true in SNSs, as enacting behaviors to protect privacy requires knowledge of how to implement the multitude privacy settings that are available and that change over time (Marwick & boyd, 2011). Protection motivation theory suggests that if people want to establish self-protecting behaviors, experiencing fear or concern does not suffice to effectively change behavior, as people also need to have sufficient self-efficacy (Rogers, 1983). Self-efficacy refers to the belief in one's ability to execute certain behaviors. As a result, we suggest integrating privacy self-efficacy as third predictor of SNS behavior in our extended privacy calculus model. To date, no studies of the privacy calculus have included this factor.

4.4 Hypotheses

4.4.1 Benefits

The most important factors to explain self-disclosure on SNSs are the positive aspects of SNS use, for example, making new friends or learning about things that are important or useful. In the context of SNSs, research shows that people have manifold motives for using SNSs: for example, information exchange, relational development, or entertainment (e.g., Choi & Bazarova, 2015). Several studies have also found empirical evidence that these motives for using SNSs manifest in several specific benefits, such as increased social capital, leveraged social support, or enacted identity management (e.g., Trepte, Dienlin, & Reinecke, 2014). All seven empirical studies on the privacy calculus for SNSs showed that if users expected benefits from using SNSs they disclosed more personal information. Benefits explained between 5% (Krasnova et al., 2012) and 66% (F. Xu et al., 2013) of variance in self-disclosure, and thus demonstrated that expected benefits have good predictive power. Thus, we hypothesize:

> *Hypothesis 1*: The more people expect benefits by using Facebook, the more they will disclose information about themselves.

The question remains though whether the expected benefits of participating in SNSs also influence self-protective behaviors online. Referring to Christofides et al. (2009), we argued that self-disclosure and self-withdrawal behaviors are related but nonetheless distinct behaviors. For example, on SNSs it is possible to have few users as friends (high self-withdrawal) to whom one nevertheless reveals a lot of information (high self-disclosure). On the one hand, one could argue that if people expect benefits from using SNSs they should withdraw less in order to maximize their outcomes; on the other hand, protection motivation theory (Rogers, 1983) suggests that only negative threat appraisals (i.e., privacy concerns), rather than positive feelings (i.e., expected benefits), determine self-protective behaviors. Hence, as we are not aware of any studies that analyzed the relationship between expected benefits and self-withdrawal empirically, and because of conflicting theoretical considerations, we propose the following research question:

> *Research question 1*: Do people who expect more benefits from using Facebook show more or less self-withdrawal behaviors?

4.4.2 Privacy concerns

For the Internet in general, privacy concerns have been found to negatively predict self-disclosure (e.g., Metzger, 2004). Also, for SNSs in particular, privacy concerns have been shown to negatively relate to self-disclosure: For example, SNS users who were concerned about their privacy tended to have profiles that were less personal, and also tended to disclose less identifying information (Dienlin & Trepte, 2015). Six of the seven studies on the privacy calculus in SNSs showed significant negative effects of concerns or risks on self-disclosure — only the study by Cheung et al. (2015) and the U.S. subsample in the study by Krasnova et al. (2012) did not show significant results.

Similarly, in a representative survey of German social media users, Taddicken (2014) examined privacy behavior in blogs, SNS, wikis, discussion forums, photo and video sharing sites and found that, across these platforms, disclosure varied depending on the sensitivity of the information to be disclosed. At the same time, no significant direct relation between privacy concern and self-disclosure was found, which shows that the relation between privacy concern and self-disclosure is still somewhat capricious. Hence, despite some inconsistency in the literature, a growing body of empirical studies has supported that concern about privacy and self-disclosure on SNSs are negatively associated with one another.

> *Hypothesis 2a*: The more concerned people are regarding privacy, the less information they will disclose about themselves in Facebook.

We also predict that privacy concerns are related to the active retention of information. Several studies report that concepts relating to privacy concerns are related to self-withdrawal behaviors: For example, Korzaan and Boswell (2008) found that users' level of information privacy concern predicted behavioral intentions to, for example, remove their name from commercial mailing lists. This association also holds in the SNS context: In a study with 340 Malaysian university students, privacy concerns were found to directly and significantly predict self-withdrawal measures on SNSs (Mohamed & Ahmad, 2012). Utz and Kramer (2009) similarly found that privacy concerns were associated with the use of privacy settings on Hyves, a SNS in the Netherlands. We therefore hypothesize that:

> *Hypothesis 2b*: The more concerned people are regarding privacy, the more they will engage in acts of self-withdrawal in Facebook.

4.4.3 Self-efficacy

The extant literature supports the notion that self-efficacy should predict implementing privacy enhancing or self-withdrawal behaviors online. For example, users who reported having more technical Internet skills related to privacy (e.g., phishing, p3p, or cache) also report employing more privacy-enhancing behaviors (e.g., using fake names for SNSs, clearing browser history, or deletion of cookies; Y. J. Park, 2013). Lee, LaRose, and Rifon (2008) found that users who reported more self-efficacy in using virus protection measures had a stronger intention to adopt virus protection behaviors. Similar results can be found for the context of SNSs: Both Cheung et al. (2015) and Zlatolas et al. (2015) evidenced that people who perceive to be in control of their privacy report less privacy concerns. Likewise, Mohamed and Ahmad (2012) found that both self-efficacy and response efficacy had a positive effect on the use of privacy measures.

> *Hypothesis 3*: People with greater privacy self-efficacy will engage in more self-withdrawal behaviors.

Finally, the question remains whether privacy self-efficacy might also affect self-disclosure. Niemann and Schenk (2014) found that privacy self-efficacy influenced self-withdrawal but not self-disclosure behaviors in SNSs. Also, from a theoretical perspective it can be argued that because the entire infrastructure of SNSs is built for self-disclosure, self-disclosing on SNSs is easy and does not necessitate high levels of competence or perceived behavioral control. However, privacy self-efficacy is conceptually close to self-efficacy regarding self-presentation, which has been shown to increase information disclosure (Krämer & Winter, 2008). Indeed, people who feel better able to protect themselves by using available SNS privacy settings, for example, may be more willing to disclose. Thus, because of conflicting theoretical and empirical considerations, we pose the following research question:

> *Research question 2*: Do people with greater privacy self-efficacy show more or less self-disclosure?

4.4.4 The extended privacy calculus model

The predictions advanced in the four hypotheses combine to suggest a novel framework to analyze the privacy calculus that we call the extended privacy calculus model. In accordance with CPM theory (Petronio, 2012), the model has two dependent variables: self-disclosure and self-withdrawal. We reason that these two variables are explained by different factors: Self-disclosure is explained on the basis of expected benefits and privacy concern, whereas self-withdrawal is explained by privacy concern and privacy self-efficacy. Due to a lack of theoretical and empirical clarity, we ask in two research questions whether perceived benefits predict privacy behaviors and whether privacy self-efficacy predicts self-disclosure.

4.5 Method

4.5.1 Procedure and participants

The data are representative of adult Facebook users ages 18 and over residing in the U.S. and were collected by the research firm GFK (www.gfk.com) in October 2012 by means of an online questionnaire. GfK samples households from its KnowledgePanel, which is a probability-based web panel designed to be representative of the U.S. To qualify for the main survey, a panel member must have had a Facebook account, as determined by a screener question at the time of data collection. The median participation time was 20 minutes.

The resulting sample consisted of $N = 1{,}156$ respondents ranging in age from 18 to 86 ($M = 46.91$) years. 57.35% of the respondents were female. Regarding ethnicity, 77.5% of the respondents were White, Non-Hispanic, 6.8% Black, Non-Hispanic, 3.2% Other, Non-Hispanic, 8.5% Hispanic, and 4% 2+ Races, Non-Hispanic. In relation to education, 6.1% indicated less than high school, 24.3% high school, 32.8% some college, and 36.8% bachelor's degree or higher. The median household income was between $60,000 to $74,999 per year. Regarding current residency, 18.9% of the respondents came from the Northeast, 22.6% from the Midwest, 34.3% from the South, and 24.2% from the West of the U.S.

4.5.2 Measures

Based on established scales and additional items that we designed in order to fit the research question more closely, confirmatory factor analyses (CFA) were run for each variable to select items that formed a unidimensional structure. To assess the assumption of normality, Shapiro-Wilk normality tests were done. As the results showed violations of normality, we used the more robust Satorra-Bentler scaled test statistic. Items that did not sufficiently load on the latent factor were deleted. To assess reliability of the constructed and congeneric scales, the usual fit indices (χ^2, CFI, TLI, RMSEA, SRNR), McDonald's composite reliability omega, and Cronbach's alpha were calculated. All scales had adequate to good factorial validity and reliability. The variables and their psychometrics appear in Table 4.1; all questionnaire items, the data, item distributions, and the CFAs can be found in the online supplementary material.[2]

Facebook benefits

Facebook benefits measured how many positive aspects people attributed to Facebook use. Twelve items were initially developed based on an earlier focus group pilot study of users who discussed the benefits and risks that they experience as a result of using Facebook. Of the 12 items, 10 were used as determined by the data preparation analysis discussed above that included, for example, using Facebook for self-expression, learning new things, and making new personal or business contacts (see Appendix). Respondents answered all items on a 5-point scale ranging from 1 = *strongly disagree* to 5 = *strongly agree*.

Privacy concerns

Privacy concerns measured how strongly people worried about their privacy online. Four items were developed based on Malhotra, Kim, and Agarwal (2004), which all were used — for example, "I do not feel especially concerned about my privacy online." Respondents answered both items on a 5-point scale ranging from 1 = *strongly disagree* to 5 = *strongly agree*. Several answers were reverse coded.

[2] https://osf.io/e3j98/?view_only=cf4c10222def4efdbecae20c1dca7dc6

Facebook privacy self-efficacy

Facebook privacy self-efficacy measured if people felt confident and capable of adjusting their privacy options on Facebook. We adapted the perceived privacy control scale by Krasnova et al. (2010) in order to better represent self-efficacy, and used all 5 items. One example item is: "I feel confident in my ability to protect myself using Facebook's privacy settings." Answers ranged from 1 = *strongly disagree* to 5 = *strongly agree*.

Facebook self-disclosure

Facebook self-disclosure measured the extent to which people share personal information on Facebook. We extended the self-disclosure scale by Krasnova et al. (2010) using 5 of the 7 items, including "I have put a lot of information about myself in my Facebook profile." Respondents answered all items on a 5-point scale ranging from 1 = *strongly disagree* to 5 = *strongly agree*.

Facebook self-withdrawal

This variable measured how many deliberate privacy-preserving behaviors people engaged in that helped to make their profiles more private. In line with Mohamed and Ahmad (2012), we asked respondents on a binary scale whether they have already implemented various privacy measures, such as the untagging of posts or photos, or making one's profile unsearchable. Respondents answered each item with either 0 = *no* or 1 = *yes*. 10 items were developed, of which 6 items formed a unidimensional scale.

4.5.3 Data analysis

All hypotheses were tested with a saturated structural equation model (SEM). Again, we used the robust Satorra-Bentler scaled test statistic. Because of the high number of items, which increases the complexity of the SEM, we used item parceling (Little, Cunningham, Shahar, & Widaman, 2002). Item-parcels average the information of several items into individual parcels. As a precondition, items that are parceled need to show unidimensionality, which

Table 4.1: Psychometric Properties of Variables

	Recom. Crit.	FB benefits	Privacy concerns	FB privacy self-efficacy	FB self-disclosure	FB self-withdrawal
m		3.13	3.34	2.89	2.65	0.67
sd		0.91	0.97	0.95	1.04	0.41
skew.		-0.49	-0.17	-0.04	0.07	-1.03
kurt.		0.09	-0.39	-0.49	-0.69	0.77
χ^2		158.50	6.06	12.14	25.34	30.47
df		35	2	5	5	9
p	>.05[a]	<.001	.050	.030	<.001	<.001
CFI	>.95[a]	0.96	0.99	1.00	0.99	0.96
TLI	>.95[a]	0.95	0.97	0.99	0.97	0.93
RMSEA	<.08[a]	0.06	0.04	0.04	0.06	0.05
SRMR	<.08[a]	0.03	0.02	0.01	0.02	0.06
α	>.70[a]	0.91	0.67	0.91	0.80	0.74
ω	>.60[a]	0.91	0.68	0.91	0.81	0.56
AVE	>.50[a]	0.77	0.55	0.83	0.71	0.32
MSV	< AVE[a]	0.37	0.15	0.08	0.37	0.15
ASV	< AVE[a]	0.09	0.06	0.05	0.10	0.04

Note: [a]Hair, Black, Babin, and Anderson (2010); α = Cronbach's alpha; ω = composite reliability. AVE = average variance extracted, MSV = maximum shared variance, ASV = average shared variance (all measured in final SEM).

was positive in our case (see Table 4.1). We used the item-to-construct balance approach and measured each variable with 2 parcels, and when possible as recommended with 3 parcels (Little et al., 2002).

Missing data were treated with listwise deletion. We tested Hypotheses with a two-tailed .05 significance level. Regarding effect sizes, coefficients with values exceeding $\beta = .10$ were considered small effects, $\beta = .30$ medium effects, and $\beta = .50$ large effects. We decided against including post-stratification weights and demographic control variables.[3] The software R was used (version 3.1.2) for the analyses, supplemented by packages such as lavaan (version 0.5-17).

4.6 Results

4.6.1 Model fit

The SEM showed adequate fit ($\chi^2 = 99.70$, $df = 44$, $p < .001$, CFI = 0.99, TLI = 0.99, RMSEA = 0.03, SRMS = 0.03). To assess convergent factorial validity, the average variance extracted (AVE) was calculated. Values above AVE = .5 indicate good convergent validity. Four of the five variables were above this threshold, and one was below (Facebook self-withdrawal, AVE = .32; see Table 4.1). Given that Facebook self-withdrawal was measured with binary items only, factorial validity can thus be considered acceptable. To assess discriminant validity, the AVE was compared to the maximum shared variance (MSV) and the average shared variance (ASV). Results showed that AVE values were above MSV and ASV values (see Table 4.1), which supports that the variables had sufficient discriminant validity.[4]

[3] To improve representativeness, GFK offers post-stratification weights that account for systematic under- and oversampling of specific parts of the population. The question of whether or not to use weights is somewhat ambivalent. We followed the U.S. Bureau of Labor Statistics advice to not use weights when conducting inferential statistics (i.e., regressions). For the results with weights, please see the online supplementary material. Generally, demographic control variables should only be included if they are theoretically related to the variables of interest. Even though demographic variables are related to privacy behavior online, they were not of major theoretical interest. For results without the control variables, please see the online supplementary material. Both alternative SEMs produced very similar results to the main SEM.

[4] When all items are measured on the basis of a single online questionnaire — as was the case for this study — a bias due to common method might occur. Several statistical methods exist to test for common method bias. However, the practice of testing for common method

4.6.2 Hypotheses

Facebook benefits as predictor

Hypothesis 1 stated that the more benefits people expect from using Facebook, the more they would self-disclose. The data supported Hypothesis 1: Respondents who reported that they would get more social benefits on Facebook also posted more personal information ($b = 0.65$, 95% CI [0.57, 0.73], $\beta = .57$, $p < .001$, $SE = 0.04$). The standardized regression coefficient of $\beta = .57$ showed that the effect was strong. Research question 1 asked whether Facebook benefits would predict Facebook self-withdrawal. Results indicated there was no significant effect of Facebook benefits on self-withdrawal ($b = 0.01$, 95% CI [-0.03, 0.04], $SE = 0.02$, $p = .713$, $\beta = .02$).

Privacy concerns as predictor

Hypothesis 2a predicted that the more concerned people are about privacy, the less information they would disclose. The data supported Hypothesis 2a: Respondents who reported higher levels of concern about their privacy also posted less personal information on Facebook ($b = -0.29$, 95% CI [-0.38, -0.20], $\beta = -.23$, $p < .001$, $SE = 0.05$). The standardized regression coefficient of $\beta = -.23$ indicated that the effect was small. Hypothesis 2b stated that the more concerned people are regarding privacy, the more they would employ active self-withdrawal. The data supported Hypothesis 2b: Respondents who reported greater concern about their privacy also reported using more self-withdrawal mechanisms on Facebook ($b = 0.19$, 95% CI [0.15, 0.23], $\beta = .45$, $p < .001$, $SE = 0.02$). The standardized regression coefficient of $\beta = .45$ showed that the effect was of medium strength. Bootstrap analyses with $N = 2000$ draws indicated that, taken together, privacy concerns explained 41.2% of variance in self-disclosure and self-withdrawal (95% CI [26.9%, 56.6%]).

bias by means of statistical post hoc test has been criticized. As a result, we used a priori precautions; for example, we took care that items did not semantically overlap on different constructs (see Table 4.1) or used some inverted items.

Privacy self-efficacy as predictor

Hypothesis 3 anticipated that people with greater Facebook privacy self-efficacy would employ active self-withdrawal more than those with lower self-efficacy. The data supported Hypothesis 3: Respondents who reported higher self-efficacy in terms of managing their privacy also reported using more self-withdrawal mechanisms on Facebook ($b = 0.08$, 95% CI [0.05, 0.11], $\beta = .27$, $p < .001$, $SE = 0.01$). The standardized regression coefficient of $\beta = .27$ indicated that this effect was small. Research question 2 asked whether privacy self-efficacy would also predict Facebook self-disclosure. Results showed that there was no significant effect of Facebook privacy self-efficacy on self-disclosure ($b = 0.03$, 95% CI [-0.03, 0.09], $SE = 0.03$, $p = .308$, $\beta = .03$).

Comparison of effects

Regarding effects on Facebook self-disclosure, comparison of confidence intervals shows that the net effect of benefits exceeded that of privacy concerns, which in turn exceeded that of privacy self-efficacy. Taken together, all three variables explained 37.87% of Facebook self-disclosure. With regard to effects on Facebook self-withdrawal, comparison of the confidence intervals shows that the net effect of privacy concern exceeded that of privacy self-efficacy, which in turn exceeded that of Facebook benefits. Taken together, all three variables explained 27.58% of Facebook self-withdrawal. In addition, we tested whether expected benefits or privacy concerns explained more variance of both dependent variables taken together (i.e., self-disclosure plus self-withdrawal behavior). Bootstrap analyses with $N = 2000$ draws showed that Facebook benefits altogether explained 32.9% of variance (95% CI [26.0%, 38.9%]) and that privacy concerns explained 41.2% of variance (95% CI [26.9%, 56.6%]). As the confidence intervals do not overlap, this shows that both variables did not differ significantly in their overall predictive power. For a list of all regression statistics see Table 4.2, and for a visual representation see Figure 4.1.

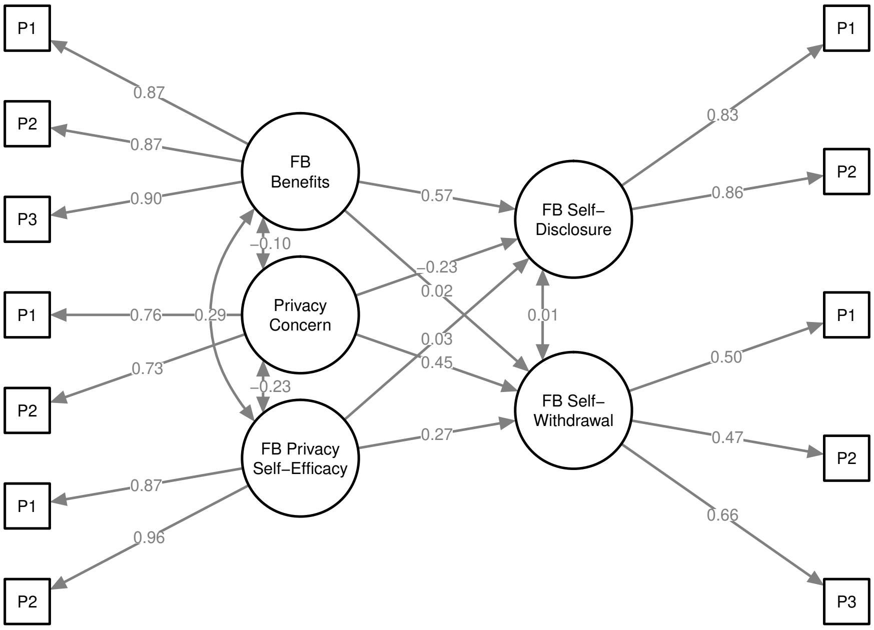

Figure 4.1: Results of the structural equation model. Only significant path coefficients are shown (.05 significance level). The effects are standardized. Dashed arrows indicate negative relations.

Table 4.2: Regression Coefficients

	b	(LL)	(UL)	*se*	*p*	β
Facebook self-disclosure						
Facebook benefits	0.65	0.57	0.73	0.04	<.001	.57
Facebook concerns	-0.29	-0.38	-0.20	0.05	<.001	-.23
Facebook privacy self-efficacy	0.03	-0.03	0.09	0.03	.308	.03
Facebook self-withdrawal						
Privacy benefits	0.01	-0.03	0.04	0.02	.713	.02
Facebook concerns	0.19	0.15	0.23	0.02	<.001	.45
Facebook privacy self-efficacy	0.08	0.05	0.11	0.01	<.001	.27

4.7 Discussion

4.7.1 Implications

This study set out to see if prior findings on the privacy calculus and its effect on self-disclosure in SNS could be replicated, to analyze the generalizability of the privacy calculus to a larger and representative U.S. sample, and to extend its theoretical framework.

The importance of replication in research has been discussed widely in recent years. Thus the first major finding of this study is that the privacy calculus findings of past work could be replicated. Specifically, this study finds that when people decide whether to self-disclose in SNSs, both concerns and benefits compete with one another. This is relevant as some research on the privacy paradox showed no, small, or complex relations between concerns and disclosure; Taddicken (2014), for example, found that perceived social relevance mediated the relation between privacy concerns and self-disclosure. The mixed findings could partly result from the fact that privacy concerns have often been operationalized differently and in specific contexts (e.g., ecommerce, SNSs); hence, results from any one study should not be overly generalized. Overall, by finding evidence for the privacy calculus, this study adds to a growing body of research that fails to find evidence for the privacy paradox in the context of SNSs (e.g., Dienlin & Trepte, 2015). However when predicting Facebook self-disclosure, expected benefits still have more predictive power than privacy concerns. This replicates findings by Min and Kim (2015) and supports the idea that when partaking actively in SNSs, benefits loom larger than concerns.

The second major finding of this study is that, by means of a nationwide representative study, the data confirmed that the privacy calculus can be generalized to the U.S. adult Facebook population. Prior research on the privacy calculus has mainly been conducted with college-age samples only, whereas this study included people from across different generations and people from a much wider variety of educational and ethnical backgrounds. As a result, this study substantiates the empirical foundation for the privacy calculus laid by prior research and, by showing that it can be applied to Facebook users in an entire nation, adds to its robustness. The third and perhaps most interesting finding is that this study makes several contributions to the privacy calculus's theoretical framework. In our extended privacy calculus model we included self-withdrawal behaviors as a new criterion and added privacy self-efficacy as a predictor. Although other studies have investigated the mechanisms underlying the privacy calculus by, for example, examining further predictors of self-disclosure (Min & Kim, 2015) or privacy risks (Krasnova et al., 2010), to our knowledge, this is the first study to show that both self-disclosure and self-withdrawal behaviors can be analyzed in a single model. This helps to show two things: First, the results further underscore the relevance of privacy concerns, as privacy concerns not only explained self-disclosure but also self-withdrawal. Hence, privacy concerns are more powerful as initially thought and play an important role in determining SNS behavior. Second, different factors help to explain variance in self-disclosure and in self-withdrawal. That is, whereas benefits predicted only self-disclosure, privacy concerns predicted both self-disclosure and self-withdrawal behaviors. A comparison of the combined effects even confirmed that benefits and concerns have equal predictive power for self-disclosure and self-withdrawal.

The results of the research questions shed further light on the role of both perceived benefits and privacy concerns in SNS, as well as self-efficacy. Prior to this study it was unclear whether perceived benefits, in addition to increasing self-disclosure, influence self-withdrawal in SNSs since no research had investigated this relationship. The data from this study support the suggestion from protection motivation theory that only negative threat appraisals (e.g., privacy concerns) should impact self-protection behaviors (e.g., self-withdrawal in SNS contexts).

Finally, this study showed that privacy self-efficacy is not related to disclosure in SNSs. This relation has not been studied previously but could be supported by research on optimistic bias (see Klein & Helweg-Larsen, 2002) in that privacy self-efficacy might impart a sense of invulnerability to potential negative consequences of using SNSs. However, we found no evidence for this notion. This study also revealed that privacy self-efficacy significantly predicted self-withdrawal, which supports one of privacy theory's central tenets that in order to regulate privacy effectively, people also need to have sufficient control (Westin, 1967), including the psychological perception that they are able to enact such control.

4.7.2 Limitations and future perspective

A limitation of the privacy calculus theory, as well as the model advanced in this study, is that it explicitly focuses on the individual. Yet, within SNS contexts, privacy is both an individual and a social issue. Indeed, one of the most exciting recent developments in the privacy research literature is the notion of "networked privacy" (Marwick & boyd d., 2014), which refers to the fact that control of information disclosure in networked environments such as SNSs does not solely reside in the actions taken by an individual user — it is collectively affected by network ties. For example, one user's action (e.g., self-disclosure, "liking," tagging, etc.) can reveal information about other users in the network to unknown or unauthorized audiences.

The idea of networked privacy, or the fact that privacy is socially contextualized in networked environments, has not been studied extensively in the privacy calculus literature, and yet an individual's calculus of the costs and benefits of using SNSs is most certainly affected by their network linkages. Indeed, Cheung et al. (2015) showed that social influences can explain up to 16% of variance in self-disclosure. Social influences on the privacy calculus need to be examined in future research, and it would be valuable to integrate socially-oriented theories to do so (e.g., the theory of planned behavior). That said, given that three variables can explain 38% of self-disclosure and 28% of self-withdrawal behavior, the extended privacy calculus offers a both parsimonious and effective approach for understanding privacy in SNSs. Because the study used cross-sectional data, the postulated directions of effects have yet to be verified with a longitudinal design. In addition, the scales used in this study need to be further optimized, as some items could not be used due to lack of reliability or factorial validity.

The study presents the psychology and behaviors of Facebook users in 2012. Since then, the online world has changed significantly: New SNSs such as Instagram entered the market, new messengers such as Snapchat appeared, and new risky behaviors such as novel forms of sexting or taking extreme selfies manifested. As a result, it is important to find out whether the extended privacy calculus model also helps to explain these novel behaviors, or whether other aspects such as fear of missing out (FoMO) or sensation seeking become increasingly relevant. It is important for future research to examine if the extended privacy calculus model holds for newer SNS platforms. It is possible, for example, that SNSs which allow for ephemeral communication (e.g., Snapchat) may alter an individual's cost-benefit calculus of posting risky messages with impacts to their self-disclosure and self-withdrawal behaviors. That said, the results of this study likely remain valid for Facebook and platforms like it, as the core structures (news feed, timeline, groups, messenger) and the main ways people interact in it (post, like, share, message) did not change significantly since the time the data for this study were collected.

4.7.3 Conclusion

By using U.S. representative data, this study adds to a growing literature that confirms the privacy calculus in SNSs. The extended privacy calculus model is the first to integrate the theoretical tenets of both SNS self-disclosure and self-withdrawal into a single model. We believe that this novel integration is important. To illustrate consider the following figurative example from the context of automobiles: To date, separate strands of research have analyzed either how cars accelerate or how they slow down. However, research should now aim to advance theory by answering these related questions together within one single model (Popper, 1959/2005) because this offers the advantage to analyze influences that are either specific to both processes (e.g., engine / brakes) or more general (e.g., aerodynamic drag). Regarding SNSs, the extended privacy calculus model is the first integrated model to show that expected benefits are a specific influence for self-disclosure, whereas self-efficacy is a specific influence for self-withdrawal. Privacy concerns, adversely, influence both SNS self-disclosure and self-withdrawal. Overall, this study thus supports the basic tenets of privacy theory in SNSs (Petronio, 2012), finds further evidence against the privacy paradox, and proposes a novel extended privacy calculus model for SNSs.

Literature

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook 6* (pp. 206–249). Beverly Hills, CA: Routledge.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites. *Internet Research*, *25*(2), 279–299. doi:10.1108/IntR-09-2013-0192

Choi, Y. H. & Bazarova, N. N. (2015). Self-disclosure characteristics and motivations in social media: Extending the functional model to multiple social network sites. *Human Communication Research*, *41*(4), 480–500. doi:10.1111/hcre.12053

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*(3), 341–345. doi:10.1089/cpb.2008.0226

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

Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. doi:10.1002/ejsp.2049

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.

Homans, G. C. (1974). *Social behavior: Its elementary forms*. New York, NY: Harcourt Brace.

Hong, W. & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275–298.

Klein, C. T. & Helweg-Larsen, M. (2002). Perceived control and the optimistic bias: A meta-analytic review. *Psychology & Health*, *17*(4), 437–446. doi:10.1080/0887044022000004920

Korzaan, M. L. & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), 15–24.

Krämer, N. C. & Winter, S. (2008). Impression management 2.0. *Journal of Media Psychology*, *20*(3), 106–116. doi:10.1027/1864-1105.20.3.106

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

Krasnova, H., 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), 127–135. doi:10.1007/s12599-012-0216-6

Laufer, R. S. & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x

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

Little, T. D., Cunningham, W. A., Shahar, G., & Widaman, K. F. (2002). To parcel or not to parcel: Exploring the question, weighing the merits. *Structural Equation Modeling: A Multidisciplinary Journal*, *9*(2), 151–173. doi:10.1207/S15328007SEM0902{_}1

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

Marwick, A. E. & boyd d., d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. doi:10.1177/1461444814543995

Marwick, A. E. & boyd, d. m. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. doi:10.1177/1461444810365313

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00. doi:10.1111/j.1083-6101.2004.tb00292.x

Min, J. & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, *66*(4), 839–857. doi:10.1002/asi.23206

Mohamed, N. & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. doi:10.1016/j.chb.2012.07.008

Niemann, J. & Schenk, M. (2014). Niemann, J. & Schenk, M. (2014). Im Spannungsfeld zwischen Risiko und Nutzen Selbstoffenbarung auf Social-Networking-Sites. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis* (Vol. 41, pp. 207–223). Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft. Konstanz, Germany: UVK.

Park, Y. J. [Y. J.]. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. doi:10.1177/0093650211418338

Park, Y. J. [Yong Jin]. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. doi:10.1016/j.chb.2015.04.011

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Pew Research Center. (2015). Americans' attitudes about privacy, security and surveillance. Retrieved from www.pewinternet.org/2015/05/20/americans-attitudes-about-

Popper, K. (1959/2005). *The logic of scientific discovery*. New York, NY: Routledge.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo, R. E. Petty, & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–177). New York: Guilford Press.

Shibchurn, J. & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. *Computers in Human Behavior*, *44*, 103–117. doi:10.1016/j.chb.2014.10.059

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292. doi:10.1016/j.chb.2015.06.006

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. doi:10.1111/jcc4.12052

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Influence of social support received in online and offline contexts on satisfaction with social support and satisfaction with life: A longitudinal study. *Media Psychology*, *18*(1), 74–105. doi:10.1080/15213269.2013.838904

Utz, S. & Kramer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2). Retrieved from www.cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, *13*(2), 151–168. doi:10.1007/s10660-013-9111-6

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52. doi:10.1016/j.dss.2010.11.017

Zhang, Y. & Leung, L. (2015). A review of social networking service (SNS) research in communication journals from 2006 to 2011. *New Media & Society*, *17*(7), 1007–1024. doi:10.1177/1461444813520477

Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158–167. doi:10.1016/j.chb.2014.12.012

Study 4

5 “Nothing to hide”: Predicting the desire for privacy

Preamble

Abstract

Objective: This study analyzes how personality relates to peoples’ desire for privacy. Specifically, we investigated whether the syllogism “I don’t mind surveillance because I have nothing to hide” is correct: Do people who lack integrity (given they have something to hide) indeed desire more privacy?

Method: Study 1 featured an online questionnaire ($N = 268$, $M_{\text{age}} = 20$ years, 72% female) and Study 2 a laboratory experiment ($N = 87$, $M_{\text{age}} = 20$ years, 51% female), where participants wrote an essay about past negative, positive, or neutral behaviors to analyze effects on desire for privacy.

Results: Study 1 showed that respondents who are more shy, less anxious, and more risk averse desired more privacy. Respondents who self-reported lacking integrity reported desiring more privacy from government and more anonymity. Study 2 replicated these results and showed a statistical trend ($p = .052$) that writing about negative past behaviors increased desire for interpersonal privacy. Moreover, the integrity IAT showed significant relations with desire for privacy from government.

Conclusion: It is possible to predict peoples’ desire for privacy based on their lack of integrity. However, other neutral personality facets also explain desire for privacy. Hence, putting everyone who desires privacy under general suspicion would be incorrect.

Keywords: privacy, integrity, anonymity, personality, SEM

Status of publication

The study has already been submitted at an academic journal. At the time of the publication of this dissertation, the results of the first reviews had not yet arrived. If the manuscript should be accepted, the published text is likely going to differ from the text that is presented here due to further adjustments that might result from the review process.

5.1 Introduction

In his novel *The Circle*, Eggers (2013) describes a dystopian society in which people are gradually forfeiting their privacy. People decide to become "transparent", which means that they start carrying a small camera around the neck in order to broadcast their daily lives to the Internet. Eventually, this causes a societal upheaval: "The pressure on those who hadn't gone transparent went from polite to oppressive. The question, from pundits and constituents, was obvious and loud: If you aren't transparent, what are you hiding?" (Eggers, 2013, p. 129). The main argument being offered to justify the surveillance is: "If you have nothing to hide, you have nothing to fear." This syllogism is familiar, given that it commonly appears in also nonfictional conversations (Sieradski, 2013.08.06). Consider, for example, the following tweet: "I don't download illegally. I don't have anything on my comp[uter] to hide. Hell, I'm sure the #NSA gave up on me years ago." (Beautiful Disaster, 14.08.2015).

However, to date there is only little research on why people desire privacy and how the desire for privacy can be predicted by aspects of personality. More specifically, and to the best of our knowledge, so far no study exists that has analyzed the nothing-to-hide argument from a scientific and empirical perspective. Why do some people not care whether government agencies such as the NSA are collecting their data (G. Greenwald, 2013.06.06), and why do others protest vehemently in order to protect their privacy? Answering this question is important: Given that government agencies are collecting large amounts of data hoping to reduce criminality and terrorism, and given that government agencies are collecting this data preemptively and without concrete suspicions, it is relevant to find out whether this practice of mass surveillance can be justified based on the nothing-to-hide argument. As a result, the main question of this paper is: Do people who desire more privacy really have more to hide and, more generally, what are personality facets that determine peoples' overall desire for privacy?

5.2 Theory

5.2.1 Desire for privacy

Privacy captures the extent of voluntary withdrawal from others (Westin, 1967). Several models suggest that privacy is a multi-dimensional concept: For example, in a theory-driven treatise Burgoon (1982) argued that privacy has four dimensions: informational, social, psychological, and physical privacy. Pedersen (1979), by contrast, did an empirical factor analysis (initially starting with 94 items) and suggested that privacy exists on six dimensions: reserve, isolation, solitude, intimacy with friends, intimacy with family, and anonymity. In addition, Schwartz (1968) differentiated between horizontal and vertical privacy: Whereas horizontal privacy captures withdrawal from peers, vertical privacy refers to withdrawal from superiors or institutions (e.g., government agencies). Next to being multi-dimensional, privacy is also contingent (Dienlin, 2014): One can, for example, distinguish between the objective privacy context, the subsequent subjective perception of privacy, the psychological desire for privacy (which is both a situational and dispositional need), and the resulting privacy behavior (as represented by self-disclosure). For the purpose of this study, we combine the aforementioned theories and focus on (a) vertical privacy with regard to the desire for withdrawal from government surveillance, (b) horizontal privacy in terms of the desire for withdrawal from peers, friends, or acquaintances, and (c) both horizontal and vertical privacy as captured by the general desire for anonymity.

5.2.2 Integrity

Which specific aspects of personality help predict desire for privacy? At its core, the nothing-to-hide argument implies that lack of integrity is an important predictor of why people desire privacy. This becomes especially apparent when we consider the definition of Solove's (2007) nothing-to-hide argument (notably, Solove is a strong critic of the nothing-to-hide argument):

> The NSA surveillance, data mining, or other government information gathering programs will result in the disclosure of particular pieces of information to a few government officials, or perhaps

> only to government computers. This very limited disclosure of the particular information involved is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information. (Solove, 2007, p. 753)

This definition helps illustrate the link between lack of integrity and desire for privacy: People who have "engaged in illegal activities" can be considered, by definition, to lack integrity (Paunonen, 2002), which is why they have a reason "to hide this information" (or, in other words, to desire more privacy). In terms of a scientific definition of integrity there is no real consensus, however most scholars agree that integrity "incorporates a tendency to comply with social norms, avoid deviant behavior, and embrace a sense of justice, truthfulness, and fairness" (Connelly, Lilienfeld, & Schmeelk, 2006, p. 82).

5.2.3 The relation between integrity and desire for privacy

Several theoretical arguments exist why lack of integrity might correlate with desire for privacy. In general, any self-disclosure is a potential risk because others might disagree, disapprove, or misuse the information in other contexts (Petronio, 2000). Privacy regulation theory showed that if self-disclosures are too risky, people raise their desired level of privacy, intensify their boundary regulation, and employ more mechanisms to seclude and protect themselves (Altman, 1976). In traditional contexts, this could range from moderate behaviors like closing doors, to extreme behaviors such as physically tossing someone out of the room (Altman, 1976). In modern contexts, protecting one's privacy can mean to avoid photographs or to deliberately shun public places that have surveillance cameras. People who have actually committed something bad, treacherous, or illegal become even more vulnerable and face a significant risk of self-disclosure, because others will surely disapprove of these activities (e.g., Petronio, 2000). Hence, the foregoing arguments illuminate an indirect link between integrity and desire for privacy: By definition, people who participate in negative activities are considered to lack integrity (Paunonen, 2002). People who have engaged in negative activities have, by definition, more to hide, and disclosures concerning those activities pose a high risk. Because of this increased risk, people will arguably desire more privacy, as a means to mitigate their felt risk (Altman, 1976). In this way, the current research extends Altman's privacy regulation theory (1976) by suggesting that lack of integrity is an important yet unexamined factor that could increase peoples' desired level of privacy.

A few studies can be found that imply a relation between privacy and integrity. For example, several studies found that surveillance reduces cheating behaviors (Corcoran & Rotter, 1987; Covey, Saladin, & Killen, 1989). Covey et al. (1989) asked students to solve an impossible maze. In the high surveillance condition, the experimenter stood in front of the students and closely monitored their behavior. In the low surveillance condition, the experimenter stood behind the students, did not monitor their behavior, and visual dividers were used to block the experimenter's view of the students. Results showed that students were more likely to cheat in the low surveillance condition, suggesting that in situations of surveillance (i.e., less privacy), people show fewer cheating behaviors (i.e., more integrity). Similarly, people are more likely to prevent others from stealing when security cameras are visible (van Bommel, van Prooijen, Elffers, & van Lange, 2014), which is also a sign of higher integrity. Next, in a longitudinal sample with 457 respondents in Germany (Trepte & Reinecke, 2013), people who reported needing more privacy were less satisfied with their lives ($r = -.47$), had more ($r = .41$) and less positive affect ($r = -.39$). More importantly however, people who felt they needed more privacy were also less authentic on their SNSs profiles ($r = -.48$) and less authentic in their personal relationships ($r = -.28$; Trepte & Reinecke, 2013). For example, people who agreed to items like "I do not talk about personal issues unless my conversation partner brings them up first" were more likely to report that their online profiles did not truly represent their personality. Given the argument that authenticity is a subset of integrity (Sheldon, 2004), we reason that the concept of integrity might relate to the desired level of privacy. Finally, Pedersen (1982) showed that three dimensions of need for privacy related to self-esteem: In his study with $N = 70$ undergraduate students, respondents who held a lower self-esteem were more reserved ($r = .29$), needed more anonymity ($r = .21$) and preferred solitude ($r = .24$). Granted, self-esteem and integrity are generally distinct concepts; however, Pedersen's specific operationalization of self-esteem integrated several aspects of integrity (e.g., by using items such as “moral, nice, fair, unselfish, good, honest, reputable, sane” to measure self-esteem). Thus, our overarching hypothesis is that people who lack integrity have a greater desire for privacy.

5.3 Study 1

In Study 1, we used a questionnaire-based design to analyze how lack of integrity and other personality facets relate to desire for privacy. In accordance with the reasoning mentioned above, we suggest that people with less integrity feel a greater desire for privacy. Specifically, we argue that integrity may relate to the desire for privacy from (a) government surveillance, as governments have the legitimate power to prosecute illegal activities. Next, we hypothesize that integrity relates to the desire privacy for (b) anonymity. Anonymity makes it more difficult for both legal and social agents to identify and address potential wrongdoers, which is why people with less integrity will prefer situations in which they are anonymous. Finally, lack of integrity likely also relates to an increased desire for privacy from (c) other people, as most other people will disapprove of immoral or illegal activities, and might reveal those activities to authorities.

> *Hypothesis 1*: People who feel lower in self-perceived integrity desire more privacy from government surveillance (H1a), more anonymity (H1b), and more privacy from other persons (H1c).

5.3.1 The relation between personality facets and privacy desire

Critics of the nothing-to-hide argument hold that people who desire privacy should not automatically be confronted with suspicion, and that privacy has several purposes that are not related to criminal behavior (e.g., Marlinspike, 13.06.2013). Westin (1967), for example, defined four primary purposes of privacy: (1) self-development (i.e., the integration of experiences into meaningful patterns), (2) autonomy (i.e., the desire to avoid being manipulated and dominated), (3) emotional release (i.e., the release of tension from social role demands), and (4) protected communication (i.e., the ability to foster intimate relationships). These are all important social factors for which people desire privacy. Hence, the argument is that people who desire privacy can have several legitimate reasons for doing so; reasons which are essential for psychosocial wellbeing and which relate to different factors of personality. Below, we thus explore other (neutral) aspects of personality that potentially predict desire for privacy. In order to be more precise, we follow the advice by Paunonen and Ashton (2001) and, instead of using generic personality factors as predictors, refer to specific personality facets.

First, we argue that people who are more reserved, who feel less comfortable in social situations, generally desire more anonymity and more interpersonal privacy. Given that privacy is, by definition, a voluntary withdrawal from society (Westin, 1967), we expect that people who are more reserved or more shy desire more privacy from others. Several empirical studies support this hypothesis: Extroverted people desire less privacy (Morton, 2013), people who describe themselves as introverted thinkers are more likely to prefer social isolation (Pedersen, 1982), and introverted people are more likely to report invasions of privacy (Stone, 1986). Finally, we did not find convincing theoretical and empirical arguments for why shyness should relate to an increased desire for privacy from government surveillance, which is why we did not include a hypothesis on this relation.

> *Hypothesis 2*: People who are more shy desire more anonymity (H2a) and more privacy from other persons (H2b).

Of course, there are also reasons why people might desire less privacy. Government agencies often curtail privacy with the aim to prevent crime: For example, the NSA's surveillance programs are often considered a direct response to the 9 / 11 terrorists attacks (G. Greenwald, 2013.06.06). It seems plausible that people who are more afraid of terrorist attacks are also more likely to consent to these surveillance programs, given that these programs promise to reduce the likelihood of future attacks. One can then argue that people who are afraid of terrorist attacks are also more afraid of threats overall, which is why we suggest that people who are, in general, more anxious desire less privacy from government surveillance and less anonymity. We did not include a hypothesis on the potential relation between anxiety and desire for interpersonal privacy. On the one hand, one could argue that people who are more anxious are more reserved, given that social interactions can pose significant risks (especially with strangers or weak ties; Granovetter, 1973). At the same time, one could suggest that especially those people who are more anxious desire less privacy from others (and especially their strong ties), in order to cope better with their daily challenges. At the end, given that we measure interpersonal privacy on a general level (and do not distinguish between desire for privacy from (a) weak ties and (b) strong ties), it seems plausible that both effects could cancel each other out.

> *Hypothesis 3*: People who are more anxious desire less privacy from government surveillance (H3a) and more anonymity (H3b).

Disclosing personal information always poses a certain risk, given that others can misuse self-disclosed personal information in different contexts, which can lead to severe consequences (Altman, 1976). Not everyone will feel intimidated by this hypothetical threat — except those who have a general tendency to avoid taking unnecessary risks. The most cautious strategy to minimize risks of personal self-disclosures would be, arguably, to keep as much information as possible private. Hence, we suggest that people who are, in general, more risk averse have a good reason to desire more privacy in all three aforementioned contexts.

> *Hypothesis 4*: People who are more risk averse desire more privacy from government surveillance (H4a), more anonymity (H4b), and more privacy from other persons (H4c).

The personal computer and the Internet have rendered the world increasingly digitized: Social interactions, purchases, and medical treatments nowadays all produce digital traces, which can be combined into accurate latent user profiles. Given the features of digital information (i.e., information is persistent, searchable, reproducible, and scalable; boyd, 2008), this allows for unprecedented ways and degrees of surveillance. Mark Zuckerberg famously observed that privacy is no longer a "social norm," rather that people share personal information (Johnson, 2010.01.11). Hence, in order to be part of contemporary life (e.g., by using SNSs), it seems necessary to give up some privacy. However, arguably not everyone is willing to pay that price, and especially people who are more conservative might prefer to stick to their usual routines and decide against giving up their privacy. This is supported by empirical research: Older people, who are generally less open and more traditional (Donnellan & Lucas, 2008), are more concerned about their privacy than younger people (Fife & Orjuel, 2012). Taken together, we suggest that people who are more traditional also desire more privacy in all three aforementioned contexts.

> *Hypothesis 5*: People who are more traditional desire more privacy from government surveillance (H5a), more anonymity (H5b), and more privacy from other persons (H5c).

5.3.2 Method

Procedure and participants

Participants were students from a university in the western U.S. who received course credit for taking part in the study. The sample consisted of $N = 296$ respondents, with an age that ranged from 18 to 56 years ($M = 20$ years). 72% of the respondents were female. The median participation time was 24 minutes. Regarding ethnicity, 37% of the respondents were Non-Hispanic White / Caucasian, 4% Black / African American, 21% Hispanic / Latino, 24% Asian / Pacific Islander, 0% Native American, 5% others, and 8% nonresponse.

Measures

Despite the fact that we mostly used well-established scales, confirmatory factor analyses (CFAs) showed that some of the original items had to be deleted in order to achieve adequate factorial validity. The final scales showed acceptable fit (CFI > .90, TLI > .90, RMSEA < .10, SRMR < .10), good composite reliability (REL(ω) > .60), and adequate convergent factorial validity (AVE > .50; see Table 5.1). Respondents answered all items on a 7-point Likert scale ranging from 1 (*strongly disagree*) to 7 (*strongly agree*).

The data, all items (including deleted ones), results of CFAs, item statistics, and distribution plots can be found in the online supplementary material.[1]

[1] https://osf.io/7ncpk/?view_only=38283fd9262646378e4ba1e19c9d707f

Lack of integrity Integrity measures the extent to which people comply with social norms and values. When measuring integrity, the question arises whether it is possible to measure integrity based on self-reports. Interestingly, integrity tests that are based on self-reports have been shown to work successfully, given that they can predict unwanted professional workplace behavior sufficiently (e.g., theft, drug and alcohol problems, or absenteeism; Ones, Viswesvaran, & Schmidt, 1993). In order to measure lack of integrity, we thus used 4 items of the subscale integrity of the Supernumerary Personality Inventory (Paunonen, 2002). An example item is "I don't think there's anything wrong with cheating a little on one's income tax forms."

Shyness Shyness captures whether people prefer to spend their time alone or in company. We measured shyness with 4 items of the inverted extraversion subscale gregariousness (Costa & McCrae, 1992). An example item is "I shy away from crowds of people."

Anxiety. Anxiety measures whether people are afraid of negative external influences. We measured anxiety with 4 items of the neuroticism subscale anxiety (Costa & McCrae, 1992). An example item is "I am easily frightened."

Risk avoidance. Risk avoidance captures whether people abstain from taking risks. We measured risk avoidance with 4 items of the conscientiousness subscale deliberation (Costa & McCrae, 1992). An example item is "I think twice before I answer a question."

Traditionalism. Traditionalism measures whether people prefer to stick with their usual routines. We measured traditionalism with 4 items of the inverted openness to experiences subscale actions (Costa & McCrae, 1992). An example item is "I'm pretty set in my ways."

Desire for privacy. We measured desire for privacy on three dimensions: (a) Desire for privacy from government surveillance, which represents the extent to which people want the government to abstain from collecting information about their personal life. One example item is "I feel the need to protect my privacy from government agencies." (b) Desire for anonymity, which measures the extent to which people feel the need to avoid identification("I need to be able to use a fake name on social network sites to preserve my privacy"). (c) Desire for privacy from other people, which measures the extent to which people want to withhold personal information from others("I don't feel the need to tell my friends all my secrets"). For each dimension, we used 3 self-developed items that build on prior studies (e.g., Masur, 2016).

Data analyses

All hypotheses were tested with structural equation modeling (SEM). To assess the SEM assumption of multivariate normality, we computed a multivariate Shapiro-Wilk normality test. The results showed a violation of multivariate normality ($W = 0.90$, $p < .001$), which is why we used the more robust Satorra-Bentler scaled test statistic as estimator. We treated missing data with casewise deletion and tested all hypotheses with a two-tailed $\mathrm{p} < .050$ significance level; values between $p = .050$ and $p = .010$ were considered trends toward significance. Regarding effect sizes, we classified regression coefficients with values exceeding $\beta = .10$ as small effects, $\beta = .30$ as medium effects, and $\beta = .50$ as large effects.

In order to estimate a convenient sample size for the SEM, we referred to the recommendations by Hair, Black, Babin, and Anderson (2010). For the design of this study, Hair et al. (2010) would recommend a sample size of $\mathrm{N} \geq 300$. We did not determine sample size based on a priori power analyses, because we analyzed a novel research question and no information on effect sizes was available. We decided against including social desirability as a control variable, because even though social desirability can affect answers to sensitive questions (de Jong, Pieters, & Stremersch, 2012), it is more likely to reflect a true personality trait than false answering behavior (de Vries, Zettler, & Hilbig, 2014). Likewise, we did not include demographic control variables such as age or education, because we used a typical student sample with little demographic variance. To analyze the data, we used the software R (R Core Team, 2016, version 3.3.0) for the analyses, alongside additional packages such as lavaan (Rosseel, 2012, version 0.5-20).

Table 5.1: Psychometric Properties and Factorial Validity of Variables

	M	*sd*	skew	curt	α	ω	ave	$p(\chi^2)$	cfi	rmsea
Privacy desire					.80	.83	.46	<.01	0.93	0.08
Government	4.09	1.3	-0.15	-0.25						
Anonymity	2.96	1.18	0.47	-0.11						
Interpersonal	4.23	0.96	-0.05	0.14						
Lack of integrity	2.61	1.17	0.39	-0.67	.78	.78	.47	.15	0.99	0.06
Shyness	3.07	1.09	0.44	0.11	.78	.78	.48	.02	0.98	0.10
Fearfulness	4.28	1.13	-0.21	-0.37	.76	.76	.44	.03	0.98	0.09
Risk avoidance	4.75	1.01	-0.69	1.23	.75	.75	.44	.73	1	<.01
Traditionalism	4.72	0.99	-0.33	0.28	.76	.76	.44	.06	0.99	0.08

5.3.3 Results

Model fit and factorial validity

In reference to the usually recommended fit criteria (e.g., Hair et al., 2010), the SEM showed acceptable fit (χ^2 (349) = 491.38, $p < .001$, CFI = 0.92, TLI = 0.91, RMSEA = 0.04, SRMR = 0.05), acceptable total convergent factorial validity (AVE = .45), and good total internal consistency ($\omega = .86$).

Hypotheses

The data confirmed Hypothesis 1a: Respondents who self-reported lower integrity were less willing to accept government surveillance ($b = 0.20$, $\beta = .18$, $p = .022$). The effect size was small. The data also confirmed Hypothesis 1b: Respondents who reported being of lower integrity were less willing to identify themselves in various contexts ($b = 0.40$, $\beta = .43$, $p < .001$). The effect size was medium. The data did not confirm Hypothesis 1c: Respondents who reported lower integrity were not more willing to withhold information about themselves from other people ($b = 0.10$, $\beta = .16$, $p = .085$). However, the *p*-value .085 showed a trend toward significance.

Results supported H2: People who reported being more shy also reported desiring more anonymity (H2a; $b = 0.18$, $\beta = .19$, $p = .035$; small effect) and more privacy from other persons (H2b; $b = 0.21$, $\beta = .33$, $p = .002$; medium effect). As expected, respondents who were more shy did not desire more privacy from the government ($b = 0.15$, $\beta = -.13$, $p = .134$).

Table 5.2: Personality Facets as Predictors of (1) Privacy Desire Government, (2) Privacy Desire Anonymity, and (3) Privacy Desire Interpersonal

	b	(LL)	(UL)	*se*	*p*	β
Privacy desire government						
Lack of integrity	0.20	0.05	0.35	0.08	.022	.18
Shyness	0.15	-0.02	0.32	0.09	.134	.13
Fearfulness	-0.30	-0.47	-0.13	0.09	.004	-.26
Risk avoidance	0.23	0.05	0.41	0.09	.031	.21
Traditionalism	0.13	-0.06	0.32	0.10	.256	.11
Privacy desire anonymity						
Lack of integrity	0.40	0.23	0.57	0.09	<.001	.43
Shyness	0.18	0.01	0.35	0.09	.035	.19
Fearfulness	-0.16	-0.35	0.03	0.10	.089	-.17
Risk avoidance	0.09	-0.10	0.28	0.10	.288	.10
Traditionalism	<0.01	-0.21	0.21	0.10	.991	<.01
Privacy desire interpersonal						
Lack of integrity	0.10	-0.07	0.27	0.09	.085	.16
Shyness	0.21	0.03	0.39	0.09	.002	.33
Fearfulness	0.02	-0.17	0.21	0.10	.686	.04
Risk avoidance	0.20	-0.01	0.41	0.11	.003	.34
Traditionalism	0.10	-0.12	0.32	0.11	.177	.16

The data confirmed H3a: People who are generally more anxious desired less privacy from government surveillance ($b = 0.30$, $\beta = -.26$, $p = .035$; small effect). Regarding H3b, results showed a statistical trend that fearfulness was associated with reduced desire for anonymity ($b = 0.16$, $\beta = -.17$, $p = .089$; small effect). As expected, we found no significant relation with desire for interpersonal privacy ($b = 0.03$, $\beta = .04$, $p = .686$).

Results supported hypothesis H4a and H4b: Respondents who were more likely to report avoiding risks also reported desiring more privacy from government surveillance ($b = 0.23$, $\beta = .21$, $p = .031$; small effect) and from other persons ($b = 0.20$, $\beta = .34$, $p = .003$; medium effect). Risk avoidance was not related to desire for anonymity (H4c; $b = 0.09$, $\beta = .10$, $p = .288$).

Results did not confirm H5: Respondents who reported being more traditional did not desire more privacy from government surveillance (H5a; $b = 0.13$, $\beta = .11$, $p = .256$), did not desire more anonymity (H5b; b < .01, $\beta < .01$, $p = .991$), and also did not desire more privacy from other persons (H5c; $b = 0.10$, $\beta = .16$, $p = .177$).

For an overview of all results, see Table 5.2 and Figure 5.1.

5.3.4 Discussion

The results of Study 1 showed that integrity relates to several dimensions of desire for privacy: People who reported being of lower integrity desired more privacy from government and more anonymity. In other words, people who agreed that there would be nothing wrong with cheating a little or lying occasionally were also more likely to agree that the government should not invade peoples' privacy, even if that could help to prevent terrorist attacks. Likewise, people who said, for example, that they would feel tempted to take things that do not belong to them were also more likely to avoid situations in which they were identifiable.

In addition, desire for privacy was predicted also by other (neutral) personality facets: People who were more shy, more risk averse, and less anxious also desired more privacy. This implies that next to lack of integrity there are various other personality-related aspects that predict desire for privacy.

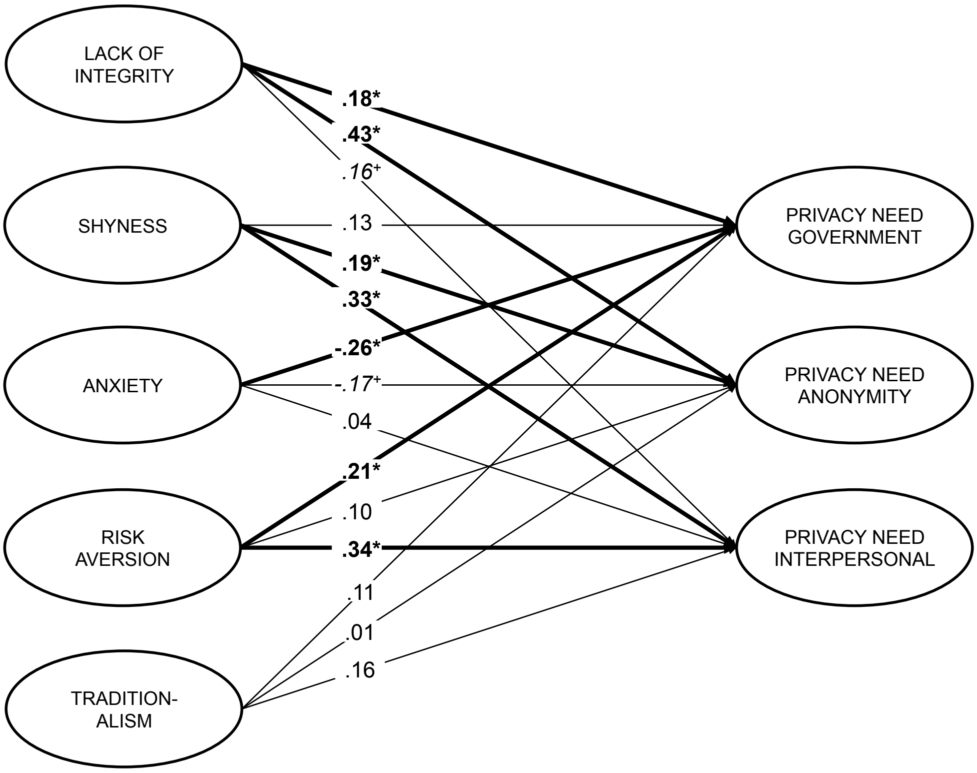

Figure 5.1: Study 1. Model shows relations between personality facets and desire for privacy. + $p \leq .10$, * $p \leq .05$.

5.4 Study 2

Using an experimental design, Study 2 aimed to replicate and expand the findings of Study 1. First, we tested the robustness of our finding that integrity relates to privacy by again analyzing self-reported integrity as a predictor of desire for privacy. Second, we analyzed the relations' generalizability by using a different way to measure self-perceived integrity. Next to an indirect self-report of integrity, we now included an implicit association test (IAT; Fischer & Bates, 2008, April) as an additional objective measure of integrity. The integrity IAT shares comparatively little statistical variance with other self-reported measures of integrity (Fischer & Bates, 2008, April), implying that the IAT measures a different latent construct. At the same time, when being used together with self-reports the integrity IAT was shown to significantly increase explained variance of actual cheating behaviors (Fischer, Thompson, & Turner, 2012, April). This suggests that although the IAT and the self-reports measure different facets of integrity, taken together they can help predicting integrity related outcomes, such as desire for privacy.

Third, we conducted an experiment in order to analyze whether people's desired level of privacy can be influenced by concrete integrity-related behaviors. If so, this would corroborate Study 1's hypothesized causality, which is that aspects of integrity influence desired levels of privacy (and not vice versa). In theory, one might use an experimental design in which one group of participants engage in negative or deceitful behaviors and another group in positive or benevolent behaviors to see whether this would affect subsequent levels of desire for privacy. In practice, however, several ethical reasons argue against this procedure, which is why we focused on a more implicit integrity-related task. In our manipulation, we asked participants to write an essay about past events in which they behaved either (a) positively or (b) negatively. We reasoned that if people write about negative behaviors they might believe they have something to hide and hence feel an increased desire for privacy, whereas if people believe that they have nothing to hide they might feel a lower desire for privacy. This led to the following new set of hypotheses:

> *Hypothesis 1*: Compared to a control group, participants who write an essay about past negative behaviors desire more privacy from government (H1a), more anonymity (H1b), and more interpersonal privacy (H1c).
>
> *Hypothesis 2*: Compared to a control group, participants who write an essay about past positive behaviors desire less privacy from government (H2a), less anonymity (H2b), and less privacy from other people (H2c).
>
> *Hypothesis 3*: People who feel lower in self-perceived integrity (as evidenced with a self-report) desire more privacy from government surveillance (H3a), more anonymity (H3b), and more interpersonal privacy (H3c).
>
> *Hypothesis 4*: People who feel lower in self-perceived integrity (as evidenced with an IAT) desire more privacy from government surveillance (H4a), more anonymity (H4b), and more interpersonal privacy (H4c).

H1 and H2 argue that the essay tasks have a direct influence on the desire for privacy. However, it also seems possible that this effect is mediated through self-perceived integrity. That is, because of having written an essay about negative past behavior people first think that they have less integrity, which then increases their desired level of privacy. On the other hand, one can also argue that self-perceived integrity is a stable trait-like concept that cannot be changed by means of a short essay task, which would argue against mediation. Hence, given that both options seem possible, we will analyze this notion in a first research question.

In Study 1, we did not analyze other negative personality factors next to lack of integrity, factors that could also explain why people desire privacy. For example, referring to the dark triad (Paulhus & Williams, 2002), it could be that people desire privacy (a) to be capable of manipulating others, (b) because they are excessively egocentric and want more room for themselves, or (c) because they lack empathy and do not want to connect with others. Hence, in research question two we analyze if the dark triad are further predictors of the desire for privacy.

5.4.1 Method

Procedure and participants

The data were collected between May and August 2015 with a laboratory experiment. The experimental manipulation was modeled after Reed and Aspinwall (1998).[2] In the positive essay group, we asked participants to write about some past behavior that they felt demonstrated high integrity (e.g., "Please describe a situation in which you demonstrated high integrity, for example, you donated something for reasons of charity"). In the negative essay group, we asked participants to write about some past behavior that they felt reflected low integrity (e.g., "Please describe a situation in which you demonstrated low integrity, for example, you lied because doing so benefitted you"). In the control group, we asked participants to write about something that was irrelevant to integrity ("Please describe the room you are currently sitting in"). Participants had 15 minutes to complete their essay. Afterwards, we measured self-perceived integrity by means of an IAT of integrity (Fischer & Bates, 2008, April). Participants then filled out a questionnaire regarding their self-reported integrity, their personality, and their desire for privacy. Finally, we allowed participants to destroy their own essay if they wanted to, and debriefed them regarding the research questions and the manipulation procedure. We asked if participants had guessed the purpose of the study and assured them that assignment to one of the groups did not reflect their integrity or personality. IRB approval was obtained for this study before any data were collected.

Participants were students from a university in the western U.S. Participants received course credit for taking part in the study. With regard to sample size, again no information on effect size was available beforehand, which is why we referred to a conventional group size of $n = 30$. The final sample consisted of $N = 87$ participants, randomly assigned to three experimental groups (negative: $n = 30$; neutral: $n = 27$; positive: $n = 30$). Participants' age ranged from 18 to 34 ($M = 20$), 51% of the participants were female, and the median for participation time was 44 minutes. Regarding ethnicity, 40%

[2] Reed and Aspinwall (1998) tested whether a positive experience (the endorsement and recall of one's past acts of kindness) would decrease biased processing of self-relevant health-risk information.

of the respondents were Non-Hispanic White / Caucasian, 2% Black / African American, 22% Hispanic / Latino, 23% Asian / Pacific Islander, and 13% reported "other" as their ethnicity.

Material

We developed new items alongside those of Study 1 in order to be able to exchange potentially malfunctioning items. The final scales showed acceptable fit, good composite reliability, and adequate convergent factorial validity (see Table 5.3).

Lack of integrity self-report We used the same 4 items as in Study 1 to measure self-reported lack of integrity. Again, the scale showed good factorial validity.

Lack of integrity IAT The integrity IAT is an indirect and implicit way to measure self-perceived integrity (Fischer & Bates, 2008, April). The IAT consists of two categories: the target category "self" (me, my, mine, self, and I) and the control category "other" (them, their, theirs, other, and they). In addition, the IAT features two attributes: the positive attribute "honest" (fair, integrity, sincere, trustworthy, truthful, and moral) and the negative attribute "dishonest" (unfair, steal, deceive, cheat, lie, and corrupt). Based on response time differentials, the IAT measures associations between categories and attributes: Participants who perceive themselves to have higher integrity associate the category "self" more readily with "honest" than they do "self" and "dishonest". We computed the IAT results based on the p1311-procedure as recommended by Richetin, Costantini, Perugini, and Schönbrodt (2015). We inverted the final scale in order to measure lack of integrity.

The dark triad In order to measure Machiavellianism, psychopathy, and narcissism, we used the Dirty Dozen scale by Jonason and Webster (2010). Machiavellianism measures how strongly people try to manipulate others toward their own ends. One example item is "I tend to manipulate others to get my way." Psychopathy captures whether people tend to lack empathy and do not reflect on their own behavior ("I tend to be unconcerned with

Table 5.3: Study 2: Psychometric Properties and Factorial Validity of Variables

	M	*sd*	skew	curt	α	ω	ave	p(χ^2)	cfi	rmsea
Privacy desire					.76	.82	.49	<.04	0.92	.08
Government	4.44	1.30	-0.04	-0.35						
Anonymity	2.36	0.90	0.30	-0.80						
Interpersonal	4.15	1.26	-0.23	0.23						
Lack of integrity										
Self-report	2.53	1.15	0.57	-0.30	.68	.70	.39	.90	1.12	<.01
IAT	-0.29	0.26	0.57	-0.03						
Dark triad					.70	.81	.53	.29	0.98	.05
Machiavellianism	3.43	1.62	0.20	-0.90						
Psychopathy	2.96	1.38	0.52	-0.27						
Narcisissim	4.72	1.30	-0.56	-0.57						

the morality of my actions"). Narcissism measures whether people are excessively self-centered and expect to receive special attention from others ("I tend to want others to admire me"). Despite being a well-established scale, we could only represent the dark triad's three dimensional factorial structure in a well-fitting way when using 2 items for each factor (instead of 4; see online material). Hence, overall we used 6 items (2 for each dimension).

Privacy desire We used the same items as in Study 1, except that we also adopted 3 newly developed items to measure desire for anonymity (e.g., "I want to be able to surf the Internet anonymously"), given that the prior items did not show optimal fit (see online material).

Data analyses

As in Study 1, we used SEM to analyze the data. Again, the data violated the assumption of multivariate normality ($W = 0.83, p < .001$), so we used the more robust Sartorra-Bentler estimator. We modeled the manipulation as a dummy variable and computed two contrasts: In contrast one, we compared the positive essay group to the control group, and in contrast two, we compared the negative essay group to the control group.[3]

[3] There is no statistical difference between analyzing experiments with ANOVAs and GLMs (Cohen, 1968). We decided to use SEMs (which are GLMs), because they provide several advantages (e.g., they allow measurement of latent constructs in complex models). When analyzing experiments within GLMs, the different conditions are included as dummy

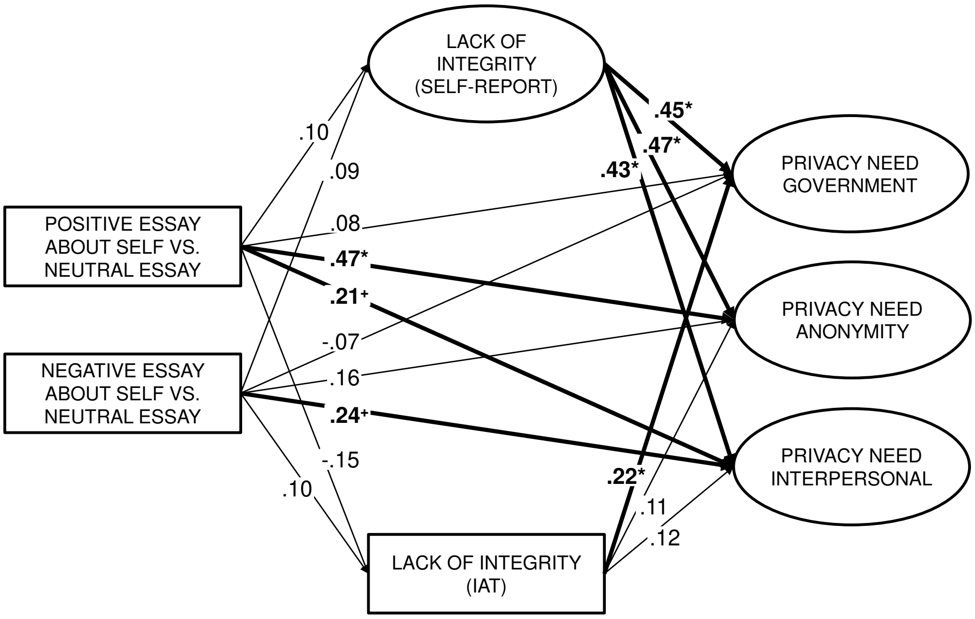
LACK OF INTEGRITY (SELF-REPORT)
POSITIVE ESSAY ABOUT SELF VS. NEUTRAL ESSAY
NEGATIVE ESSAY ABOUT SELF VS. NEUTRAL ESSAY
LACK OF INTEGRITY (IAT)
PRIVACY NEED GOVERNMENT
PRIVACY NEED ANONYMITY
PRIVACY NEED INTERPERSONAL
.10
.09
.08
.47*
.21+
-.07
.16
.24+
-.15
.10
.45*
.47*
.43*
.22*
.11
.12

Figure 5.2: Study 2. Model 1 shows the results of Hypotheses 1a, 1b, 1c and 2a, 2b, 2c. Model 2 shows the results of Hypotheses 3a, 3b, 3c. In the positive group, participants wrote an essay about positive past behaviors, in the negative group about negative behaviors. In the control group, participants wrote a neutral essay that described the room they were sitting in. + $p \leq .10$, * $p \leq .05$.

5.4.2 Results

Model fit and factorial validity

The SEM showed acceptable fit (χ^2 (167) = 198.65, p = .048, CFI = 0.92, TLI = 0.89, RMSEA = 0.05, SRMR = 0.07), adequate total convergent factorial validity (AVE = .49), and good total internal consistency (ω = .83).

In our experimental design, we followed the recommendation of O'Keefe (2003) and did not define our manipulation in terms of its effects on a psychological state (here, self-perceived integrity). Instead, we used a manipulation with intrinsic features and external validity (essay task). As a result, there was no need include a manipulation check (O'Keefe, 2003).

Hypotheses

The data did not confirm Hypothesis 1a and 1b, which predicted that participants who were in the negative essay group would desire more privacy from government (M_{neg} = 0.06; M_{con} = -0.07; b = -0.18, β = -.07, p = .633) and more anonymity (M_{neg} = 0.01; M_{con} = -0.15; b = 0.46, β = .16, p = .219). However, regarding H1c, which predicted that participants who were in the negative essay group would desire more interpersonal privacy, the data showed a statistical trend (M_{neg} = 0.46; M_{con} = -0.39; b = 0.70, β = .24, p = .052). This implies that participants who reflected about past behavior showing low integrity indicated they would generally want more privacy from other people.

The data did not confirm Hypothesis 2a, 2b, and 2c. H2a predicted that participants who wrote an essay about positive past behaviors would desire less privacy from government, which was not confirmed by the data (M_{pos} = 0.01; M_{con} = -0.07; b = 0.22, β = .08, p = .618). Regarding H2b and H2c, results actually showed the opposite: Participants who reflected upon past positive behaviors actually desired more anonymity afterwards (H2b; M_{pos} = 0.49; M_{con} = -0.56; b = 1.33, β = .47, p = .003). There was also a statistical trend that

variables / contrasts (here: pos. vs. con; neg. vs. con). In the results section, we reported the latent factor means. For using contrasts to model experimental designs in GLMs, see Field, Miles, and Field (2012).

Table 5.4: Study 2: Predictors of (1) Privacy Desire Government, (2) Privacy Desire Anonymity, (3) Privacy Desire Interpersonal, Lack of Integrity (self-report and IAT), and the Dark Triad

	b	(LL)	(UL)	*se*	*p*	β
Privacy desire government						
Lack of integrity (self-report)	0.52	0.22	0.82	0.15	.008	.45
Lack of integrity (IAT)	1.11	0.89	1.33	0.11	.043	.22
Positive essay	0.22	-0.09	0.53	0.16	.618	.08
Negative essay	-0.18	-0.45	0.09	0.14	.633	-.07
Machiavellianism	-0.63	-1.15	-0.11	0.27	.039	-.58
Psychopathy	0.79	0.33	1.25	0.24	.023	.57
Narcissism	-0.12	-0.49	0.25	0.19	.659	-.09
Privacy desire anonymity						
Lack of integrity (self-report)	0.56	0.20	0.92	0.18	.013	.47
Lack of integrity (IAT)	0.57	0.36	0.78	0.11	.321	.11
Positive essay	1.33	1.03	1.63	0.15	.003	.47
Negative essay	0.45	0.20	0.70	0.13	.219	.16
Machiavellianism	-0.90	-1.53	-0.27	0.32	.014	-.81
Psychopathy	0.74	0.28	1.20	0.23	.023	.52
Narcissism	0.38	-0.02	0.78	0.21	.171	.27
Privacy desire interpersonal						
Lack of integrity (self-report)	0.53	0.22	0.84	0.16	.011	.43
Lack of integrity (IAT)	0.63	0.42	0.84	0.11	.257	.12
Positive essay	0.61	0.37	0.85	0.12	.068	.21
Negative essay	0.70	0.46	0.94	0.12	.052	.24
Machiavellianism	-0.17	-0.63	0.29	0.23	.531	-.15
Psychopathy	0.64	0.22	1.06	0.21	.054	.43
Narcisissim	0.20	-0.01	0.41	0.11	.060	.34
Lack of integrity (self-report)						
Positive essay	0.23	-0.47	0.92	0.35	.522	.10
Negative essay	0.22	-0.45	0.88	0.34	.523	.09
Lack of integrity (IAT)						
Positive essay	-0.08	-0.21	0.04	0.07	.202	-.15
Negative essay	0.05	-0.09	0.19	0.07	.453	.10
Machiavellianism						
Positive essay	0.17	-0.57	0.92	0.38	.649	.07
Negative essay	0.06	-0.61	0.73	0.34	.867	.02
Psychopathy						
Positive essay	-0.11	-0.70	0.48	0.30	.708	-.06
Negative essay	0.18	-0.47	0.82	0.33	.594	.09
Narcissism						
Positive essay	-0.32	-0.92	0.29	0.31	.309	-.15
Negative essay	-0.31	-0.85	0.22	0.27	.253	-.15

after having written an essay about positive past behaviors, participants desired more privacy from other people (H2c; $M_{\text{pos}} = 0.09$; $M_{\text{con}} = -0.61$; $b = 0.61$, $\beta = .21$, $p = .068$).

The data confirmed Hypothesis 3a, 3b, and 3c: Participants with higher self-reported lack of integrity desired more privacy from government (H3a; $b = 0.52$, $\beta = .45$, $p = .008$), more anonymity (H3b; $b = 0.56$, $\beta = .47$, $p = .013$), and more interpersonal privacy (H3c; $b = 0.54$, $\beta = .43$, $p = .011$). All three effects were medium to large-sized.

Concerning H4a, results confirmed that participants whose IAT showed higher lack of integrity desired more privacy from government ($b = 1.11$, $\beta = .22$, $p = .043$). The effect was small. Hypotheses 4b and 4c, which predicted that participants with lower integrity IATs would desire more anonymity and more interpersonal privacy, were not supported (H4b; $b = 0.57$, $\beta = .11$, $p = .321$; H4c; $b = 0.63$, $\beta = .12$, $p = .257$).

In research question one, we analyzed if the essay tasks changed levels of self-perceived lack of integrity. Results showed that essay tasks did not affect participants' self-perceived lack of integrity (both self-report and IAT; see Table 5.4).

The results of research question two showed several significant relationships of the dark triad with desire for privacy: Contrary to expectation, participants who had higher results in Machiavellianism desired less privacy from government ($b = -0.63$, $\beta = -0.58$, $p = .039$) and less anonymity ($b = -0.90$, $\beta = .81$, $p = .014$). As expected, higher levels of psychopathy were related to an increased desire for privacy from the government ($b = 0.79$, $\beta = .35$, $p = .023$) and for anonymity ($b = 0.74$, $\beta = .52$, $p = .023$). Narcissism was not related to the desire for privacy.

For an overview of the results, see Table 5.4 and Figure 5.2.

5.4.3 Discussion

The analyses of Study 2 replicated several findings of Study 1. Results again showed that people who self-reported lacking integrity indeed desired more privacy. Study 2 evidenced this relation not only regarding desire for privacy from government and regarding desire for anonymity (as was shown in Study 1), but also for the desire for privacy from other people. In addition, an IAT of integrity also confirmed that lack of integrity corresponds with a higher desire for privacy from government: People who were quicker to associate words such as unfair, steal, deceive, cheat, lie, and corrupt with themselves reported an increased desire to protect their privacy from the government. In addition, results of research question two showed that the desire for privacy can also be affected by other negative personality traits. For example, people who have higher levels of psychopathy also desire more privacy from government surveillance.

Next, the experimental setting revealed a statistical trend that people who reflected upon past behavior that showed low integrity reported desiring more privacy from other people. This implies that people seem to withdraw from others when they are reminded of their own negative behaviors of the past. Interestingly, we also found that when people reflect upon past behaviors that are positive they desire more anonymity and (potentially) more privacy from other persons. On the one hand, this seems counterintuitive as one might believe that people would rather want to tell others about their good deeds, which is something they can only do when they forfeit their privacy by self-disclosing. On the other hand, there are also reasons why desiring more privacy after having reflected upon positive aspects is plausible. For example, we find a similar pattern when we look at personal diaries: Here, the author keeps note of moments he or she treasures and which the author does not want to forget. Beside the fact that these moments are often positive, they also have another feature: They are personal, even intimate. In our positive essay task, respondents might have realized just that, which could be an explanation why they afterwards desired more privacy. So far, we know at least that the effect was not mediated through lower levels of self-perceived integrity (see research question one). Hence, it is still worthwhile to keep on looking for other potential mediators. Taken together, results imply that reflecting about both positive and negative past behavior can increase the desire for privacy.

5.5 General discussion

5.5.1 Implications

This paper analyzed why people desire privacy and whether there is some truth to the nothing-to-hide argument, which argues that people desire privacy because they lack integrity. Indeed, Study 1 supports that people who report lacking integrity — in other words, people who might have something to hide — desire more privacy from government and more anonymity. Study 2 replicated this finding, which, taken together, implies that the relation can be considered robust. Similarly, taking into account that strong effects are not very common in socio-psychological research, it is notable that 4 out of 6 relations between self-reported integrity and privacy were medium- to large-sized — which again underscores the relationship's robustness. Finally, given that we found several significant relations with the dark triad, the results also suggest that it would be promising to further elaborate on which negative aspects of personality exactly make people desire more privacy; results suggested that people with higher levels in psychopathy desire more privacy. Interestingly, some negative aspects of personality might also reduce desire for privacy, given that people who reported higher levels of Machiavellianism desired less privacy. In conclusion, our studies support that there is some truth to the implicit premise behind the nothing-to-hide argument: People who want more privacy also seem to have more things that they might wish to hide — in this study, this included things such as (minor) theft, tax evasion, or leaving a restaurant without paying the bill.

Notably however, the results showed that lack of integrity is not the only aspect of personality why people desire privacy. That is, people who are more shy, more risk averse, or less anxious also desire more privacy. For example, people who are less anxious are less likely to accept government surveillance (arguably because they are less afraid of terrorist attacks). When looking at the bigger implications of the results, this shows the importance to make differentiated claims on why people desire privacy: Indeed, the results suggest that some people desire privacy because they might have something to hide. However, putting everyone who desires privacy under a general suspicion is wrong given that shy, risk averse, and less anxious people are also more likely to desire privacy.

Next, Study 2 suggests that desire for privacy relates to implicit measures of integrity, given that participants who had lower integrity as indicated by an IAT reported desiring more privacy from government surveillance. This shows that even when we measure integrity with a different, arguably more objective approach, we can still find a significant relation between self-perceived lack of integrity and desire for privacy. Moreover, Study 2 offers another perspective that adds to the generalizability of the relation between integrity and privacy: That is, when people write an essay about negative past behavior, it is likely that this increases their desired level of interpersonal privacy. Interestingly, the results also suggest that when people reflect upon positive past behavior, this increases desired levels of anonymity and interpersonal privacy.

In conclusion, our results follow Altman (1976), who reasoned that if exposure of information is risky it is likely that people will use more mechanisms to strengthen their social boundaries and increase their desired level of privacy. This study thus aligns with Altman's privacy regulation theory by showing that, in several contexts, people with lower integrity had a higher level of desired privacy.

5.5.2 Limitations and future perspective

In our analysis of predictors of privacy, we followed the recommendation by Paunonen and Ashton (2001) and did not analyze broad factors of personality (e.g., neuroticism); instead, we focused on more specific personality facets (e.g., fearfulness). For future research, we suggest going one step further by analyzing predictors that are even more specified. For example, it seems possible that people who hold dissenting political beliefs could also have a higher desire for privacy from the government. Similarly, it would be interesting to focus on different minority groups. For example, it seems plausible that people from a LGBT background might desire more privacy from government (because it is potentially repressive or unfriendly toward LGBTs). Finally, in this study we focused mostly on escapist motives for why people desire privacy (e.g., shyness, risk aversion). Interestingly, Leary, Herbst, and McCrary (2003) were able to show that when predicting engagement in solitary activities, it is less preferable to measure how strongly people want to escape society (avoidance oriented), but rather how much they seek solitude (approach oriented). Hence, future studies might want to include predictors that are more approach oriented (e.g., peoples' desire for contemplation).

To our knowledge, this is the first study that used essay tasks to change peoples' desire for privacy. On the whole, the approach proved valuable. We now suggest further optimizing the experimental manipulation in order make the manipulation stronger; for example, by using additional ease-of-retrieval tasks (e.g., Tormala, Petty, & Brinol, 2002). Similarly, we recommend making the essay task more specified: We suggest that participants elaborate on past behaviors that focus on either legal aspects (e.g., "When was the last time you did something that was probably against the law?") or on social aspects (e.g., "When was the last time that you lied to one of your friends?").

From a methodological perspective, future research should continue to improve the instruments we used, given that factorial validity of some scales was only moderate. Similarly, we recommend elaborating on the general understanding of integrity as a theoretical concept. To date, there is not one overarching concept of integrity that incorporates all the different aspects of integrity, yet it would be valuable to examine how other aspects of integrity (e.g., authenticity, trustworthiness, or consistency) relate to privacy desires.

The manipulation produced small to medium-sized effects ($\beta \approx .20$). Power analyses showed that future research should use samples above $N \approx 260$ in order to test hypotheses with the recommended power of at least .80 (Cohen, 1992). In Study 2, we tested some hypotheses with a power of approximately .60, which is relatively low and might explain why some effects were not significant. Besides, SEM stability would benefit from using larger samples.

In general, the question arises whether it is possible, or even socially desirable, to measure a person's integrity. On the one hand, integrity implies absolute criteria: Stealing is bad and forbidden, whereas helping is good and encouraged. On the other hand, integrity implies relative criteria: Whereas some cultures disapprove of lying whatever the context, others consider lying okay — for example "white lies" in order to save face or to avoid hurting someone's feelings (Altman, 1977). Thus, ranking behaviors, opinions, and character traits with regard to integrity is a moral dilemma. As a result, throughout the entire study we have understood integrity as a transgression of social norms that is strong and that most societies would agree upon (for example, most societies would consider stealing as a sign of low integrity).

As a final note, we measured integrity based on self-ratings. One can criticize this approach by saying it is not possible to measure integrity based on self-reports because of social desirability influences. However, self-reports of integrity can indeed predict malevolent behavior: In a meta-analysis with 665 correlation coefficients, integrity tests related to counterproductive behaviors with a coefficient of $r = .47$ (Ones et al., 1993). Also, the implicit measure we used is much less vulnerable to social desirability (A. G. Greenwald, Nosek, & Banaji, 2003). Nonetheless, future research would benefit from including behavioral manifestations of integrity, such as concrete cheating behaviors. If concrete cheating behaviors also increase desires for privacy, this would strengthen the underlying premise of the nothing-to-hide argument.

5.5.3 Conclusion

In his paraphrase of the nothing-to-hide argument, Daniel Solove ends as follows: "Although there may be some cases in which the information might be sensitive or embarrassing to law-abiding citizens, the limited disclosure lessens the threat to privacy. Moreover, the security interest in detecting, investigating, and preventing terrorist attacks is very high and outweighs whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information." (Solove, 2007, p. 753). It seems plausible that at some point, society has a justified interest in limiting privacy in order to prevent crime and to improve public safety (e.g., by wiretapping concrete suspects or by having trials that are public), given that privacy, obviously, offers opportunities for immoral, malevolent, and illegal behavior. And the results of this study offer further support for this hypothesis because, in both studies, people's desire for privacy could indeed by predicted by peoples' lack of integrity.

At the same time, it would be wrong to monolithically claim that all people who desire privacy always have something to hide. By contrast, results showed that people who desire more privacy can also be more shy, more risk averse, and less anxious. Or, it could also be that they have just been reflecting upon some specific past negative of good behaviors. Hence, results do not imply that privacy is bad per se or that it is always alright to limit privacy. On the contrary, we stress that everyone needs privacy in order to be able to think freely, to act autonomously, to be authentic, to relax, to become intimate, and to foster social support (Westin, 1967).

Literature

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, *8*(1), 7–29. doi:10.1177/001391657600800102

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84. doi:10.1111/j.1540-4560.1977.tb01883.x

Beautiful Disaster. (14.08.2015). I don't download illegally. I don't have anything on my comp to hide. Hell, I'm sure the #NSA gave up on me years ago [Tweet]. Retrieved from https://twitter.com/IdiosynCyto/status/632250548553695232

boyd, d. m. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13–20. doi:10.1177/1354856507084416

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook 6* (pp. 206–249). Beverly Hills, CA: Routledge.

Cohen, J. (1968). Multiple regression as a general data-analytic system. *Psychological Bulletin*, *70*(6, Pt.1), 426–443. doi:10.1037/h0026714

Connelly, S., Lilienfeld, S. O., & Schmeelk, K. M. (2006). Integrity tests and morality: Associations with ego development, moral reasoning, and psychopathic personality. *International Journal of Selection and Assessment*, *14*(1), 82–86. doi:10.1111/j.1468-2389.2006.00335.x

Corcoran, K. J. & Rotter, J. B. (1987). Morality-conscience guilt scale as a predictor of ethical behavior in a cheating situation among college females. *The Journal of General Psychology*, *114*(2), 117–123. doi:10.1080/00221309.1987.9711061

Costa, P. T. & McCrae, R. R. (1992). *Revised NEO Personality Inventory (NEO PI-R) and NEO Five Factor Inventory. Professional manual.* Odessa, FL: Psychological Assessment Resources.

Covey, M. K., Saladin, S., & Killen, P. J. (1989). Self-monitoring, surveillance, and incentive effects on cheating. *The Journal of Social Psychology*, *129*(5), 673–679. doi:10.1080/00224545.1989.9713784

de Jong, M. G., Pieters, R., & Stremersch, S. (2012). Analysis of sensitive questions across cultures: An application of multigroup item randomized response theory to sexual attitudes and behavior. *Journal of Personality and Social Psychology*, *103*(3), 543–564. doi:10.1037/a0029394

de Vries, R. E., Zettler, I., & Hilbig, B. E. (2014). Rethinking trait conceptions of social desirability scales: Impression management as an expression of honesty-humility. *Assessment*, *21*(3), 286–299. doi:10.1177/107319111 3504619

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

Donnellan, M. B. & Lucas, R. E. (2008). Age differences in the Big Five across the life span: Evidence from two national samples. *Psychology and Aging*, *23*(3), 558–566. doi:10.1037/a0012897

Eggers, D. (2013). *The circle*. New York, NY: Knopf Publishing Group.

Field, A. P., Miles, J., & Field, Z. (2012). *Discovering statistics using R*. Thousand Oaks, CA.: Sage.

Fife, E. & Orjuel, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*, 1–10. doi:10.5772/51645

Fischer, D. & Bates, J. (2008, April). The development and investigation of an IAT for workplace integrity. San Francisco, CA.

Fischer, D., Thompson, P., & Turner, B. (2012, April). Predicting integrity behavior with the Implicit Association Test. San Diego, CA.

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, *78*(6), 1360–1380.

Greenwald, A. G., Nosek, B. A., & Banaji, M. R. (2003). Understanding and using the Implicit Association Test: I. An improved scoring algorithm. *Journal of Personality and Social Psychology*, *85*(2), 197–216. doi:10.1037/0022-3514.85.2.197

Greenwald, G. (2013.06.06). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from www.theguardian.com

Hair, J., Black, W., Babin, B., & Anderson, R. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice-Hall, Inc.

Johnson, B. (2010.01.11). Privacy no longer a social norm, says Facebook founder. *The Guardian*. Retrieved from www.theguardian.com

Jonason, P. K. & Webster, G. D. (2010). The dirty dozen: A concise measure of the dark triad. *Psychological Assessment*, *22*(2), 420–432. doi:10.1037/a0019265

Leary, M. R., Herbst, K. C., & McCrary, F. (2003). Finding pleasure in solitary activities: Desire for aloneness or disinterest in social contact? *Personality and Individual Differences*, *35*(1), 59–68. doi:10.1016/S0191-8869(02)00141-1

Marlinspike, M. (13.06.2013). Why 'I have nothing to hide' is the wrong way to think about surveillance. Retrieved from www.wired.com

Masur, P. K. (2016). *Situational privacy and self-disclosure: Dissertation in preparation*. Hohenheim, Germany: University of Hohenheim.

Morton, A. (2013). Measuring inherent privacy concern and desire for privacy - A pilot survey study of an instrument to measure dispositional privacy concern. In *International Conference on Social Computing (SocialCom)* (pp. 468–477). doi:10.1109/SocialCom.2013.73

O'Keefe, D. J. (2003). Message properties, mediating states, and manipulation checks: Claims, evidence, and data analysis in experimental persuasive message effects research. *Communication Theory*, *13*(3), 251–274. doi:10.1111/j.1468-2885.2003.tb00292.x

Ones, D. S., Viswesvaran, C., & Schmidt, F. L. (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology*, *78*(4), 679–703. doi:10.1037/0021-9010.78.4.679

Paulhus, D. L. & Williams, K. M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, *36*(6), 556–563. doi:10.1016/S0092-6566(02)00505-6

Paunonen, S. V. (2002). Design and construction of the Supernumerary Personality Inventory. London, Canada: University of Western Ontario.

Paunonen, S. V. & Ashton, M. C. (2001). Big Five factors and facets and the prediction of behavior. *Journal of Personality and Social Psychology*, *81*(3), 524–539. doi:10.1037/0022-3514.81.3.524

Pedersen, D. M. (1979). Dimensions of privacy. *Perceptual and Motor Skills*, *48*(3), 1291–1297. doi:10.2466/pms.1979.48.3c.1291

Pedersen, D. M. (1982). Personality correlates of privacy. *The Journal of Psychology*, *112*(1), 11–14. doi:10.1080/00223980.1982.9923528

Petronio, S. (Ed.). (2000). *Balancing the secrets of private disclosures*. Mahwah, NJ: Lawrence Erlbaum Associates.

R Core Team. (2016). R: A language and environment for statistical computing [Computer Software]. Vienna, Austria: R Foundation for Statistical. Retrieved from www.R-project.org

Reed, M. B. & Aspinwall, L. G. (1998). Self-affirmation reduces biased processing of health-risk information. *Motivation and Emotion*, *22*(2), 99–132. doi:10.1023/A:1021463221281

Richetin, J., Costantini, G., Perugini, M., & Schönbrodt, F. (2015). Should we stop looking for a better scoring algorithm for handling implicit association test data? *PloS one*, *10*(6), e0129601. doi:10.1371/journal.pone.0129601

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(2). Retrieved from www.jstatsoft.org/v48/i02/paper

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*(6), 741–752. doi:10.1111/j.1468-2389.2006.00335.x

Sheldon, K. M. (2004). Integrity [authenticity, honesty]. In C. Peterson & Seligman, M. E. P. (Eds.), *Character strengths and virtues: A handbook and classification* (pp. 249–271). Oxford, UK: Oxford University Press.

Sieradski, D. (2013.08.06). Nothing to hide. Retrieved from http://danielsieradski.com/2013/06/14572/nothing-to-hide/14572/

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

Stone, D. L. (1986). Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy. *Perceptual and Motor Skills*, *62*(2), 371–376. doi:10.2466/pms.1986.62.2.371

Tormala, Z. L., Petty, R. E., & Brinol, P. (2002). Ease of retrieval effects in persuasion: A self-validation analysis. *Personality and Social Psychology Bulletin*, *28*(12), 1700–1712. doi:10.1177/014616702237651

Trepte, S. & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior*, *29*(3), 1102–1112. doi:10.1016/j.chb.2012.10.002

van Bommel, M., van Prooijen, J.-W., Elffers, H., & van Lange, P. A. M. (2014). Intervene to be seen: The power of a camera in attenuating the bystander effect. *Social Psychological and Personality Science*, *5*(4), 459–466. doi:10.1177/1948550613507958

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Overall discussion

6 Overall discussion

6.1 Summary

The introduction ended with the following question: "What happens in each one of us when we provide information about ourselves, for example on SNSs, and what could this process reveal about our personality? What is the psychology of privacy?" Taken together, this dissertation offers the following answer:

Our context determines the degree of privacy we are currently perceiving. The more privacy we are perceiving, the more information we are likely to disclose (Study 1; Dienlin, 2014). In addition to context, also our psychological expectations affect our behavior. For example, if we are concerned about our privacy on SNSs we are less likely to disclose personal things on Facebook (Study 2; Dienlin & Trepte, 2015). Vice versa, if we think that we will benefit from self-disclosing we are more likely to communicate information about ourselves (Study 3; Dienlin & Metzger, 2016a). However, our psychological expectations do not only affect self-disclosure, they also influence self-withdrawal (i.e., using privacy settings such as friends lists). When comparing online self-disclosure with online self-withdrawal, we found that privacy concerns are more powerful to predict self-withdrawal, whereas expected benefits are more effective to predict self-disclosure. Finally, our desire for privacy resonates profoundly with several aspects of our personality. For example, people who are more likely to report lacking integrity, people who are more shy, less anxious, and more risk averse are also more likely to desire privacy (Study 4; Dienlin & Metzger, 2016b).

In short, this dissertation can be summarized as follows: Privacy consists of three major elements, the objective privacy context, the subjective privacy perception, and the consecutive self-disclosure or self-withdrawal. The behavioral manifestations of privacy (disclosure or withdrawal) can be predicted accurately if we know a person's privacy concerns and expected benefits, and the desire for privacy is itself a powerful predictor for a person's overall personality.

6.2 Implications

6.2.1 Privacy is contingent, tripartite, and multidimensional

In what follows, I present and elaborate on four overarching findings of this dissertation. They stem from a joint analysis of all studies and aim to provide a broader perspective. The first finding that I want to focus on is that privacy is contingent, tripartite, and multi-dimensional.

One major aim of this dissertation was to advance our theoretical understanding of privacy. What is privacy, what are important psychological mechanisms? Is it possible to measure it, to feel it, or to conceptualize it? Of course, these questions are not new and have been asked many times before. According to Kammerer (2014), academic research on privacy began already in the late 19th century when Warren and Brandeis (1890) published their seminal article "The right to privacy" in the Harvard Law Review, featuring the famous claim that privacy is the "'right to be let alone'" (p.195). Since then, several theories and studies followed that all contribute significantly to a better understanding of privacy. However, these theories and studies also contradict each other regarding various aspects, which became especially apparent when the digital revolution of recent years challenged our entire academic understanding of privacy.

With the aim of answering the aforementioned questions, I combined several well-tried theories into one encompassing theory of privacy, the privacy process model (PPM). As a result, the PPM is not so much a new theory of privacy, but rather an integration of already existing theories. It is the theoretical corner stone of this dissertation, and each of the following empirical studies build upon it. In short, the PPM advances that privacy is a contingent, tripartite, and multi-dimensional construct. It consists of the privacy context, the privacy perception, and the consecutive self-disclosure or self-withdrawal. The distinction between the objective context and the subjective perception of privacy offers a potentially better understanding of self-disclosure, given that people often overestimate their true level of privacy (e.g., on SNSs; Trepte & Reinecke, 2011). From a larger perspective, one could thus say that the PPM introduced the well-known differentiation between constructivism and objectivism (see, e.g., Jonassen, 1991) to privacy theory, since constructivism predicates that there is no independent objective reality but only a personal and subjective construction of it. Next, referring to interpersonal boundary regulation as suggested by Altman (1975), another central aspect of the PPM is the claim that users constantly engage in a privacy regulation. That is, if the desired level of privacy differs from the achieved level of privacy, users either change their context or their self-disclosure. In conclusion, the PPM combines the notion of interpersonal boundary regulation through self-disclosure (Altman, 1975) with the well-known privacy related aspects of self-withdrawal (Westin, 1967), whilst employing a multi-dimensional perspective (i.e., informational, social, psychological, and physiological privacy; Burgoon, 1982). Thus, most claims of the PPM are not new, given that the PPM substantially builds upon a large body of studies on privacy literacy. Conversely, what's new is the combination, the synthesis of all the aforementioned specific notions into one encompassing psychological theory of privacy. In other words, one might describe the PPM as a kit that encompasses the most important tools in order to arrive at a fundamental understanding of privacy as a psychological concept.

The PPM potentially helps to advance privacy research in various contexts. For example, one major aim of current literature is to explain and predict specific online privacy behaviors as best as possible, and the so-called privacy calculus emerged as one of the most prolific theories to achieve just that (e.g., Krasnova, Veltri, & Günther, 2012). However to date, when measuring online privacy behaviors, privacy calculus theory only referred to self-disclosure. The PPM, by contrast, emphasized that in order to regulate privacy people do not only self-disclose but also self-withdraw — a notion that goes all the way back to Altman (1975). As a result, in the extended privacy calculus model for SNSs (Study 3; Dienlin & Metzger, 2016a) we introduced this bivariate perspective to privacy calculus theory and added self-withdrawal as a second dependent variable. It seems important to stress that, so far, empirical research focused mostly on one behavior at a time.

That is, whereas several studies analyzed which factors can explain online self-disclosure (e.g., Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010), other studies investigated which factors can explain online self-withdrawal (e.g., Lang & Barton, 2015). Some did, in fact, analyze both behaviors in one study — however, they either used separate statistical models (e.g., Yong Jin Park, 2015; Walrave, Vanwesenbeeck, & Heirman, 2012) or analyzed them as independent variables instead of as dependent variables (e.g., Masur & Scharkow, 2016). As a result, the PPM inspired the extended privacy calculus model for SNSs, which integrated a bivariate understanding of privacy by including both self-disclosure and self-withdrawal as dependent variables. This had several positive outcomes: For example, it showed that privacy concerns are more important for self-withdrawal than for self-disclosure. Altogether, the extended privacy calculus model might thus help to update our general theoretical understanding of privacy.

Next, it becomes increasingly apparent that privacy is not a uni-dimensional variable. Instead, privacy consists of several interrelated sub-dimensions that all display individual characteristics. On a theoretical basis, the PPM integrated Burgoon's (1982) notion that privacy consists of four dimensions: informational, social, psychological, and physiological privacy. On an empirical basis, we found support for this multi-dimensional nature of privacy as well. For example, in a theory of planned behavior approach, we designed three models of privacy behaviors: One focused on informational privacy, one on social privacy, and one on psychological privacy (Dienlin & Trepte, 2015). Results showed that the three dimensions differed substantially from one another. For example, privacy intentions and behaviors were most identical for psychological privacy behaviors (the empirical regression coefficient $\beta = .79$ showed that people were capable of disclosing almost exactly as much personal information as they wanted to reveal). However, the relation between privacy intentions and behaviors was weaker for the dimension of social privacy behaviors (the coefficient $\beta = .47$ implied that even when people wanted to restrict access to their SNS profile they were less likely to put that behavior into practice). At the same time, one can even argue that additional privacy dimensions exist, as was evidenced when analyzing the relationship between privacy and integrity (Study 4; Dienlin & Metzger, 2016b). Here, it was shown that aspects relating to anonymity, which partly resonate with the dimension of informational privacy, can offer incremental benefit when they are included in a specific research design.

Finally, the study showed that in addition to privacy *dimensionality*, it is equally important to differentiate privacy *directionality*. In other words, one has to consider from whom people desire privacy. In our last study, we showed that it can make a large difference whether people desire privacy from their peers or from the government (Dienlin & Metzger, 2016b). When people reflect upon negative past behavior, they do not desire more privacy from institutions but, instead, desire more privacy from their peers. As Laufer and Wolfe (1977) already suggested: Sometimes it is not important to have more privacy per se, but rather to have privacy from specific people.[1]

6.2.2 Privacy behaviors are not paradoxical

The second overarching finding of this dissertation is that privacy behaviors are not paradoxical. So far, several studies argued that online privacy behaviors are contrary to expectation, that they cannot be predicted sufficiently based on psychological antecedents and are thus paradoxical (Acquisti & Gross, 2006; Barnes, 2006; Norberg, Horne, & Horne, 2007; Taddei & Contena, 2013; Taddicken, 2014; Tufekci, 2008). However taken together, the results of the studies arrive at a different estimation of the plausibility of privacy behaviors.

The PPM already showed that if we distinguish between objective and subjective privacy we have a better chance to understand users' privacy behaviors (Dienlin, 2014). In addition to this theoretical argument, we adopted an empirical theory of planned behavior-based approach (TPB; Ajzen, 1985) and explicitly analyzed the predictability of online self-disclosure. The TPB approach built upon the PPM by using three of the four privacy dimensions (i.e., informational, social, and psychological privacy), and showed that online privacy behaviors are not random or paradoxical but instead are heavily influenced by psychological antecedents such as privacy intentions, privacy attitudes, and privacy concerns. Results showed that the antecedents explained

[1] For example, in a vivid illustration Laufer and Wolfe (1977) argued that kids, above all, prefer to have privacy from their parents.

between 20 percent (social dimension) and 62 percent (psychological dimension) of online behaviors — effects that are large compared to those usually found in social research.

By focusing on privacy concerns, the TPB approach analyzed antecedents of online self-disclosure that are mostly negative. However, if we broaden the perspective and reconsider the most important tenets of privacy theory (e.g., Altman, 1975) it becomes apparent that this can only be one side of the "privacy coin" and that self-disclosure should be determined by positive aspects as well. And indeed, referring to privacy calculus theory (Culnan & Armstrong, 1999), a growing body of research has confirmed by now that online self-disclosure is influenced significantly by both costs and benefits (Cheung, Lee, & Chan, 2015; Krasnova et al., 2012; Krasnova et al., 2010; Min & Kim, 2015; Shibchurn & Yan, 2015; Sun, Wang, Shen, & Zhang, 2015). As a result, in the so-called extended privacy calculus model for SNSs we hence broadened the TPB approach and included expected benefits as further antecedents of online self-disclosure.

The extended privacy calculus model replicated the results of the TPB approach and showed that privacy concerns explained self-disclosure significantly. In addition, results confirmed that benefits predicted self-disclosure and that privacy self-efficacy in turn determined self-withdrawal. More precisely, perceived benefits and privacy concerns explained 30 percent of online self-disclosures, whilst privacy concerns and privacy self-efficacy explained 14 percent of online self-withdrawal. For the context of social sciences, these numbers again represent medium to large effect sizes (Cohen, 1988) — which seems somewhat remarkable, and again shows that privacy behavior can be predicted to a large extend based on psychological antecedents, arguing against the privacy paradox.

How can we explain the diverging results on the privacy paradox? Obviously, the studies used different methods, samples, and underlying theories. As a result, one could argue that studies which found significant relations between concerns and behavior simply used superior methods. However, this might be only one part of the truth, because at the same time these studies also took completely different perspectives. Whereas those studies that supported the privacy paradox explicitly looked for discrepancies (e.g., Norberg et al., 2007), newer ones rather tried to bridge the attitude behavior gap and aimed to find similarities (e.g., Dienlin & Trepte, 2015). As illustration what this difference of perspectives can signify, let us briefly consider the following notions (which are, of course, somewhat polemic and oversimplified):

1. Human behavior can be predicted by three variables: the person, the situation, and the error (e.g., Lewin, 1935; Novick, 1966).
2. Error represents entropy and is chaotic. The person and the situation represent structure and are systematic.
3. The privacy paradox focuses on the error, and thus finds entropy. The PPM, the theory of planned behavior approach, and the extended privacy calculus model focus on the situation and the person, and hence find structure.

At this point, Karl Popper might reply: If we look for paradoxes we will find paradoxes, and we look for structures we will also find structures (Popper, 1959/2005). Even when taking Poppers scientific desiderata of objectivity, falsifiability, parsimony, and falsification into account, the question still remains: Which aspect do we want to focus on? Finding paradoxes or finding structures? The dissertation's combined results hopefully show that it might be more helpful and sustainable to adopt the second perspective, because this way we increasingly have the chance to better understand a substantial part of privacy behavior online, the underlying psychology of privacy, and to offer concrete individual and societal recommendations.

Hence, by attaching significance to situation and person the combined results of this dissertation echo the views of Rogers (1951/2003) and support a perspective that is profoundly humanistic: Taken together, all studies provide evidence that online behaviors are substantially based upon psychological antecedents, and that inner values, attitudes, concerns, joys, and intentions alike all relate to privacy behaviors. The results show that our online behavior is not only due to error, chance, or misfortune. In conclusion, this dissertation hence refutes the privacy paradox perspective and, alternatively, offers both theoretical and empirical support for a more humanistic perspective by emphasizing the significance of both situation and person.

6.2.3 Privacy is a powerful predictor

The PPM, the TPB approach to the privacy paradox, and the extended privacy calculus model all aimed to contribute to a better understanding of privacy and its underlying psychological mechanisms. However, one might ask, "What is the big deal? Why do we need a better understanding of privacy?" By linking privacy with other more distal psychological constructs, we arrive at the third overarching finding of the dissertation: Because privacy has strong and paramount predictive power.

In the last study of this dissertation we analyzed the relation between privacy and personality and, more specifically, the relation between privacy and a novel variable, one that had not been analyzed alongside privacy so far, which is *lack of integrity*. And indeed, results showed that people who have shown more negative behaviors in the past (which can be interpreted as a sign of lower integrity) on average desire more privacy (probably because they face a higher risk when self-disclosing; Altman, 1976). Interestingly, desired levels of privacy did not only correspond with integrity that was measured with self-reports but also with integrity that was measured with an implicit association test (Fischer & Bates, 2008, April). This triangulation of methods further supports that the relation between integrity and desired levels of privacy is profound, which is noteworthy given that the relation was tested for the first time.

From a theoretical perspective, the study argues that if we engage in negative behaviors this will increase our desire for privacy. From a methodological perspective, this is a causal and one-way assumption. It does not mean that if the privacy needs of a person increase he or she will show more negative behaviors. However, and by definition, this causal one-way relation still allows for the following statistical inference: If we know someone's desire for privacy, we have a better chance to infer his or her level of integrity. However, be that as it may, by no means we can conclude that a person who has a high desire for privacy *must* have low integrity — in the end, there is only a slightly higher chance that this might be true. Because next to significant relations with integrity, the study also showed that the desire for privacy relates to other (neutral) facets of personality. That is, people who are more shy, less anxious, and more risk averse also desire more privacy.

Taken together, the results suggest that if we know the privacy needs of a person we can partly predict that person's self-perceived integrity. Given that the relation between privacy and freedom, privacy and security, and security and freedom are all interrelated and complementary, and that one should not come at the expense of the other, this ultimately shows one thing: Both scholars and practitioners need to be cautious and use the predictive statistical power of privacy with sufficient responsibility.

The research question of this final study — does the desire for privacy relate to peoples' integrity? — was novel altogether. Hence, the results are especially important to contextualize. Prior research already showed that people cheat less when they are being surveilled (e.g., Covey, Saladin, & Killen, 1989), which supports that people who are of less integrity desire more anonymity and privacy from the government. Similarly, other studies also found that aspects of personality relate with the need for privacy: For example, people who were less authentic in their relationships desired more privacy from others (Trepte, Dienlin, & Reinecke, 2013), or people who reported to be less agreeable also desired more privacy (Erlmoser, 2016). Nonetheless, it remains to be seen whether the relation between privacy needs and integrity will be replicated in different contexts and with other samples. Moreover, the results could also be challenged from a theory-based position, because the relation might be mediated by other third variables (e.g., the need to hide something). At any rate, Laufer and Wolfe (1977) argued already in 1977 that "what is hidden from us either individually or collectively can be potentially harmful" (p. 23) — a statement that the results of the last study corroborate, and which eventually shows that it is important to extend our understanding of privacy.

6.2.4 Privacy is profoundly psychological

Finally, the last meta-finding I want to emphasize is that privacy as a concept is profoundly psychological. What defines a concept that can be considered psychological? According to Zimbardo, Gerrig, and Graf (2008), psychology as a scientific discipline describes, explains, predicts, and controls individual human behavior by analyzing underlying mental processes, which most prominently consist of cognitions and emotions. Hence, a concept can be labeled psychological when it focuses on human cognitions and emotions—and it becomes quickly apparent that all four studies either introduced or emphasized aspects of privacy that refer to cognitions and emotions.

First of all, and as has already been stated throughout the discussion, the PPM introduced the concept of perception to a model of privacy. At the same time, the PPM still maintains the concept of the objective privacy context. Hence, there is first an objective situation, which is then processed in a subjective perception, and which finally manifests in a behavior (i.e., self-disclosure). This tripartite and contingent distinction seems familiar in the context of psychology, since it was most prominently established during the period of the *cognitive turn/revolution* (e.g., Chomsky & Skinner, 1959; Dember, 1974). The distinction is well known and reads as follows: First, there is an objective stimulus, which is subsequently processed by a subjective organism (often described as the black-box), which eventually leads to a behavioral reaction.[2] This new cognitive perspective replaced the simpler stimulus-response or input-output view of behaviorism, which was established by John Watson or B. F. Skinner (e.g., Skinner, 1953/2014).

Of course, psychological aspects pertaining to privacy have also been discussed before this dissertation (maybe most prominently by the work of Irvin Altman); however, the PPM seems to be the first privacy model that makes this distinction explicit. And I argue that this explicitness is important because scholars sometimes still think predominantly in the input / output perspective. For example, take the studies that support the privacy paradox, and let us look at their results from a slightly different angle: One could also argue that they marvel about peoples' behavior (output) in the context of the Internet (input), without really focusing on the organism's mediating cognitions such as expected benefits, subjective norms, or perceived self-efficacy—which are all of a psychological nature.

Next, both the theory of planned behavior approach toward the privacy paradox and the extended privacy calculus model include at least some aspects of emotions, given that they both focus on privacy concerns. In general, according to Katz (1960) there are three types of attitudes: affectively based attitudes, behaviorally based attitudes, and cognitively based attitudes.[3] Cog-

[2] Also known as *SOR* process

[3] Also known as *ABC* model

nitively based attitudes represent a deliberate appraisal of an object, person, or behavior (e.g., "I think that SNSs are useful, because they help foster friendships"). Affectively based attitudes focus on the emotions toward these entities (e.g., "I think that SNSs are distressing, because people always try to impress others"). Behaviorally based attitudes are attitudes that people infer by observing their own behavior (e.g., "I think I like SNSs, because I use them so much"). Now, let us consider the definition of privacy concerns: "Privacy concerns capture the negatively valenced emotional attitude that people feel when personal rights, information, or behaviors are being regressed by others" (Dienlin, 2014, p. 286). By addressing "negatively valenced emotional attitudes", privacy concerns thus differ from the closely related concept of perceived privacy risks, which measures "the expectation of losses associated with the release of personal information" (Xu, Luo, Carroll, & Rosson, 2011, p.46). Hence, the main difference is that privacy concerns emphasize implicit emotions, whereas privacy risks prioritize explicit cognitions.

Interestingly, it is actually relevant to draw this distinction. Both the theory of planned behavior approach toward the privacy paradox study and the extended privacy calculus study showed significant relations between privacy concerns and both self-disclosure and self-withdrawal. However, it seems that privacy concerns relate more closely to behaviors than expected privacy risks. In an additional analysis of the extended privacy calculus (which we could not include into the publication for reasons of length), we integrated both privacy concerns and expected privacy risks simultaneously to predict self-disclosure and self-withdrawal.[4] And indeed, results showed that privacy risks did not influence self-disclosure ($b = 0.01$, $\beta = .01$, $SE = 0.03$, $p = .739$) and self-withdrawal ($b = -0.01$, $\beta = -.04$, $SE = 0.01$, $p = .739$), whereas privacy concerns were shown to be a strong predictor of both self-disclosure ($b = -0.29$, $\beta = -.23$, $SE = 0.05$, $p < .001$) and self-withdrawal ($b = 0.19$, $\beta = .45$, $SE = 0.02$, $p < .001$).

[4] As a reminder, we measured privacy concerns with items such as "I worry about my privacy as a result of using Facebook" or "I do not feel especially concerned about my privacy online". Expected privacy risks, conversely, were measured with items such as "I might be embarrassed by information or pictures posted on Facebook" or "I might get unwanted attention or even harassment, like from a stalker". The scale showed good factorial validity ($\chi^2 = 132.50$, $df = 27$, $p < .001$, CFI = 0.98, TLI = 0.97, RMSEA = 0.06, SRMS = 0.03).

Altogether, the combined results imply that if we want to predict online behavior most accurately, both internal cognitive and emotional aspects must be taken into account, as they potentially offer a better way to open the black-box. Overall, it becomes increasingly apparent that privacy is a concept which is profoundly psychological.

6.3 Criticism and future perspectives

What are points of criticism and useful directions for future research? In what follows, I offer thoughts that compared to the points put forward in the respective studies are of a more general nature.

6.3.1 Stronger emphasis on control

What is the most important theoretical component of privacy? Whereas one group of scholars emphasizes that privacy is about the extent of personal *withdrawal*, a second group suggests that privacy is more about *control*. The latter holds that privacy only exists if people can determine when and where to self-disclose (according to Masur (2016), the first group is most prominently represented by Gavison (1980) and the second group by Miller (1971)). The PPM argues in favor of the first position, and arguably there are several good reasons for doing so. For example, the literal meaning of the word private is *deprived*, *robbed*, *free*, or *personal*. As the literal meaning emphasizes withdrawal, it is thus justified to make it the central notion of a conceptual definition of privacy. Besides, if we define privacy solely as amount of control, the entire concept would become increasingly redundant with other notions such as autonomy or freedom.

At the same time, there are also several good reasons to integrate aspects of control more prominently into a definition of privacy.[5] Let us briefly leave the context of online media and turn to an example of the offline world (for

[5] Notably, also the PPM does incorporate some aspects of control. That is, the PPM states that in situation where the desired level of privacy differs from the achieved level of privacy people either change their privacy context or their self-disclosure depending on their level of control. For example, the level of control determines whether people are either leaving a room or switching the subject of a conversation. Nevertheless, it can still be argued that the PPM somewhat underprioritizes aspects of control.

which the PPM is also configured to apply). According to the PPM, a prisoner has to be considered completely private given that he / she is withdrawn and all by himself / herself. However, this operationalization disregards the psychological manifestation of privacy, in other words its cognitive and subjective representation. That is, if we asked the prisoner whether he or she would *feel* private or not he / she would most likely reply: "No." Asked why, the prisoner would probably go on: "Because I cannot decide when to wake up, what to do, or with whom to talk. However, I could do that at home, and only there I would feel truly private." For the context of online media, one could think of the following example: If we cut off the Internet connection of a person, according to the PPM he / she should be more private. However, that person would probably not agree and rather consider this forced disconnection as an invasion into his / her privacy. In conclusion, it seems somewhat coercive trying to establish an academic definition of privacy that is not shared by the individual. Constructivists such as Kelly (1991) and also Watzlawick (1984) would probably agree, given that they have often urged to understand psychological concepts based on peoples' own personal understanding, an aspect that is under-prioritized in the PPM.

Similarly, according to Laufer and Wolfe (1977) children often state that the context in which they feel most private is not at home but outdoors — simply because their parents cannot supervise and interfere, which provides children with more control over their own behavior and the chance to act independently. Children even say that the harshest invasion into their privacy takes place when others deprive them of this exact control. "Interestingly the inability to manage interaction stands out as the single most common experience of invasion among our respondents" (Laufer & Wolfe, 1977, p. 34). In conclusion, there are several good reasons why an updated version of the PPM could benefit from incorporating aspects of control more prominently into its central understanding of privacy.

6.3.2 Reanalysis of privacy dimensions

Another point of criticism regarding theory are the privacy dimensions as advanced by Burgoon (1982). Burgoon (1982) argued that privacy has four dimensions: informational, social, psychological, and physiological privacy.

In this dissertation, I have continually referred to this dimensionality (for example, in the PPM in Study 1 and in the analysis of the three different dimensions of informational, social, and psychological privacy behaviors in Study 2). However, next to several positive outcomes there are also negative aspects to using Burgoon's dimensionality. Most notably, the adoption of the psychological privacy dimension proved to be somewhat difficult. The exact definition of psychological privacy by Burgoon (1982) is as follows:

> Basically, psychological privacy concerns one's ability to control affective and cognitive inputs and outputs. On the input side, it involves the ability to think, to formulate attitudes, beliefs, and values, to develop an individual identity, to assimilate personal experiences with one's understanding of the world and its problems, and to engage in emotional catharsis free from outside impediments of interferences. On the input side,[6] it entails determining with whom and under what circumstances one will share thoughts and feelings, reveal intimate information and secrets, extend emotional support, and seek advice. (p. 224)

As stated before, two prominent perspectives on privacy exist: One that focuses on privacy as a withdrawal process and one that focuses on privacy as a control process. So first of all, the statement that psychological privacy is the "ability to control affective and cognitive inputs and outputs" (p. 224) shows that Burgoon represents the second party. By contrast, the PPM prioritizes aspects of withdrawal and thus understands psychological privacy somewhat differently (Dienlin, 2014, p. 110):

> I thus propose that psychological privacy be taken as a measure of the extent to which people present in a situation engage in intimate and personal, or trivial and impersonal conversations. The more that people disclose intimate information, the higher the psychological privacy context. If people elaborate on mundane topics like the weather, psychological privacy is regarded as low.

[6] Sic; should probably mean *output* side

> Defining psychological privacy this way offers one benefit: It accounts for all the situations in which people are able to think as they please, but not speak as they like. (p. 32)

This new definition has some advantages, most prominently because it enables an operationalization of privacy that is more comprehensive. For example, by defining it as degree of intimacy of self-disclosure it also allows for a measurement of psychological privacy *behaviors* (e.g., "Do you express personal aspects such as emotions and inner feelings on Facebook?"). Conversely, because Burgoon's definition focuses on controllability it only allows for the measurement of psychological privacy *situations* (e.g., "Can you express yourself freely and independently on Facebook?").

However, the novel conceptualization of psychological privacy as advanced by the PPM leads to different problems. First of all, it has one major flaw: If we consider privacy as degree of withdrawal and describe situations in which we withdraw as more private, the operationalization's directionality is technically wrong: Situations in which we talk about the weather should not as is currently suggested represent situations of low psychological privacy but actually situations of high psychological privacy. Why is that, one might ask? Because when we talk about the weather we have the chance to withdraw and are not forced to disclose personal information. Remember that in the extended privacy calculus model, we argued that self-disclosure always reduces privacy. Hence, when we talk about personal aspects such as failures or regrets, we always decrease our psychological privacy context, and when we talk about trivial aspects such as the weather, we increase our psychological privacy context.

Nevertheless, there are also reasons to maintain the PPM's original directionality. The most important one is its inferential logic, given that the PPM continually states that privacy increases the willingness to self-disclose. This logic would not work with the new and inverted directionality, as here people would self-disclose less when they have more psychological privacy. In other words, with the new and inverted directionality a *low* psychological privacy perception should lead to more self-disclosure, which thus contradicts the PPM inferential logic that a *high* privacy perception leads to more self-disclosure. Moreover, the new and technically correct directionality would be counter-intuitive: Because of the fact that people only disclose personal information in very intimate and private settings (high social and informational privacy), it intuitively feels wrong to label an intimate and personal situation a low psychological privacy situation.

Besides these problems of terminology and inferential logic (which are, admittedly, somewhat cumbersome), the PPM's conceptualization of psychological privacy also reduces the capacity to distinguish between informational and psychological privacy behaviors. This is because one could argue that informational privacy is actually a sub-dimension of psychological privacy: If we disclose our name, address, or birth date, situations become more intimate and more personal. People can self-disclose different types of aspects: identifying information, thoughts, or emotions. For reasons of parsimony, it does not seem necessary to consider informational privacy as another meta-dimension of privacy, when it could instead be considered a sub-dimension of psychological privacy. Moreover, the psychological privacy dimension is per se conceptually very close to self-disclosure (which is itself one of the three elements of the PPM): By definition, the more people self-disclose, the less psychological privacy they have. This is a somewhat circular and another reason for a different understanding of psychological privacy.

Finally, the empirical foundation of Burgoon's dimensionality could be further substantiated. Since Burgoon's work in the 1980s, the empirical methodology has improved significantly and it seems the time to reanalyze the dimensionality from an empirical bottom-up perspective. Given that a substantial part of current work on privacy is build upon her work, it seems desirable to reestablish the theory's legitimacy.

6.3.3 Integration of affordances

The PPM differentiates between the objective privacy context and the subjective privacy perception. As mentioned above, this can be seen as a variation of the classical antagonism between constructivism and objectivism / empiricism (Jonassen, 1991). Recently, a novel theoretical focus of communication research developed around the notion of so-called *affordances*. Introduced by Gibson (1979/2015), he described the concept of affordances as follows:

> The affordances of the environment are what it offers the animal, what it provides or furnishes, either for good or ill. The verb to afford is found in the dictionary, but the noun affordance is not. I have made it up. (p. 119)

Even though Gibson originally developed the concept for visual perceptions of animals it was quickly adopted in other contexts as well. First, communication science applied the concept of affordances in the late 2000's for computer mediated communication in general (e.g., Sundar, 2008), later for social media specifically (Treem & Leonardi, 2013), and currently also for questions regarding privacy (Trepte, 2015). For example, one affordance of the SNSs Facebook is its positive communication, as epitomized by the *like* button. Facebook designed the structure of its SNS in a way that people are invited, almost inclined both to communicate *and* to like — structure and behavior blend into one. So, why is the concept of affordances promising? It seems that, most of all, for reasons of parsimony. That is, affordances offer the chance to merge objective and subjective viewpoints into one single entity. Gibson (1979/2015) expressed this advantage very poignantly as follows:

> [...] the absolute duality of "objective" and "subjective" is false. When we consider the affordances of things, we escape this philosophical dichotomy. (p. 35)

Future research could, thus, analyze the option whether including privacy affordances might make the distinction between context and perception redundant. At any rate, one could argue that the PPM's contingent relationship between (1) privacy context, (2) privacy perception, and (3) self-disclosure is in fact not that strict. Technically speaking, and in the words of Baron and Kenny (1986), the PPM implies a *full mediation* of the relationship between privacy context and self-disclosure through the privacy perception — a notion that one could challenge. For example, several scholars have already emphasized that the context or situation itself can strongly influence peoples' self-disclosure (e.g., Masur, 2016), and that this influence takes place subconsciously without a deliberate cognitive representation. As a result, one could either solve this problem by adding another path to the PPM — a path that would model a direct relation between privacy context and self-disclosure. Or, instead, one could also refer to the affordances approach and treat them as one single variable altogether.

Next, one can criticize that both the theory of planned behavior approach toward the privacy paradox and the extended privacy calculus model did not sufficiently discuss influences on user behavior that are external. Granted, the two studies deliberately analyzed internal influences on online behavior (such as personality, attitudes, or intentions). However, if one really aims to maximize the predictability of behavioral variance one would also need to implement *external* influences, factors such as social influences or infrastructural affordances. In other words, if we want to maximize our chances to find out whether Person A leaves a post on Person B's Facebook profile today, it might be more important to measure whether he or she received a message from Person B that day (social influence), and whether Person A has activated the setting to be notified upon arrival of new messages (infrastructural affordance). However, the need to compare the influence of situational versus personal factors when analyzing privacy behaviors has already been ascertained elsewhere and will be subject matter of further research (e.g., Masur, 2016).

6.3.4 Increase of explained behavioral variance

The theory of planned behavior approach toward the privacy paradox and the extended privacy calculus model both show that large parts of online behavior can be explained by means of psychological variables such as concerns, attitudes, or intentions. As mentioned above, prior research often found a gap between these psychological variables and behavior. The theory of planned behavior approach was able to bridge this gap by implementing the principle of compatibility (Fishbein & Ajzen, 2010). Nevertheless, this approach also has some critical aspects. Hence, let us briefly recapture the principle of compatibility by looking at its definition:

> According to the *principle of compatibility* [...], an intention is compatible with a behavior if both are measured at the same level of generality or specificity — that is, if the measure of intention involves exactly the same action, target, context, and time elements as the measure of behavior. (p. 44)

This leads to the problem that items measuring attitudes, intentions, and behaviors are very similar to one another. Let us consider the following example of informational privacy:

- Informational privacy attitude: "I think that giving information on FB that identifies me is: not useful vs. useful"
- Informational privacy intention: "How much identifying information do you currently want to provide on FB?"
- Informational privacy behavior: "How many personal things do you currently communicate on FB?"

Hence, the principle of compatibility could potentially lead to a shared variance that is somewhat artificial, due only to similar wording and not meaningful conceptual overlap. As a result, it is possible to conclude that one of the TPB's biggest strengths is also one of its most significant weaknesses. Nevertheless, future research could still ameliorate this aspect by using a longitudinal design that measures the behavior one or two weeks after the prior scales were collected. In general, the entire TPB is actually configured to analyze behavior by means of a longitudinal approach — a notion that most studies using the TPB, however, often do not put into practice (and the study presented here is obviously no exception). By using a longitudinal approach no memory effects would take place, and as a welcome side effect the relation's causality could be further substantiated. The primary way, however, of solving problems that arise with the principle of compatibility is to analyze concrete behavioral data, which would provide all the incremental benefits associated with method triangulation.

Be that as it may, we can of course still raise the following (general) question: Should we as researchers really be satisfied with explaining 30 percent of online privacy behaviors? If the aim was to explain as much behavioral variance as possible, which is legitimate and generally desirable, this might not be satisfactory. Other empirical methods such as artificial neural networks (ANN) are often capable of explaining more behavioral variance than traditional statistical procedures (e.g., West, Brockett, & Golden, 1997). In this dissertation, all empirical analyses were top-down theory-based and did not use bottom-up automated self-learning algorithms. As a result, bottom-up techniques such as ANN appear to be a promising path upon which future research should try to tread — especially in the context of social sciences, where these techniques are still not well established.

The question is: Do we really and only want to *predict* privacy behaviors and privacy needs as accurately as possible? Then, of course, bottom-up procedures such as ANN are useful. Or, by contrast, do we want to *understand* privacy behaviors and needs as best as possible? If so, top-down procedures such as theory-based structural equation modeling remain the way to go. At any rate, future research should venture in directions that include bottom-up methodology as well, because this might help to corroborate already existing theories and explore new relations that might have not been addressed so far. In conclusion, the true question does not seem to be either or, but rather which and when?

6.3.5 Further elaboration of integrity

Of all studies, Study 4 offers the widest range for future research. Three aspects stand out that have to be addressed. First, given the considerable potential societal explosiveness the results ask to be replicated in different contexts with other samples in order to further analyze the findings' stability, generalizability, and profoundness. Next, the concept of integrity itself needs more research. Currently, a multitude of redundant concepts exists that have yet to be arranged within one large, consistent, and overarching model of integrity. Finally, future studies should continue to develop experimental settings that help to effectively manipulate participants' perceived integrity.

On a more general level, we addressed aspects of integrity that mostly referred to behaviors that are illegal (or even criminal). However, other aspects belonging to the broader concept of integrity are relevant as well — for example, aspects of authenticity and consistency could be very interesting to analyze. Whereas criminality, by definition, refers closely to privacy needs from authorities, consistency might relate more closely to privacy needs from other people in general. People who behave differently in distinct social contexts might have a stronger need to selectively withhold specific information about themselves, which might result in a generally higher need for interpersonal privacy. Overall, Study 4 should be considered a first step into a novel research direction — it will be very interesting to see which new arguments, methods, and results future research will provide.

6.4 Societal and practical implications

What does it mean that our privacy is decreasing, how does it affect the world that we are living in? Is this "brave new privacy" good or bad, do the positive or the negative aspects prevail, and what can we do about it? In the introduction, I proposed the thesis that privacy has decreased significantly over the course of the past years, and identified the total privacy and the post privacy reactions as the two most prominent antitheses. Can the thesis and the two antitheses be reconciled into one synthesis?

When trying to find privacy related answers for these question, two starting points are often suggested: the individual and the collective (e.g., Trepte, von Pape, & Dienlin, 2016). In what follows, I adopt this differentiation and offer some individual- and collective-oriented thoughts in order to extrapolate the results of this dissertation.[7] So, after all, let us now consider the practical and societal implications that this dissertation can offer.

6.4.1 Increasing privacy literacy

In order to improve the way the *individual* engages with privacy, several aspects will be decisive. To date, one specific aspect seems to be of paramount importance, which is: increasing privacy literacy. Privacy literacy "encom-

[7] Granted, the negative perspective of the privacy thesis and the antitheses are, to some extent, arbitrary as one could also focus on the inherent positive aspects — for example, that SNSs are a perfect place to leverage informational social support (e.g., Trepte, Dienlin, & Reinecke, 2014a) or that communication on SNSs can increase life satisfaction (e.g., Dienlin, Masur, & Trepte, 2016). However, even though these positive evaluations are acknowledged throughout the next section, I primarily elaborate on aspects that first and foremost ask for improvement.

passes an informed concern for [...] privacy and effective strategies to protect it" (Debatin, 2011, p. 51). It consists of two major components: declarative and procedural privacy literacy (Trepte, Teutsch, et al., 2015).

> In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection, and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection. (p. 339)

Privacy literacy is important because it increases agency and thus empowers the user. The theory of planned behavior-based approach toward the privacy paradox showed that behavioral intentions differed most strongly from actual behaviors for the dimension of social privacy. In other words, the privacy behavior people struggle with the most are social privacy behaviors. Social privacy behaviors represent all those kinds of behaviors that restrict access to personal content for specific social groups. For example, on SNSs this can be represented by the use of friends list. The behavioral problems might be due to the fact that implementing social privacy behaviors on SNSs is difficult and can necessitate several dozens of clicks (Bilton, 2010.05.12). Given that users make, on average, one negative privacy experience every two months (e.g., someone spread a rumor in the online community, or someone posted embarrassing pictures; Trepte et al., 2014a), this is somewhat worrisome. Similarly relevant is that even after users have made negative experiences online they only increase their informational online privacy behaviors but not their social or psychological privacy behaviors (Trepte, Dienlin, & Reinecke, 2014b). Privacy literacy, as it encompasses procedural knowledge (Trepte, Teutsch, et al., 2015), could thus help empower the user and improve the status quo.

To date, only few studies on online privacy literacy and its cultivation exist (e.g., Hargittai, 2010; Y. J. Park, 2013). So far, we know that time spent online and past privacy regulations are positively related with self-perceived online privacy literacy (Bartsch & Dienlin, 2016). However, it remains unclear whether concrete educational programs also help to leverage online privacy literacy. Not only do people who report having more online privacy literacy also protect their privacy more strongly, online privacy literacy is in addition associated with more perceived safety when using SNSs (Bartsch & Dienlin, 2016). Therefore, leveraging online privacy literacy seems desirable at any rate.

6.4.2 Encouraging change

The results of the empirical studies showed that a large part of online behavior can be explained based on psychological antecedents such as intentions, attitudes, or concerns. What does this imply for a privacy synthesis? It shows that we still have some control over our online behaviors. Our behaviors largely represent our intentions, and our behaviors can be explained, at least partially, by a psychological tradeoff between costs and benefits of online services. It can therefore be stated that we are living an online life that resonates significantly with how we want to live.

Because of that, I argue that despite the enormous power of online companies such as Facebook or Google, users are not entirely powerless but still retain a significant influence over their own virtual representation. Yes, the status quo represents a loss of control. However, that does not mean that people have no control whatsoever. By contrast, it seems likely that if users can be convinced of the advantages of encrypting mails or of using privacy-enhancing browsers such as TOR they will adapt their behaviors. Of course, this would not change everything, but according to Dienlin and Trepte (2015) it has the potential to change up to 30 percent of behavioral variance. Therefore, based upon the results of Study 2 and Study 3, it is worth trying to improve peoples' online behavior by, for example, emphasizing the benefits of PGP.[8]

6.4.3 Spreading the knowledge

The PPM aimed to provide a new theoretical framework of the way privacy unfolds. I argue that spreading this knowledge and thus leveraging our understanding of privacy theory could help in several ways. Why is that? Because very similar to Lewin (1935), the PPM states that behavior depends on the person (subjective perceived privacy) who is, borrowing the words

[8] Acronym for "pretty good privacy", which is a method to encrypt e-mail communication.

of Heidegger (1927/1996, p.127), always "thrown" into a specific situation (objective privacy context). And by distinguishing privacy situation from privacy perception, the PPM offers a theoretical explanation as to why so many privacy mistakes happen on SNSs.

Let us briefly consider a typical example of a privacy mistake that happens routinely on SNSs: An employee who calls in sick at work. Later, the employee posts pictures of a concert that he or she attended in the evening. Unfortunately, however, the employee had forgotten that one of his / her followers is his / her superior. The PPM advances that even though the employee was not private while he or she posted the picture from an *objective* point of view, he / she nonetheless perceived to be private from his / her own *subjective* point of view. If we want people to commit less privacy mistakes, it is important to propagate this distinction — one needs to understand that sometimes one's feeling of privacy can be very misleading, and that the subjective privacy perception can differ substantially from the objective privacy context.

On an intrapersonal level, understanding privacy correctly could thus be considered as a modern developmental task: How private we feel does not necessarily imply how private we are — which is why we have to learn this distinction. On an interpersonal and societal level, this new perspective seems equally important to integrate. However, this might take some time: For example, the Copernican perspective that the earth *is* round also took several decades to manifest, only because the ground we are currently standing on *feels* so very flat.[9] At any rate, I think that by understanding how privacy works, unfolds, and manifests, online behaviors will mature and our privacy will be less endangered.

6.4.4 Updating the legislative system

In order to improve the way the *collective* engages with privacy two aspects appear to be most decisive. First of all, the legislative system needs to be updated. From a media psychology perspective, what seems most urgent regarding legal measures might be that information which was passed on to one specific company / website should be used only by this company and

[9] Example taken from: http://www.thebookoflife.org/know-yourself/

only for those purposes that were explicitly stated beforehand. The high number of privacy mistakes people commit show that nobody can perfectly process who has access to his or her data. However, as privacy perceptions do not always comply with objective privacy contexts, people cannot be aware of how their data is being used. Regarding the factual objective privacy context, let us consider Facebook's statement of rights and responsibilities that defines the following so-called IP License (Facebook, 2016):

> For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook. (para. 2.2.2)

Hence, users are not given access to the information on how their data is transferred to other companies, which makes it impossible to understand how one's information is being used. From a psychological viewpoint, this is simply not sustainable.

The aspects mentioned above become even more worrisome given that users of SNSs are willing to transfer content that is very intimate. For example, in 2012 40% of students of one specific high school in the United States used instant messengers or SNSs such as Facebook for sexting. Sexting represents the "transfer of sexually explicit pictures via cell phone" (Strassberg, McKinnon, Sustaíta, & Rullo, 2013). Results showed that 20% of the students had already sent nude pictures of themselves to others (Strassberg et al., 2013). Therefore, the IP Licence makes it theoretically possible for Facebook to obtain a considerable number of explicit pictures of their users and sell them to other companies. Even though this does not seem likely, it is not as absurd as one might think. Already to date, Facebook was shown to sell privately shared photos to advertising agencies. Uwe Buermann presented the case of a Facebook user who shared pictures of his family holiday in Spain with some of his friends in a restricted photo album (Schlag & Wenz, 2015.12.19). Several months later, when the family was on their way to their skiing holidays in the Czech Republic, they accidentally encountered one of the photos: On a large screen, a Czech travel agency published an advertisement that depicted the family including the two children during their holidays on the beach in Spain. Given that the user could not know that his objective privacy context was that low, his perceived privacy when uploading the pictures was very incorrect and misleading.

Which legal options exist? In Germany, the so-called *right of informational self-determination* exists, which interdicts to pass on information to third parties — information is allowed to be used only for the exact reason it was submitted (see, e.g., Lüpken-Räder, 2012). I argue that this right should be effective on Facebook as well. In the future, this might be the case. On the 15th December 2015, the European Parliament, the European Commission, and the European Council agreed on the new data protection rules (European Commission, 2015.12.15), which are part of the general data protection regulation (European Commission, 2012). Eventually, the following *right to object and profiling* of the data protection regulation might better represent the psychology of privacy online and could contribute significantly to a privacy synthesis:

> Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information (European Commission, 2012, p.53).

6.4.5 Establishing a Privacy-Knigge

Regarding collective actions, other options for a privacy synthesis exist. At its core, privacy is a behavioral concept about the regulation of interpersonal social relationships (Altman, 1976). In social cybernetic processes, societies oftentimes establish norms of conduct that eventually become codified in laws, rules, or books (e.g., Luhmann, 1984). In Germany, this was very prominently done by Freiherr Adolph Knigge in 1788, when he published his seminal book "On human relations" (Knigge, 1788/1853). Hoping to help and guide people in difficult social situations, Knigge proposed several exemplary role-model behaviors. For example, his first remark and rule on the conduct with other people is: "Society judges each human based only on the picture that he or she portrays of himself to the world" (Knigge, 1788/1853, p.8; translation by author).[10] Therefore, according to Knigge, one should always try to be very careful and candid with others. At this moment, it might be at the time to establish new social cybernetics by updating privacy-related norms of conduct, and to write a first "Privacy-Knigge".[11]

Which aspects would have to be included that might help to improve social cybernetics of privacy? First, considering the high number of privacy mistakes (which mostly happen due to context collapse; boyd, 2008), society should be aware of its own responsibility in the appraisal processes that usually follow after someone has committed a privacy mistake. Not only the individual but also the collective needs to learn that, today, information leaks very easily and that it is not difficult to detect others' idiosyncrasies or wrongdoings. Study 4 showed that privacy needs are related to integrity, but as complete withdrawal in order to avoid privacy errors cannot be the solution it might be preferable for society to account for that technological change. This means that one should not be surprised to find out inconsistencies in other peoples' life — on the contrary, one should rather expect to find these.

Moreover, three conditions have been suggested that necessitate a more pronounced protection of privacy (Dienlin, 2015): low publication intention, low status of expertise, and small-scale analyses. Low publication intention refers to the fact that it is a difference whether someone posts a message on Twitter, which is mainly used for public communication, or if someone sends a personal message via instant messengers such as WhatsApp, which are primarily used for private communication. I hold that information communicated in the latter needs to be protected more. Low status of expertise refers to the status of the communicator: If someone posts racist comments on SNSs it is important to consider whether that person is a 14 year old student expressing his or her still fleeting opinion, or if it is a person that wrote his or her master thesis about immigration. Finally, small scale analyses represent

[10] In the German original: "Jeder Mensch gilt in dieser Welt nur so viel, als er sich selbst gelten macht."

[11] In fact, the German Knigge council already published a Privacy-Knigge. However, this is only a first and preliminary online-version (Wälde, 2012)

the difference between analyzing the post of a single identifiable person, in contrast to a compound analysis of several anonymous communicators. The smaller the scale the more identifiable a person becomes, the more his or her privacy needs to be protected. If society learns to consider these three aspects more carefully when evaluating the communications of people, including all their various forms of privacy mistakes, hopefully a communication that is more fair and sustainable will result.

6.4.6 Making considerate inferences

What makes the aforementioned even more relevant becomes apparent when we reflect the results of Study 4. That is, if we analyze the privacy needs of a person, we have a good chance to get a decent understanding about a person's personality. According to Trepte et al. (2013), if we know someone's privacy needs we can predict his or her life satisfaction, positive and negative affect, and authenticity in interpersonal relationships. Study 4 now added that based on the desire for privacy it is even possible to predict aspects of integrity, shyness, anxiety, and risk aversions. For example, results showed that people who feel more inclined to violate social rules also have a slightly higher desire for privacy from government or from identification.

Hence, it seems that next to the several positive aspects of privacy one should also account for the notion that privacy offers room for deviant behaviors, such as cheating, theft, or exploitation. From a broader perspective, Study 4 supports that there are situations in which the benefits of surveillance might outweigh the benefits of privacy. For example, surveillance in public transport does seem justifiable, as people who have the need to avoid public surveillance also showed having less integrity.

At the same time, we need to be very considerate in order to interpret the aforementioned results correctly — most prominently, because the study also evidenced relations of the desire for privacy with other facets of personality. We have to take into account that, obviously, several other aspects also determine the privacy needs of a person. Next to the aforementioned relations with shyness, anxiety, and risk aversion, there is, for example, additional evidence that people who desire privacy are, by trend, more introverted (Stone, 1986). At any rate, the results are no basis upon which to infer that a person who desires more privacy always has to be of less integrity — yes, there is a slightly higher chance, but it could also be that he or she is simply more introverted. In conclusion, privacy can be compared to all the other things that entail both chances and risks, such as transport, sports, the Internet, or SNSs. They all have one thing in common: They must be treated with some consideration.

6.4.7 Having a two-sided privacy discourse

This directly leads to the next practical implication of this dissertation: If we want to continue toward a privacy synthesis, the combined results showed that it does not seem justified to uni-dimensionally and always strive for more privacy. Privacy is not better in each and every situation — a notion that was already included in Irvin Altman's understanding of privacy (see, e.g., Altman, 1975). Obviously, even though privacy is very important for almost everyone there are still considerable differences in how people enact their privacy (e.g., Trepte, Masur, Scharkow, & Dienlin, 2015).

In which situations do we need privacy as a protective and replenishing retreat, and in which situation do we need to limit privacy in order to prevent crime and exploitation? The answers will not always be easy and have to be found for specific contexts separately. However, one thing becomes increasingly apparent: In order to find solutions we need to discuss privacy from a two-sided perspective, which includes both pros *and* cons of privacy.

6.4.8 Designing new cultural artifacts

Finally, I suggest looking at the potential influences of culture. Culturalism puts forward that culture is one of the most powerful factors in providing social values and social actions (Znaniecki, 1919). Books such as *1984* (Orwell, 1950) or *The Circle* (Eggers, 2013) and films such as *Her* (Jonze, 2013) or *Citizenfour* (Poitras, 2014) are vivid examples of a culture's strong influence on its people. For example, Orwell's *1984* paved the way for a healthy societal concern regarding overtly repressive, exploitative, and omnipresent states. The term *big brother* became a commonplace expression and provided a palpable way for everyone to describe the atrocities of too much surveillance. Cultural artifacts have the power to change perceptions, values, and actions.

It might be time for a new *1984*, a new novel that presents an exemplary way to deal with the current challenges. For example, a novel that describes the story of the birth of an Anti-Facebook, an Anti-Google, or an Anti-Amazon. A coalition of anti-companies, which could culminate in a clash between a prior and a future economy. A new *Das Kapital* (Marx, 1867/1990), but with privacy as a novel currency. *The Circle* (Eggers, 2013) ranked 7th place in the New York Times' bestseller list — hence, given that the public is currently very interested in the topic, now might be a good time for another try.

6.5 The privacy synthesis

Both antitheses, the post privacy and the total privacy reaction, encompass their individual part of the truth. However, a true privacy synthesis cannot be as extreme as the two antitheses. It is time to talk about privacy from a two-sided perspective, a perspective that is more mature: So far, the existing privacy antitheses focused too strongly on one side — I argue that the conversation about privacy needs to be distinctively more differentiated.

Based on the results of this dissertation, I hence suggest the following privacy synthesis: Modern societies should try to design new cultural artifacts about privacy, update old and obsolete social privacy cybernetics, foster a better understanding of the conceptual nature of privacy, work toward new and more protective privacy laws, and, above all, aim to leverage overall privacy literacy.

Literature

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Proceedings of 6th Workshop on Privacy Enhancing Technologies* (pp. 36–58). Cambridge, UK: Robinson College.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control* (pp. 11–39). Berlin, Germany: Springer. doi:10.1007/978-3-642-69746-3{_}2

Altman, I. (1975). *The environment and social behavior*. Monterey, CA: Brooks Cole.

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, *8*(1), 7–29. doi:10.1177/001391657600800102

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from www.firstmonday.org/issues/issue11_9/barnes/index.html

Baron, R. M. & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173–1182. doi:10.1037/0022-3514.51.6.1173

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

Bilton, N. (2010.05.12). The price of Facebook privacy? Start clicking. *The New York Times*. Retrieved from www.nytimes.com

boyd, d. m. (2008). *Taken out of context. American teen sociality in networked publics: Doctoral dissertation*. Berkeley, CA: University of California.

Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication yearbook 6* (pp. 206–249). Beverly Hills, CA: Routledge.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites. *Internet Research*, *25*(2), 279–299. doi:10.1108/IntR-09-2013-0192

Chomsky, N. & Skinner, B. F. (1959). Verbal behavior. *Language*, *35*(1), 26. doi:10.2307/411334

Cohen, J. L. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). New York, NY: Academic Press.

Covey, M. K., Saladin, S., & Killen, P. J. (1989). Self-monitoring, surveillance, and incentive effects on cheating. *The Journal of Social Psychology*, *129*(5), 673–679. doi:10.1080/00224545.1989.9713784

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

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 47–60). Berlin, Germany: Springer.

Dember, W. N. (1974). Motivation and the cognitive revolution. *American Psychologist*, *29*(3), 161–168. doi:10.1037/h0035907

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

Dienlin, T. (2015). Ist die politische Meinung privat oder öffentlich? Der Blick der Medienpsychologie. In P. Richter (Ed.), *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data* (pp. 111–126). Baden-Baden, Germany: Nomos. doi:10.5771/9783845264165-111

Dienlin, T., Masur, P. K., & Trepte, S. (2016). Displacement or reinforcement? The reciprocity of FtF, IM, and SNS communication and their effects on loneliness and life-satisfaction. *Manuscript in preparation*.

Dienlin, T. & Metzger, M. J. (2016a). An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*. doi:10.1111/jcc4.12163

Dienlin, T. & Metzger, M. J. (2016b). "Nothing to hide": Predicting the desire for privacy. *Manuscript under review*.

Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. doi:10.1002/ejsp.2049

Eggers, D. (2013). *The circle*. New York, NY: Knopf Publishing Group.

Erlmoser, V. (2016). *Sorry! No data available: Bachelor thesis*. Hohenheim, Germany: University of Hohenheim.

European Commission. (2012). Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Retrieved from www.ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission. (2015.12.15). Agreement on Commission's EU data protection reform will boost Digital Single Market. Retrieved from www.europa.eu/rapid/press-release_IP-15-6321_en.htm

Facebook. (2016). Statement of rights and responsibilities. Retrieved from www.facebook.com/terms.php?locale=de_DE

Fischer, D. & Bates, J. (2008, April). The development and investigation of an IAT for workplace integrity. San Francisco, CA.

Fishbein, M. & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. New York, NY: Psychology Press.

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*(3), 421–471.

Gibson, J. J. (1979/2015). *The ecological approach to visual perception*. New York, NY: Psychology Press.

Hargittai, E. (2010). Digital na(t)ives? Variation in Internet skills and uses among members of the "net generation". *Sociological Inquiry*, *80*(1), 92–113. doi:10.1111/j.1475-682X.2009.00317.x

Heidegger, M. (1927/1996). *Being and time*. New York, NY: State University of New York Press.

Jonassen, D. H. (1991). Objectivism versus constructivism: Do we need a new philosophical paradigm? *Educational Technology Research and Development*, *39*(3), 5–14. doi:10.1007/BF02296434

Jonze, S. (2013). Her. Burbank, CA.

Kammerer, D. (2014). Die Enden des Privaten. Geschichten eines Diskurses. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 243–258). Passau, Germany: Karl Stutz.

Katz, D. (1960). The functional approach to the study of attitudes. *Public Opinion Quarterly*, *24*(2), 163. doi:10.1086/266945

Kelly, G. A. (1991). *The psychology of personal constructs*. London, UK: Routledge.

Knigge, A. (1788/1853). *Über den Umgang mit Menschen* (13. Aufl.). Hannover, Germany: Hahn'sche Hofbuchhandlung.

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

Krasnova, H., 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), 127–135. doi:10.1007/s12599-012-0216-6

Lang, C. & Barton, H. (2015). Just untag it: Exploring the management of undesirable Facebook photos. *Computers in Human Behavior*, *43*, 147–155. doi:10.1016/j.chb.2014.10.051

Laufer, R. S. & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x

Lewin, K. (1935). *A dynamic theory of personality*. New York, NY: McGraw-Hill.

Luhmann, N. (1984). *Soziale Systeme: Grundriss einer allgemeinen Theorie*. Frankfurt, Germany: Suhrkamp.

Lüpken-Räder, G. (2012). *Datenschutz von A - Z*. Freiburg, Germany: Haufe-Lexware.

Marx, K. (1867/1990). *Capital: A critique of political economy*. Penguin classics. London, UK: Penguin Books in association with New Left Review.

Masur, P. K. (2016). *Situational privacy and self-disclosure: Dissertation in preparation*. Hohenheim, Germany: University of Hohenheim.

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). doi:10.1177/2056305116634368

Miller, A. R. (1971). *The assault on privacy: Computers, data banks, and dossiers.* Ann Arbor, MI: University of Michigan Press.

Min, J. & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, *66*(4), 839–857. doi:10.1002/asi.23206

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. doi:10.1111/j.1745-6606.2006.00070.x

Novick, M. R. (1966). The axioms and principal results of classical test theory. *Journal of Mathematical Psychology*, *3*(1), 1–18. doi:10.1016/0022-2496(66)90002-2

Orwell, G. (1950). *1984*. New York, NY: Penguin Books USA Inc.

Park, Y. J. [Y. J.]. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. doi:10.1177/0093650211418338

Park, Y. J. [Yong Jin]. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. doi:10.1016/j.chb.2015.04.011

Poitras, L. (2014). Citizenfour. New York, NY.

Popper, K. (1959/2005). *The logic of scientific discovery*. New York, NY: Routledge.

Rogers, C. R. (1951/2003). *Client-centered therapy: Its current practice, implications and theory*. London, UK: Constable.

Schlag, G. & Wenz, B. (2015.12.19). Ich im Netz: Die Folgen der Selbstdarstellung. Retrieved from www.swr.de/-/id=16215044/property=download/nid=660374/1updb01/swr2-wissen-20151219.pdf

Shibchurn, J. & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. *Computers in Human Behavior*, *44*, 103–117. doi:10.1016/j.chb.2014.10.059

Skinner, B. F. (1953/2014). *Science and human behavior*. Upper Saddle River, NJ: Pearson Education.

Stone, D. L. (1986). Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy. *Perceptual and Motor Skills*, *62*(2), 371–376. doi:10.2466/pms.1986.62.2.371

Strassberg, D. S., McKinnon, R. K., Sustaíta, M. A., & Rullo, J. (2013). Sexting by high school students: An exploratory and descriptive study. *Archives of sexual behavior*, *42*(1), 15–21. doi:10.1007/s10508-012-9969-8

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292. doi:10.1016/j.chb.2015.06.006

Sundar, S. S. (2008). Self as source: Agency and customization in interactive media. In E. Konijn, S. Utz, M. Tanis, & S. B. Barnes (Eds.), *Mediated interpersonal communication* (pp. 58–74). LEA's communication series. New York, NY: Routledge.

Taddei, S. & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. doi:10.1016/j.chb.2012.11.022

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. doi:10.1111/jcc4.12052

Treem, J. W. & Leonardi, P. M. (2013). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. In C. T. Salmon (Ed.), *Communication yearbook 36*. Oxford, UK: Routledge.

Trepte, S. (2015). Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media + Society*, *1*(1). doi:10.1177/2056305115578681

Trepte, S., Dienlin, T., & Reinecke, L. (2013). Privacy, self-disclosure, social support, and social network site use. Research report of a three-year panel study. Retrieved from University of Hohenheim website: http://opus.uni-hohenheim.de/volltexte/2013/889/.

Trepte, S., Dienlin, T., & Reinecke, L. (2014a). Influence of social support received in online and offline contexts on satisfaction with social support and satisfaction with life: A longitudinal study. *Media Psychology*, *18*(1), 74–105. doi:10.1080/15213269.2013.838904

Trepte, S., Dienlin, T., & Reinecke, L. (2014b). Risky behaviors. How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis* (Vol. 41, pp. 225–244). Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft. Konstanz, Germany: UVK.

Trepte, S., Masur, P. K., Scharkow, M., & Dienlin, T. (2015). Privatheitsbedürfnisse verschiedener Kommunikationstypen on- und offline. *Media Perspektiven*, (5), 250–257.

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). Berlin, Germany: Springer. doi:10.1007/978-3-642-21521-6{_}6

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (Vol. 20, pp. 333–365). Dordrecht, Netherlands: Springer.

Trepte, S., von Pape, T., & Dienlin, T. (2016). *Trendmonitor Privatheit 2016: Welche Perspektiven werfen deutsche Bürger und deutsche Medien auf das Thema Privatheit im digitalen Zeitalter?* Stuttgart, Germany: University of Hohenheim.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36. doi:10.1177/0270467607311484

Wälde, R. (2012). Privacy Knigge schützt die Privatsphäre in sozialen Netzwerken. Retrieved from www.mupaki.de/downloads/Privacy_Knigge_Deutscher_Knigge_Rat.pdf

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(1). doi:10.5817/CP2012-1-3

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

Watzlawick, P. (1984). *The invented reality: How do we know what we believe we know? Contributions to constructivism* (1st ed). New York, NY: Norton.

West, P. M., Brockett, P. L., & Golden, L. L. (1997). A comparative analysis of neural networks and statistical methods for predicting consumer choice. Marketing Science, 16(4), 370-391. *Marketing Science*, *16*(4).

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52. doi:10.1016/j.dss.2010.11.017

Zimbardo, P. G., Gerrig, R. J., & Graf, R. (2008). *Psychologie* (18th ed.). Munich, Germany: Pearson Studium.

Znaniecki, F. (1919). *Cultural reality*. Chicago, CH: University of Chicago Press.

List of figures

List of tables

Acknowledgements

First and foremost I want to thank my advisor and co-author Prof. Dr. Sabine Trepte. I want to thank you for all your encouragement, motivation, feedback, and inspiration. Sabine, you enabled so many things: the stipend, the conferences, the research stays at OSU and UCSB, ... All in all, I want to thank you, Sabine, for making this thesis possible.

I want to express so many thanks to my co-author Prof. Dr. Miriam Metzger. I thank you for welcoming me at UCSB, for your incredible help with setting up the questionnaires and doing the IAT at UCSB. I want to thank you, Miriam, for all the time you have very generously invested in me — it is so great working together with you!

I thank Prof. Dr. Nicole Krämer, who is the second advisor of this thesis. Thank you, Nicole, for your support: You were one of the first to provide valuable feedback on my first ideas at the ICA's doctoral consortium in London in 2013, and I feel privileged that you accompanied me until the dissertation's very last moments — thank you so much!

I want to thank all my colleagues at the University of Hohenheim. I especially want to thank Philipp Masur: Thank you Philipp, for not just being a colleague but a true friend. I want to thank you for your continual support and the willingness to always discuss my ideas. I also want to thank Michael Scharkow: Thank you for all your statistical advice and your help with R and LaTeX. Thank you Cornelia, Doris, Josi, Laura, Max, Thilo, and Susanne for all your help throughout the years!

I want to thank Adam Boger, Alyea Sandovar, Benjamin K. Johnson, Laura Willis-Abdurraqib, and Simon Garnett for feedback (especially in terms of language!). I express thanks to Aylin Ögun, Henning Müller, Leonard Reinecke, Ricarda Moll, Roland Toth, and Stefan Mayer, who contributed either actively or passively, but at any rate very significantly to this thesis.

I want to thank the Studienstiftung des deutschen Volkes for the stipend that made this dissertation possible. I want to express thanks to the Hamburg Media School, the University of Hohenheim, the Ohio State University, and the University of Santa Barbara. I want to thank Silvia Knobloch-Westerwick, Ronald Rice, Andrew Flanagin, and Lasse Lindekilde, who either welcomed me at their departments or homes.

I want to thank my family, my friends, and my girlfriend — I want to thank you for your continual support, your understanding, and your love. Auf Physio!

Declaration of pre-published parts

Designated parts of this cumulative dissertation entitled "The psychology of privacy: Analyzing processes of media use and interpersonal communication" have been published. These include Chapter 2 (*The privacy process model*), Chapter 3 (*Is the privacy paradox a relic of the past?*), and Chapter 4 (*The extended privacy calculus model for SNSs*). Chapter 5 (*Predicting the desire for privacy*) has currently been submitted for publication at an academic journal.

The content of the texts has not been altered. For reasons of consistency, some minor changes in formatting have been carried out. Similarly, the language and the formatting of Chapter 2 (*The privacy process model*) have been changed from British English to American English.

Chapter 2, 3, and 4 have been published as follows:

- Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. doi:10.1002he/sheejsp.2049.

- Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs — Analyzing self-disclosure and privacy behaviors in a representative U.S. sample. *Journal of Computer-Mediated Communication, 21*, 368–383. doi:10.1111/jcc4.12163

Declaration of individual contribution

Study 1: The privacy process model The research question, the design of the privacy process model, and the writing of the study were either developed or carried out by Tobias Dienlin. Prof. Dr. Sabine Trepte, who is the advisor of this dissertation, accompanied the development of the PPM and provided continuous feedback.

Study 2: Is the privacy paradox a relic of the past? The research question, the design of the questionnaire, the statistical analyses, and the writing of the study were either developed or carried out by Tobias Dienlin. Prof. Dr. Sabine Trepte, who is the advisor of this dissertation, accompanied the process, provided continuous feedback, and individually authored the paragraph *A second answer* (section 3.2.2 on page 56).

Study 3: The extended privacy calculus model for SNSs The study is the first analysis of data that Prof. Dr. Miriam J. Metzger collected in October 2012. The research question, the statistical analyses, and the writing of the study were either developed or carried out by Tobias Dienlin. The manuscript was co-authored by Prof. Dr. Miriam J. Metzger, who accompanied the process, contributed the initial data set, provided continuous feedback, and individually authored the paragraph *Conclusion* (section 4.7.3, page 111).

Study 4: Predicting the desire for privacy The research question, the design of the questionnaires, the design of the experiment, the statistical analyses, and the writing of the study were either developed or carried out by Tobias Dienlin. The manuscript was co-authored by Prof. Dr. Miriam J. Metzger, who accompanied the process, provided continuous feedback, and supervised the conduction of the experiment at the laboratories of UCSB.

You are invisible now,
got no secrets to conceal.

Bob Dylan, Like a Rolling Stone