



INFORMATION PRIVACY IN THE DIGITAL AGE

THEORETICAL FOUNDATION AND EMPIRICAL EVIDENCE

Jakob Wirth
University of Bamberg

INFORMATION PRIVACY IN THE DIGITAL AGE

THEORETICAL FOUNDATION AND EMPIRICAL EVIDENCE

Dissertation in der Fakultät Wirtschaftsinformatik und Angewandte Informatik der Otto-Friedrich-Universität Bamberg

Erstgutachter: Prof. Dr. Tim Weitzel

Zweitgutachter: Prof. Dr. Daniel Beimborn

Mitglied der Promotionskommission: Prof. Dr. Dominik Herrmann

Tag der Disputation: 28. April 2020

URN: urn:nbn:de:bvb:473-irb-478454

DOI: <https://doi.org/10.20378/irb-47845>

Lizenz: Creative Commons - CC BY - Namensnennung 4.0 International



Dedicated to Maike

TABLE OF CONTENT

Dedication by Prof. Dr. Tim Weitzel (Widmung)	6
Acknowledgements	7
German Summary (Zusammenfassung)	8
Introductory Paper	12
<i>Information Privacy in the Digital Age: Theoretical Foundation and Empirical Evidence</i>	
Chapter I: Literature Review on Privacy	102
Paper I	103
Jakob Wirth <i>Dependent Variables in the Privacy-Related Field: A Descriptive Literature Review</i> Proceedings of the 51st Hawaii International Conference on System Sciences (2018), Waikoloa Village, Hawaii	
Chapter II: Privacy Ownership	104
Paper II	105
Jakob Wirth, Christian Maier, Sven Laumer <i>Justification of Mass Surveillance: A Quantitative Study</i> Proceedings of the 14th International Conference on Wirtschaftsinformatik (2019), Siegen, Germany	
Paper III	106
Jakob Wirth, Christian Maier, Sven Laumer <i>The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: An Empirical Analysis</i> Proceedings of the 26th European Conference on Information Systems (2018), Portsmouth, UK	
Chapter III: Privacy Control	107
Paper IV	108
Jakob Wirth, Christian Maier, Sven Laumer <i>Subjective Norm and the Privacy Calculus: Explaining Self-Disclosure on Social Networking Sites</i> Proceedings of the 27th European Conference on Information Systems (2019), Stockholm & Uppsala, Sweden	
Paper V	109
Jakob Wirth, Christian Maier, Sven Laumer, Tim Weitzel <i>Laziness as an explanation for the privacy paradox: An empirical investigation with multiple snapshots</i>	

Paper VI	Christian Maier, Sven Laumer, Jakob Wirth, Tim Weitzel <i>Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples</i> European Journal of Information Systems (28:5), pp. 496–522 (2019)	136
Paper VII	Jakob Wirth, Christian Maier, Sven Laumer, Tim Weitzel <i>The Effect of Mindfulness on Threat Appraisal and Coping Appraisal: An Empirical Analysis</i>	137
Paper VIII	Jakob Wirth, Christian Maier, Sven Laumer, Tim Weitzel <i>Anchoring Influences Actual Disclosure: Four Studies on the Amount and Accuracy of Information Disclosure</i>	162
Paper IX	Jakob Wirth, Christian Maier, Sven Laumer, Tim Weitzel <i>Perceived Information Sensitivity and Interdependent Privacy Protection: A Quantitative Study</i> electronic markets (29:3), pp. 359–378 (2019)	186
Chapter IV: Privacy Turbulence		187
Paper X	Jakob Wirth <i>Strength of Ties as an Antecedent of Privacy Concerns: A Qualitative Research Study</i> Proceedings of the 23rd Americas Conference on Information Systems (2017), Boston, MA, USA	188
Paper XI	Jakob Wirth, Christian Maier, Sven Laumer, Tim Weitzel <i>Drivers of Email Tracking Privacy Protection Behavior: A Two-Wave Quantitative Study</i>	189
Appendix		216
Publications		217

DEDICATION BY PROF. DR. TIM WEITZEL (WIDMUNG)

*An American has no sense of privacy.
He does not know what it means.
There is no such thing in the country.
(GB Shaw, 1933)*

*Privacy is a big deal for social media
(Internet Meme, 2020)*

Viele reden von Privacy, alle finden Privacy wichtig, aber - wie bei Sport oder gesunder Ernährung - verhalten sich die Wenigsten so, wie sie eigentlich wollen. Warum ist das so? Dr. Jakob Wirth bietet in seiner Dissertationsschrift wohlfundierte, originelle Antworten, die die Forschung wie Praxis bereichern.

INFORMATION PRIVACY IN THE DIGITAL AGE gelingt es, in einem wichtigen und wohlerforschten Themenfeld bestehende Literatur und neue Ideen zu verbinden, um somit Beiträge zu „klassischen“ Fragen der Privacy-Forschung zu erarbeiten. Dr. Wirth identifiziert und formuliert Variablen und Hypothesen, die etwa das Privacy Paradox etwas besser zu erklären helfen und legt Grundbausteine für eine relationale Privacy-Theorie. So weist er theoretisch wie empirisch den (direkten und indirekten) Einfluss von Resignation, anderen Personen und individueller Faulheit auf Privacy-Verhalten im Rahmen des Privacy Calculus nach. Wunderbare Experimente zu Cognitive Biases zeigen, dass die (manipulierte) Eingabefeldgröße in Webformularen Art und Genauigkeit freiwillig bereitgestellter, privacy-relevanter Informationen mitbestimmt und wie (im Experiment beeinflusste) „Angst“ das Privacy-Verhalten verändert.

Neben derartigen inhaltlich wie methodisch originellen Forschungsansätzen ist die sorgfältige und kenntnisreiche Literaturarbeit beeindruckend und ermöglicht das Identifizieren und Beantworten offener sowie das Stellen neuer Fragen. Damit hat Dr. Wirth nicht nur eine exzellente wissenschaftliche Arbeit vorgelegt, sondern auch vielversprechende Wege für die zukünftige Forschung aufgezeigt.

Das Wirtschaftsprüfungs- und Steuerberatungsunternehmen Deloitte¹ formulierte als ein Ziel zu Beginn des Jahres 2020 im Eindruck der erlebten GDPR-Unruhen (und offenbar vor der COVID-19-Pandemie): „Looking forward to 2020: making privacy awareness fun“. Die Dissertationsschrift von Dr. Wirth erfüllt diesen Anspruch und kann jedem, der sich für Privacy-Forschung interessiert, ebenso dringend empfohlen werden wie Nachwuchswissenschaftlern, die Vorlagen für ernsthafte und gleichzeitig moderne Forschungsarbeiten suchen.

¹ <https://www2.deloitte.com/nl/nl/pages/risk/articles/looking-forward-to-2020-making-privacy-awareness-fun.html>

ACKNOWLEDGEMENTS

Writing this dissertation has been an intellectual journey for me. Without the support of many people, I would never have embarked on this journey, not to mention reached its goal. I wish to extend my sincerest thanks to my thesis supervisor, my colleagues, my friends and my family who supported me along this journey.

First and foremost, I would like to thank my PhD supervisor, Prof. Dr. Tim Weitzel, for giving me the opportunity to write my dissertation with him. I remember Tim's shining eyes when I first mentioned any new idea and his passionate support for exploring this idea further. I have always admired Tim's tireless inquisitiveness, which has always inspired me to delve deeper into my research. Tim always provided very valuable input, gave me room to be as flexible as I needed, and was always open for intellectual exchange, questions and needs, but also for every entertaining conversation. This created an ideal working environment for writing a dissertation, for which I am very grateful. I would also like to thank Prof. Dr. Daniel Beimborn and Prof. Dr. Dominik Herrmann for their willingness to be part of my PhD committee, for their interest in my work and for their help, tips and advice.

Special thanks also to two extraordinary researchers: Dr. Christian Maier and Prof. Dr. Sven Laumer. My dissertation would not have been possible without them. Through countless paper revisions, discussion groups, e-mails and conversations, they have helped me to keep moving forward and explore a little further. Especially their openness to trying out new things has always inspired and deeply impressed me. I remember when I had already been working at the department chair for some time, I told both of them that I would like to take a closer look at the subject "information privacy". Both were immediately hooked and offered to help me. I am extremely grateful for such openness, which is anything but commonplace. I am especially grateful to both for supporting me even in the difficult phases of my dissertation and for inspiring me to move forward. I am extremely honored that extraordinary researchers like Christian and Sven have supported me over the past years.

I would also like to thank my current and former colleagues Dr. Thomas Friedrich, Dr. Christoph Weinert, Dr. Robert Rockmann, Caroline Oehlhorn, as well as Axel Hund, Dr. Janina Kettenbohrer, Jens Mattke, Dr. Bernhard Moos, Katharina Pflügner, Lea Reis, Diana Renner and Gudrun Stilkerich for their generous support and for many wonderful moments away from work.

Special thanks to my friends, who always managed to change my outlook and maintain a healthy distance from my dissertation, especially in difficult times. I particularly want to mention the help of my friends Dorothee and Miriam, who gave me very valuable insights into particular research projects.

I owe my family, especially my siblings and my mother, but also my parents-in-law and brothers-in-law, a big thank you for accompanying me on this journey and for always giving me courage and helping me to follow my path over the last years. Finally, my biggest thanks go to my dear wife, Maike, and my son, Jonathan. Maike has always believed in me, supported me in every possible way and bolstered me with her love. Without her, this dissertation would not have been possible. My special thanks also to Jonathan for the creative breaks and the endless joy he brings to my life.

GERMAN SUMMARY (ZUSAMMENFASSUNG)

Technologien im digitalen Zeitalter, wie bspw. das Internet oder smarte Geräte, haben dazu beigetragen, dass persönliche Informationen von Individuen viel schneller und in völlig neuen Größenordnungen gesammelt, verarbeitet und weitergegeben werden können (Carnegie and Abell 2009; Lane and Levy 2019; Solove 2006).

Das weckt die Begehrlichkeiten von Organisationen. Sie können neue Produkte und Services entwerfen und bessere Managemententscheidungen treffen, wenn sie Zugang zu solch persönlichen Informationen haben und sie zu ihren Gunsten auswerten und weitergeben können (Posey et al. 2017). Gleichzeitig ist der Staat bemüht, den Menschen Kontrolle über ihre persönlichen Informationen zu verschaffen (Kokolakis 2017). Die Datenschutzgrundverordnung ist hierfür ein Beispiel (Politou et al. 2018).

Vereinfacht gesagt führt Kontrolle von Informationen dazu, dass Individuen ihre privacy² schützen können (Clarke 1999; Petronio and Altman 2002; Smith et al. 2011). Zu einem gewissen Grad können Individuen den Schutz ihrer privacy selbst beeinflussen (Dinev et al. 2015; Petronio 2013; Petronio and Altman 2002): Wenn sie persönliche Informationen von sich preisgeben, dann erhöht sich die Gefahr, dass ihre privacy gefährdet ist – wenn sie persönliche Informationen für sich behalten, dann ist diese Gefahr geringer. Diese Entscheidung, die eigene privacy zu kontrollieren, ist der Hauptfokus von privacy management (Petronio 2013). Organisationen, die den Zugang zu persönlichen Informationen anstreben und der Staat, der versucht, Bürgern Kontrolle über ihre persönlichen Informationen zu geben, haben also beide ein starkes Interesse daran, zu verstehen, wie Individuen ihre privacy managen und damit auch mit ihren persönlichen Informationen umgehen.

Tatsächlich zeigt sich zunächst, dass Individuen um ihre privacy sehr besorgt sind (statista.com 2019b). Allerdings ist das Verhalten von Individuen inkonsistent. Auf der einen Seite versuchen sie zwar, ihrer Besorgnis Ausdruck zu verleihen, indem sie persönliche Informationen manchmal zurückhalten (statista.com 2015, 2018a, 2018b) – auf der anderen Seite geben sie häufig viele persönliche Informationen preis (Marr 2018; statista.com 2019a, 2019c).

Aus Forschungssicht wurde bereits viel getan, um dieses Verhalten und damit das Management von privacy zu verstehen (Acquisti and Grossklags 2005; Dinev and Hart 2006; Li 2011). Allerdings wurde auch häufig auf weiteren Forschungsbedarf hingewiesen (Bélanger and Crossler 2011; Dinev et al. 2015; Smith et al. 2011). Diese Dissertation hat das Ziel, zu dieser Forschungsdomäne beizutragen, indem sie tiefergehend erklärt, wie Individuen ihre privacy managen. Die Forschungsfrage lautet:

Wie managen Individuen ihre privacy?

Um die Forschungsfrage zu beantworten, wird diese Dissertation anhand der „communication privacy management theory“ (Petronio 2013; Petronio and Altman 2002) strukturiert. Die Theorie betrachtet ganzheitlich, wie Individuen ihre privacy managen. Der Fokus liegt hierbei auf der Kontrolle über die Freigabe oder das Zurückhalten persönlicher Informationen (privacy control). Ebenfalls wird

² Obwohl dies eine deutsche Zusammenfassung darstellt, wird der englische Begriff *privacy* (auch *information privacy* genannt) verwendet. Dieser wird in der Literatur grob umrissen als das Ausmaß der Kontrolle über persönliche Informationen definiert (Clarke 1999) und diese Definition wird auch in der Dissertation angewandt. Die beiden deutschen möglichen Äquivalente sind die Begriffe "Datenschutz" und "Privatsphäre". Gründe, dennoch den Begriff *privacy* zu verwenden, sind die folgenden: Datenschutz betrachtet den tatsächlichen „Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten“ (Witt 2010, p. 4). Es wird also weniger das Ausmaß der Kontrolle, sondern das Recht von Individuen auf informationelle Selbstbestimmung betrachtet. Privatsphäre wäre der passendere Begriff zu *privacy*, da Privatsphäre Individuen „Kontrolle über ihre Selbstdarstellung garantiert“ (Hotte 2010, p. 44). Jedoch beinhaltet Privatsphäre auch die physische Privatsphäre. Es müsste daher eher von informationeller Privatsphäre gesprochen werden, wobei diese Begriffe wiederum mit Privatheit oder informationeller Privatheit vermischt werden. Insgesamt ist Privatsphäre daher ein Begriff, der nicht klar definiert ist (Hotter 2011). Um mit den Begrifflichkeiten der *communication privacy management theory*, die die Basis für die Strukturierung der Dissertation legt, einher zu gehen und auch, um Unklarheiten bzgl. des zentralen Begriffs der Dissertation möglichst zu vermeiden, wird daher hier, trotz einer deutschen Zusammenfassung, der englische Begriff *privacy* verwendet.

aber auch behandelt, wie Individuen die Eigentümerschaft von persönlichen Informationen betrachten (privacy ownership) und wie sie sich verhalten, sollte ihre privacy eingeschränkt werden (privacy turbulence) (Petronio 2013; Petronio and Altman 2002).

Die Dissertation setzt sich aus elf Studien zusammen, die anhand dieser drei Elemente strukturiert werden. Die Ergebnisse zeigen, dass das Management von privacy von vielen verschiedenen Faktoren abhängt und komplex ist. So zeigt sich, dass Individuen die momentane Massenüberwachung durch den Staat häufig gutheißen, v.a. dann, wenn sie sich dadurch einen Sicherheitsgewinn versprechen. Ein möglicher Verlust an privacy durch Massenüberwachung spielt jedoch keine Rolle bei der Frage, ob man Massenüberwachung unterstützt oder nicht. Gleichzeitig zeigt sich auch, dass Individuen häufig bereits aufgegeben haben, ihre privacy zu schützen. Das führt dazu, dass mögliche privacy-Risiken durch Datenpreisgabe weniger einen Einfluss auf ihr Verhalten haben, während mögliche Vorteile durch die Datenpreisgabe überproportional wichtig werden. Beide Ergebnisse haben einen Einfluss darauf, wie Individuen die Eigentümerschaft (privacy ownership) ihrer persönlichen Informationen betrachten.

Aus Sicht der eigentlichen Kontrolle der privacy (privacy control) zeigt sich, dass Individuen ihre Entscheidung zur Datenpreisgabe auch davon abhängig machen, was ihrem Eindruck nach andere von ihnen erwarten. Ist der Erwartungsdruck zur Datenpreisgabe hoch, dann geben sie diesem Druck häufig nach. Darüber hinaus gehen die Ergebnisse auf individuelle Persönlichkeitsmerkmale ein, die das Verhalten von Individuen bzgl. ihrer privacy beeinflussen. So sind faule Individuen, die um ihre privacy besorgt sind, weniger bereit, dieser Besorgnis auch Taten folgen zu lassen als weniger faule Leute. Zudem sehen Individuen, die generell achtsam in Bezug auf privacy sind, auch tatsächlich mehr Gefahren. Allerdings sehen sie sich gleichzeitig aber auch eher in der Lage, ihre eigene privacy zu schützen. Die Ergebnisse zeigen des Weiteren auch, dass Individuen bei der Frage, ob sie Informationen preisgeben sollen oder nicht, nicht immer alles durchdenken. Sie lassen sich auch durch einen sogenannten Ankereffekt beeinflussen. Beispielsweise zeigen die Ergebnisse, dass Individuen mehr Informationen preisgeben, wenn das Textfeld, in dem sie die Informationen eintragen sollen, ein großes Textfeld ist. Im Vergleich dazu geben Individuen, denen ein kleines Textfeld angezeigt wird, weniger Informationen preis, obwohl die Anfrage zur Informationspreisgabe identisch ist. Eine Erklärung hierfür ist, dass Individuen die Größe des Textfeldes als „Anker“ betrachten, auf den sie sich stützen, wenn sie selbst nicht genau wissen, wie viele Informationen sie in der Situation preisgeben sollen. Ein weiteres Ergebnis der Dissertation ist, dass Individuen nicht nur ihre eigene privacy kontrollieren – sie können zu einem Teil auch die privacy anderer kontrollieren, sobald sie Zugang zu deren Informationen haben. Dabei beurteilen Individuen vor allem die Sensitivität von Informationen und fragen sich, welche negativen Auswirkungen eine Preisgabe von Informationen haben könnte – für sie selbst aber vor allem auch für diejenigen, denen diese Informationen eigentlich gehören.

Schlussendlich betrachten die Ergebnisse auch den Fall, dass die privacy von Individuen beeinträchtigt wurde (privacy turbulence). Hier zeigt sich, dass es für Individuen einen Unterschied macht, wer der Verursacher einer Beeinträchtigung ist – ein nahes Familienmitglied, ein entfernter Bekannter oder ein gänzlich Unbekannter, wie bspw. ein Geheimdienst. Zudem weisen die Ergebnisse auch darauf hin, dass im digitalen Zeitalter Individuen häufig gar nicht wissen, dass ihre privacy beeinträchtigt ist, weil Informationen über sie unwissentlich preisgegeben wurden. Klärt man die Individuen jedoch auf und versucht sie zudem zu einem gewissen Grad zu ängstigen, so steigt die Chance, dass die Individuen versuchen, den Schutz ihrer privacy wiederherzustellen.

Diese Ergebnisse haben Auswirkungen auf die Forschung im Bereich privacy aber auch für die Praxis. So wird mit den Ergebnissen die Betrachtungsweise der „communication privacy management theory“ in Frage gestellt, dass sich Individuen immer als alleiniger Eigentümer ihrer persönlichen Informationen sehen. Das wiederum kann Auswirkungen darauf haben, wie sie ihre privacy kontrollieren. Beispielsweise können Forscher auf Basis der Ergebnisse der Dissertation auf ein

erweitertes Konzept von Informationssensitivität zurückgreifen oder den Ankereffekt in ihren eigenen Studien tiefergehend betrachten. Auch die Einbeziehung von individuellen Persönlichkeitsmerkmalen hilft, bestehende Theorien in der privacy-Forschung besser zu verstehen. Zudem tragen die Ergebnisse zur privacy-Forschung bei, indem aufgezeigt wird, dass es für Individuen einen Unterschied macht, wer eine mögliche Beeinträchtigung ihrer privacy verursacht hat.

Aus organisationaler Sicht zeigt diese Dissertation auf, dass bspw. soziale Netzwerke nicht nur das Individuum selbst, sondern auch für sie wichtige Personen in Betracht ziehen sollten. Organisationen hätten zudem die Möglichkeit, bspw. mittels des Ankereffekts, Individuen zur Datenpreisgabe zu manipulieren – hier müssen Organisationen aber auch ethische Grundsätze mit einbeziehen. Diese Dissertation beleuchtet zudem den Umstand, dass Individuen bereits aufgegeben haben könnten, ihre privacy zu schützen. In solchen Fällen sollte der Staat versuchen, zu zeigen, dass seine Gesetzgebung auch tatsächlich effektiv ist. Zudem wird der Fall untersucht, dass persönliche Informationen von Individuen ohne deren Wissen preisgegeben wurden, was v.a. durch das digitale Zeitalter vermehrt auftritt. Der Staat sollte hier dazu beitragen, dass solch unwissentliche Datenpreisgabe nicht stattfindet, wenn das Ziel des Schutzes der Kontrolle über persönliche Informationen beibehalten werden soll.

Insgesamt betrachtet geben die Ergebnisse der hier vorliegenden Dissertation einen Einblick darin, wie Individuen ihre privacy managen. Die Ergebnisse zeigen, dass das management der privacy komplex ist und viele Faktoren betrachtet werden müssen. Die daraus für Forschung und Praxis abgeleiteten Implikationen werden vorgestellt.

LITERATURVERZEICHNIS

- Acquisti, A., and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security & Privacy* (3:1), pp. 26–33.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.
- Carnegie, T. A. M., and Abell, J. 2009. "Information, Architecture, and Hybridity: The Changing Discourse of the Public Library," *Technical Communication Quarterly* (18:3), pp. 242–258.
- Clarke, R. 1999. "Internet privacy concerns confirm the case for intervention," *Communications of the Association for Information Systems* (42:2), pp. 60–67.
- Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61–80.
- Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* (26:4), pp. 636–655.
- Hotter, M. 2011. *Privatsphäre: Der Wandel eines liberalen Rechts im Zeitalter des Internets*, Frankfurt am Main: Campus Verlag GmbH.
- Kokolakis, S. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* (64), pp. 122–134.
- Lane, K., and Levy, S. J. 2019. "Marketing in the Digital Age: A Moveable Feast of Information," in *Marketing in a digital world*, A. Rindfleisch and A. J. Malter (eds.), Bingley: Emerald Publishing, pp. 13–33.
- Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the Association for Information Systems* (28:28), pp. 453–496.
- Marr, B. 2018. How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/>. Accessed 28 March 2019.
- Petronio, S. 2013. "Brief Status Report on Communication Privacy Management Theory," *Journal of Family Communication* (13:1), pp. 6–14.
- Petronio, S. S., and Altman, I. 2002. *Boundaries of privacy: Dialectics of disclosure*, Albany, NY: State University of New York Press.

- Politou, E., Alepis, E., and Patsakis, C. 2018. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *Journal of Cybersecurity* (4:1), p. 1.
- Posey, C., Raja, U., Crossler, R. E., and Burns, A. J. 2017. "Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA," *Eur J Inf Syst* (26:6), pp. 585–604.
- Smith, J. H., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 980–1015.
- Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477–564.
- statista.com 2015. Leading actions taken by consumers due to online privacy concerns in Great Britain (GB) in January 2015 and December 2015. <https://www.statista.com/statistics/507115/leading-actions-taken-due-to-online-privacy-concerns-in-great-britain-gb/>. Accessed 3 April 2019.
- statista.com 2018a. Facebook usage changers over privacy concerns by adults in the United States as of April 2018. <https://www.statista.com/statistics/972877/behavioral-changes-consumers-facebook-privacy-concerns-usa/>. Accessed 3 April 2019.
- statista.com 2018b. Least common actions undertaken to protect data on the internet in Australia as of August 2018. <https://www.statista.com/statistics/958030/australia-least-common-actions-taken-to-protect-data/>. Accessed 3 April 2019.
- statista.com 2019a. Media usage in an internet minute as of March 2019. <https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/>. Accessed 17 December 2019.
- statista.com 2019b. Share of internet users who are concerned about risks to their online privacy vs. their willingness to accept certain risks to their online privacy to make their life more convenient as of October 2018, by country. <https://www.statista.com/statistics/1023952/global-opinion-concern-internet-privacy-risk-convenience/>. Accessed 29 October 2019.
- statista.com 2019c. Smart speaker with intelligent personal assistant ownership rate among U.S. broadband households from 2017 to 2019. <https://www.statista.com/statistics/791575/us-smart-speaker-household-ownership/>. Accessed 29 January 2020.
- Witt, B. C. 2010. *Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung*, Wiesbaden: Vieweg.



Introductory Paper

1 INTRODUCTION

“If this is the age of information, then privacy is the issue of our times” (Acquisti et al. 2015, p. 509)

The way personal information can be processed has changed in the digital age, or the age of information. The digital age has given rise to technologies such as personal computers and smart devices, which are supplemented and enhanced by the Internet. Such technologies enable personal information to be collected, processed and disseminated faster and on a larger scale than ever before (Carnegie and Abell 2009; Lane and Levy 2019; Solove 2006).

This has also changed how organizations and the state perceive and handle such personal information. By taking advantage of new ways to collect and process personal information, organizations can design better products and services, make better management decisions and outperform their competitors (Dinev and Hart 2006). Organizations therefore often have a keen interest in access to personal information (Dinev et al. 2006; Posey et al. 2017). In an effort to protect the individual, the state responds to private efforts to collect and process personal information by introducing laws that help citizens control their personal information. One example is the European Union’s General Data Protection Regulation (GDPR) that helps individuals retain control over their personal information (Politou et al. 2018). The state justifies such laws on the grounds that it is in the interest of citizens to control their personal information (Kokolakis 2017).

Broadly speaking, being able to control one’s personal information is critical to protecting one’s privacy (Clarke 1999; Petronio and Altman 2002; Smith et al. 2011). To some degree, the level of privacy can be maintained by the individual herself (Dinev et al. 2015; Petronio 2013; Petronio and Altman 2002): If the individual discloses personal information, her level of privacy is potentially lower. If the individual does not disclose personal information, privacy is potentially protected because the individual is more likely able to maintain control over her personal information. Deciding to either increase or to lower ones’ level of privacy is the main focus of privacy management (Petronio 2013). For organizations that rely on personal information and thus on how individuals manage their privacy, and for the state that bases its privacy laws on its citizens’ privacy management decisions, it is thus important to understand how individuals manage their privacy.

Also, from an individual perspective, privacy management is a key global concern. According to a recent survey, 83 percent of citizens worldwide are concerned about their privacy (statista.com 2019c), and 81 percent of EU citizens (statista.com 2015a) and 91 percent of US citizens believe that they only have partial or no control over their privacy (Madden 2014). The lack of privacy can have serious implications. For example, 22 percent of US citizens who use the Internet have been victims of identity theft caused by a loss of privacy (statista.com 2018c). This in turn has led to widespread fraud costing an estimated \$16 billion in annual damages (Grant 2017).

However, individuals manage their privacy inconsistently. On the one hand, they give away huge volumes of data. For example, 95,000,000 photos and videos get uploaded to Instagram every day (Marr 2018), 41,600,000 mobile messages get sent every minute (statista.com 2019b), and 31 percent of US broadband households use smart speakers such as Alexa or Google Home (statista.com 2019d). Overall, more information is being disclosed today than ever before (Jetzek et al. 2013). On the other hand, individuals also protect their privacy. For example, 31 percent of individuals in the UK have stopped using a website because of privacy concerns, and 53 percent have withheld personal information at times (statista.com 2015c). Furthermore, nine percent of US citizens with access to the Internet have deleted their Facebook account because of privacy concerns (statista.com 2018a), and 29 percent of Australian individuals have used a false name on the Internet to protect their privacy (statista.com 2018b).

Some reasons for this inconsistent behavior have been identified by research. For example, the privacy calculus shows that individuals weigh the benefits of disclosing personal information against the privacy risks involved. The information is only disclosed if the expected benefits outweigh the estimated risks (Dinev and Hart 2006). Other explanations relate to the cognitive effort individuals put into managing their privacy (Acquisti and Grossklags 2005) or individual differences such as personality traits that affect the way how individuals manage their privacy (Junglas et al. 2008). Nevertheless, scholars call for a better understanding of how individuals manage their privacy (Bélanger and Crossler 2011; Dinev et al. 2015; Pavlou 2011; Smith et al. 2011).

The aim of this dissertation is to expand this stream of research by explaining in more detail how individuals manage their privacy, in answer to the overarching research question:

How do individuals manage their privacy?

To answer the research question, the **communication privacy management theory (CPM)** (Petronio 2013; Petronio and Altman 2002) is applied as an overarching scheme (Farrell et al. 2014). The CPM is a theory that explains on a general level the entire process of how individuals manage their privacy, including but not limited to the decision to disclose or conceal personal information. The CPM contains three basic elements: *privacy ownership*, which is how individuals think about who owns their personal information; *privacy control*, which is how individuals control their privacy by disclosing or concealing information; and *privacy turbulence*, which is how privacy can be maintained by individuals if others have unwanted access to their personal information (Petronio 2013; Petronio and Altman 2002).

To understand the management of privacy, all three elements of the CPM need to be considered and understood (Petronio 2013; Petronio and Altman 2002). However, the three elements of the CPM are neither in a causal order, nor do they reveal causal relationships that explain the management of privacy, nor do they provide concrete theoretical insights into how individuals manage their privacy (Petronio and Altman 2002). To fill these gaps, eleven papers constituting this dissertation collectively answer the overall research question of this dissertation which is how individuals manage their privacy. Given the digital age context of this dissertation, the individual is considered to be a user of technology which has been introduced by the digital age. Furthermore, the perspective of the individual is a private individual perspective and not the perspective of an employee in an organization, mirroring the shifting focus in privacy research from the employee perspective to the individual in the private domain (Li 2011b).

The papers constituting this dissertation apply various lenses and concepts to understand the cause-effect relationships in the context of the management of privacy. These theoretical lenses and concepts are presented in the following section on the theoretical background in this **introductory paper**. Afterwards, the CPM is presented as a useful way to structure the main findings of the eleven papers. In the following, the papers' methodologies are discussed, and the main results of the eleven papers and their contributions to literature and practice are summarized. The remainder of this dissertation consists of the eleven papers structured in four chapters, following CPM structure, except for chapter I (see Figure 1).

Chapter I: Literature Review on Privacy

This chapter consists of **Paper I**³. **Paper I** provides an overview of the current state of research in the domain of privacy. It gives an overview of the dependent variables, theories and methodologies used, as well as the research contexts. Based on this literature review, several research gaps are

³ The literature review has been updated to also cover the most recent findings. The key results have not changed. More details are given in the appendix (section 8.1) of the introductory paper.

identified, many of which are filled by the ten remaining papers.

Chapter II: Privacy Ownership

This chapter consists of **Paper II** and **Paper III**, which both focus on privacy ownership. **Paper II** shows how individuals respond to mass surveillance of governmental agencies, which gives individuals less freedom to manage their privacy. **Paper III** demonstrates how individuals may have given up on being able to protect their privacy and what consequence that may have.

Chapter III: Privacy Control

This chapter presents six papers focusing on privacy control. **Paper IV** investigates how individuals' control of their own private information is influenced by other individuals around them. **Paper V**, **Paper VI** and **Paper VII** focus on the influence of individual differences on privacy control. In more particular, **Paper V** examines the influence of laziness on privacy control behavior. **Paper VI** and **Paper VII** investigate the importance of mindfulness in a general IS context and how it can help explain how individuals control their privacy. Furthermore, **Paper VIII** illustrates that individuals do not always make a great effort into decision making and rely on biases with regard to controlling their privacy. Finally, **Paper IX** gives insight into how individuals control not only their own privacy but also the privacy of others.

Chapter IV: Privacy Turbulence

This chapter consists of two papers focusing on privacy turbulence. **Paper X** illustrates the influence of who gains access to the private information on privacy turbulence. **Paper XI** shows how individuals can be guided to better privacy protection behavior when that privacy is in danger, especially when they are not aware of the danger.

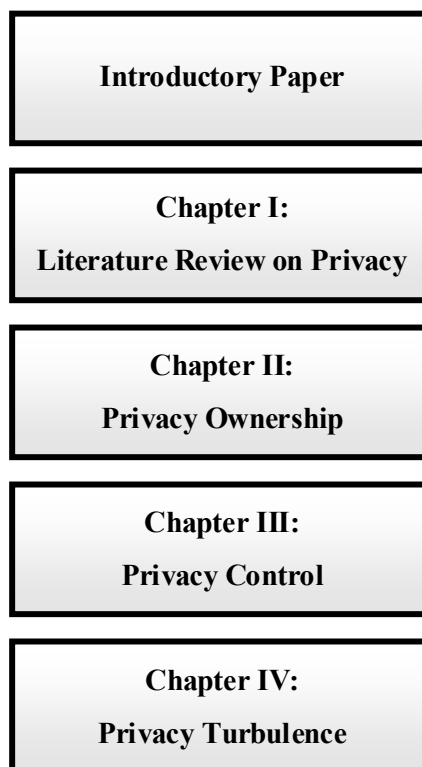


Figure 1. Structure of this dissertation

An overview of the structure of this dissertation is given in Figure 1. The following section introduces

the theoretical lenses through which this dissertation views privacy, defines the digital age context, and discusses the key concepts used in the eleven papers constituting this dissertation.

2 THEORETICAL BACKGROUND

This dissertation explores and explains the management of privacy by individuals in the domain of the digital age. Therefore, although it has already broadly defined in the introduction, it is generally important to particularly define what privacy exactly means. Since the term privacy has changed in the context of the digital age (Smith et al. 2011), the first part of this section will define the *digital age* and then (*information*) *privacy*.

In order to manage privacy, three concepts are diametrically opposed: Firstly, information must be disclosed if there is a potential threat to one's own privacy (Petronio and Altman 2002). The disclosure of information must therefore be defined. On the other hand, individuals can also protect their privacy. Therefore, how privacy can be protected must be described (Son and Kim 2008). Finally, privacy is about the disclosure or protection of information. These can differ in their sensitivity. The second part of this section therefore explains the *disclosure of information* as a potential threat to privacy (Petronio and Altman 2002), the concept of *privacy protection* (Son and Kim 2008) and the role of *information sensitivity* (Mothersbaugh et al. 2011).

In order to concretely understand how individuals manage their privacy, there are many different theoretical lenses in privacy research that will be used by the 11 papers in this dissertation (Bélanger and Crossler 2011; Li 2011b; Smith et al. 2011). First of all, research has shown that many individuals want to protect their privacy, but often act contrary. This is called the privacy paradox (Norberg et al. 2007). In order to understand why individuals act so contrary, the privacy calculus (Dinev and Hart 2006) is the most widely used theoretical lens in privacy research (Kokolakis 2017; Smith et al. 2011), as explanations for why individuals give away their information. However, not all individuals always act paradoxically. In many cases, individuals also protect their privacy. The factors that lead to such protection are explained using the protection motivation theory, which is the most widely used theory of privacy protection (Rogers and Prentice-Dunn 1997; Wirth 2018) and is applicable as a lens for understanding data protection behavior. All three theoretical lenses have also mainly been used throughout the 11 papers of this dissertation. Therefore, the *privacy paradox*, the *privacy calculus* and the *protection motivation theory* are explained in more detail in the third part of this section.

All these theoretical lenses assume that individuals always put a high cognitive effort into their decision making (Dinev et al. 2015). This is indeed often the case - but in several cases it is not. In the latter case, it is then apparent that individuals often rely on *behavioral economics*, which explains behavior beyond the scope of the above-mentioned classical theories, i.e. when individuals put little cognitive effort into their decision making (Dinev et al. 2015). An introduction to *behavioral economics* is therefore given in the fourth part of section two.

Section	Content	Author(s)
Digital age and (information) privacy	Digital age	Solove (2006)
	(Information) privacy	Smith et al. (2011)
Concepts	Disclosure of Information	Derlega (1993)
	Privacy-Protection	Son and Kim (2008)
	Information sensitivity	Mothersbaugh et al. (2011)
Theoretical lenses	Privacy paradox	Norberg et al. (2007)
	Privacy calculus	Dinev and Hart (2006)
	Protection motivation theory	Rogers and Prentice-Dunn (1997)
Behavioral economics	Level of effort, peripheral cues, biases, and misattributions	Dinev et al. (2015)

Table 1. Overview of the theoretical background in section two of this dissertation

Finally, a summary is presented in the fifth part of this section. Here the most important findings

from the four subsections are described, especially the definitions and theoretical lenses used.

An overview of section two is given in Table 1. Based on this theoretical background, the CPM is then introduced in the section afterwards. The CPM is used as an overarching scheme in this dissertation to structure parts of the introductory paper and the four subsequent chapters.

2.1 DIGITAL AGE AND INFORMATION PRIVACY

This section introduces the digital age as the context of this dissertation and defines (information) privacy.

2.1.1 Digital age

The digital age began around 1970 when silicon began to be used to manufacture microchips (Lane and Levy 2019). As information technology use rose, the computer became the defining technology of the digital age, a “*period in which digital technology has made the production, transmission, and consumption of information central to social and economic well-being*” (Carnegie and Abell 2009, p. 248).

With the use of technologies, much more information is available than ever before, the speed and frequency with which information is communicated has increased and so has the ease with which information can be access by other entities (Lane and Levy 2019). Information which was long ago disclosed through gossip and storytelling is now, aided by technological advancements, predominantly disseminated through technology (Solove 2006).

Over the last decades, the digital age has become increasingly digital. For example, in 1986, 0.8 percent of the information worldwide was stored in digital format – in 2007, this share increased to 94.0 percent (Hilbert and López 2011). From 2011 – 2013, as much information was created as had been created before 2011 (Jetzek et al. 2013). In the digital age, individuals now have access to a plethora of information and are both consumers of information and creators of information. This is especially caused by the rise of the Internet (Lane and Levy 2019).

2.1.1.1 Rise of the Internet

The Internet originated in a former military and researcher network in the 1960s. In the mid-1980s, the Internet entered the commercial phase. Through new technological hardware (personal devices as well as backbones and fiber cables), software protocols (such as TCP/IP), software in general (such as browsers) but also because of the healthy curiosity of the individuals, the Internet has grown from 50 web pages in 1992 to 1.72 billion today (Armstrong 2019; Cohen-Almagor 2013). Whereas in the late 1980s email was the main purpose for using the Internet, starting in the mid-1990s, finding information, researching, business, commerce, entertainment and travel found their place in the Internet, along with ever-stronger search engines, such as Google, which was founded in 1996 (Cohen-Almagor 2013).

In 2001, the European council acknowledged that the Internet could also be used for criminal activities and adopted a law addressing potential cybercrime on the Internet. In the same year, through the proliferation of broadband technology, wireless access and gigantic storage mechanisms, now huge amounts of information could be shared. This paved the way for social media such as mySpace (founded in 2003 and bought by Facebook in 2008) or YouTube (invented 2005 and bought by Google in 2006) (Cohen-Almagor 2013).

Today, Google is the most visited website on the Internet, followed by YouTube and Facebook. 4.4 billion individuals worldwide use the Internet every day (statista.com 2019a). They send 188,000,000 emails and 41,600,000 mobile messages and type in 3,800,000 search queries on Google every minute

(statista.com 2019b). Through information technologies, such information can now be *collected*, *processed* and *disseminated* in new ways (Solove 2006).

2.1.1.2 The collection, processing and dissemination of information has changed through technology

Three basic processes show how the digital age has changed the way personal information is handled: collection of information, the processing of information and the dissemination of information.

Collection: The collection information has changed through technology. More potential entities have arisen that are able to collect information. Whereas without technology, information was usually collected by individuals (Solove 2006), today new actors such as hackers or intelligence agencies use technology to collect information. In addition, the bandwidth of individuals and organizations has increased. Whereas earlier only mainly individuals who knew each other were able to collect information about each other, now, through technology, individuals can also collect information about people they do not know. The same applies for organizations which are now able to collect information from many individuals at the same time and may even buy further information about these individuals from other organizations (Karwatzki et al. 2017).

In short, everyone is able to collect personal information about other individuals – individuals, organizations as well as the government (Solove 2004). In this regard, much attention has been paid to mass surveillance by governmental agencies. Although the state often tries to protect its citizens' ability to control their personal information (Politou et al. 2018), the state can also commit mass surveillance of its citizens, reducing that control. Mass surveillance is generally defined as any method that collects information of a population without any attempts to limit the surveillance to a particular individual but rather to monitor an entire group of individuals (Privacy International 2017). Mass surveillance entered mainstream awareness when the whistleblower Edward Snowden leaked highly classified information from the USA National Security Agency about global mass surveillance programs. The growth of the Internet and the digitization of society has led to a massive proliferation of information which can be examined by intelligence agencies. Today, it is widely known that intelligence agencies worldwide store and examine most information sent over the Internet (Gidda 2013).

In addition to governmental agencies collecting vast amounts of information through technological development, the private sector also collects information about individuals. For example, through web tracking and email tracking, an individual's personal information is collected by organizations. Web tracking, which has become ubiquitous on websites today, refers to Internet techniques to collect personal information for online advertisement, individual authentication, content personalization and other purposes (Ermakova et al. 2018). This personal information can include the browser configuration and history (Sanchez-Rola et al. 2017). E-Mail tracking on the other hand is a technology which allows an email sender to gather information about the recipient (Bender et al. 2016). The information gathered about the recipient may include the IP address, the geo-location, whether and when the email was opened, the operating system, device and provider used to open the email. Besides web tracking and email tracking, there are many other ways to collect information about individuals: retailers collect personal information about existing and potential customers online (Schwaig et al. 2006), and social networking sites (SNS) collect personal information for advertisement purposes (Lukka and Paul 2014). Information is also collected by other technologies such as the connected car, where information about the driver and the car are sent to the manufacturer of the car (Coppola and Morisio 2016) or smartphones, where location information is collected by providers (Shin et al. 2012).

Processing: Through technology, information collected by governmental agencies and private organizations can be processed in new ways and faster than ever (Bélanger and Crossler 2011; Malhotra

et al. 2004). Through new analytical tools, especially through the analysis of big data, the processing of information leads to new insights about individuals, groups and society. For example, big data analyzes make it possible to reveal patterns and correlations among customers of private organizations that were previously hidden (Sagiroglu and Sinanc 2013). Through better analyzing-methods, real-time behavioral advertisement is possible (Ermakova et al. 2018). Furthermore, governmental agencies use new analyzing techniques to predict crimes in the future (Mohler et al. 2015). Information that has been created through processing other information or also information that has not been processed, yet, can also be disseminated.

Dissemination: Governmental agencies, organizations and individuals can disseminate information much faster and more conveniently than before the rise of technology. Using technology, information can be copied and duplicated with little effort or cost. This makes it very easy to disseminate information. For example, governmental agencies and organizations use their own databases and the Internet to disseminate information about individuals to each other (Solove 2004). In addition, individuals can also use technology to disseminate information in new ways: For example, they can use SNS to disseminate information about other individuals very conveniently (Poremba 2012).

These three processes show how the digital age has drastically changed the way how information is handled, raising new questions about the (information) privacy of individuals (Acquisti et al. 2015).

2.1.2 (Information) privacy

Historically, privacy was first only considered from a physical perspective: Who has access to an individual's private space and to the individual herself? In the digital age and due to the ease of information collection, processing and dissemination, the concept of information privacy gained importance and drew increasing attention (Smith et al. 2011; Westin 2003).

Taken together, physical privacy and information privacy are known as general privacy. General privacy can be considered from four different perspectives, grouped into two value-based and two cognate-based perspectives. Whereas the value-based perspectives state that general privacy is a human right and integral to the society the individual is in, the cognate-based perspectives are more related to the individual's mind, perceptions and cognitions. Table 2 below defines these four perspectives and lists key scholarly contributions for each (Smith et al. 2011):

Perspective	Definition	Author(s)
Value-based: right	General privacy is considered a right that every individual possesses. It is based on a normative view, i.e. referring to guidelines and norms.	Warren and Brandeis (1890)
Value-based: commodity	General privacy should be treated as an economic commodity. The right to privacy can be given up in some instances. When individuals willingly cooperate by providing personal information about themselves, their privacy is treated as an economic good.	Campbell and Carlson (2002); Davies (1997)
Cognate-based: state	Privacy was first defined through four substates: anonymity, solitude, reserve, and intimacy. Later on, it was tied to concrete situations with three dimensions: self-ego, environmental, and interpersonal. This was then again narrowed to the state of limited access of information.	Westin (1967)
Cognate-based: control	The cognate-based control perspective is the main perspective adopted in IS literature. According to the perspective, general privacy is defined as follows: " <i>Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability</i> " (Margulis 1977, p. 10).	Altman (1975); Westin (1967)

Table 2. Four different perspectives of general privacy, based on Smith et al. (2011)

Since this dissertation is located in the domain of information systems (IS), in this dissertation, it is concurred with previous research and thus the *cognate-based: Control* perspective is adopted (Smith et al. 2011). Furthermore, it is not focused on the concept of general privacy (i.e. physical privacy and

information privacy) but solely focus on the concept of information privacy. The reason is because this dissertation is in the domain of IS research, which has mainly focused on this concept of information privacy and not on physical privacy or general privacy (Bélanger and Crossler 2011). Thus, the private nature of information is considered as data traceable to a particular individual (Derlega 1993; Lin and Armstrong 2019; Posey et al. 2010; Wheelless and Grotz 1976). Information that is not of private nature and therefore not traceable back to a particular individual is not covered by the concept of information privacy. Furthermore, following the lead of previous research (Smith et al. 2011), this dissertation uses the abbreviated term *privacy* to refer to information privacy.

Most definitions of privacy from a control perspective focus on the control component (Bélanger et al. 2002). In line with Bélanger and Crossler (2011), in this dissertation, privacy is therefore defined as “*the claims of individuals that data about themselves should generally not be available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use*” (Clarke 1999, p. 60). As this definition indicates, the information is of private and therefore personal nature (Lin and Armstrong 2019). If information is private, it is not public, i.e. not accessible by the public (Petronio and Altman 2002). In other words, privacy of the individual can only be harmed when the information that the individual has lost control of can be linked to that particular individual and if it is private and thus not already disclosed (Petronio and Altman 2002). To better understand, how individuals react in the domain of privacy, concepts, theoretical lenses as well as behavioral economics need to be understood.

2.2 CONCEPTS: DISCLOSURE, PRIVACY-PROTECTION AND INFORMATION SENSITIVITY

As discussed above, privacy is threatened when an individual’s personal information is *disclosed*. Steps taken to prevent such disclosure are considered privacy *protection* measures, which vary according to the *sensitivity of information* being threatened.

2.2.1 Disclosure of information

Disclosure of information is one of the most used variables in privacy research (Smith et al. 2011). It is generally defined as the revelation of private information (Derlega 1993; Lin and Armstrong 2019; Posey et al. 2010; Wheelless and Grotz 1976), making it no longer fully private and giving at least one other entity access to it (Petronio and Altman 2002). Disclosure is thus closely associated with the risk that privacy may be diminished. It is a necessary prerequisite of privacy loss, but does not *necessarily* lead to a loss of privacy (Wirth et al. 2019). The term collection represents the viewpoint of the entity receiving the information, while disclosure represents the viewpoint of the individual who reveals the information.

In most cases, researchers traditionally measure the degree to which individuals disclose information about themselves. This is called self-disclosure and is defined as the “*act of revealing personal information to others*” (Archer 1980, p. 183). This concept is generally considered along five dimensions: The *amount* refers to the frequency and duration of disclosure; the *accuracy* is the correctness of the disclosed information, especially regarding unintended or unconscious incorrectness of the disclosed information (Wheelless 1978; Wheelless and Grotz 1976). *Depth* refers to the degree of intimacy of the disclosed information. *Intent* is the willingness of the individual to disclose information about herself. Finally, *valence* refers to whether the disclosed information is positive, neutral or negative (Posey et al. 2010; Wheelless 1978; Wheelless and Grotz 1976).

However, recent research also indicates that further dimensions need to be considered, such as when individuals disclose information about others (Biczók and Chia 2013). In more particular, recent research emphasizes the role of interdependent disclosure (Biczók and Chia 2013). Based on the CPM,

“disclosure *per se*, necessarily should be viewed in a larger conceptual framework that extends beyond information of the “self.” Telling private information to someone carries an obligation (implicit or otherwise) for the recipient regarding third-party dissemination” (Petronio 2010, p. 177). In other words, disclosure of information applies not only to self-disclosure of one’s own personal information, but also to disclosure of information about other individuals (Petronio and Altman 2002). Hence, in addition to threatening one’s own privacy by disclosing information about oneself, one can also threaten the privacy of others by disclosing personal information about them which is traceable to the individual (Clarke 1999). This notion is reflected by the additional dimension *nature of information*, which refers to whether information is about oneself or about others.

Furthermore, the level of *awareness* needs to be considered as a final dimension of disclosure: The traditional view on disclosure is that the individual whose personal information is disclosed by herself or someone else is aware of the disclosure. However, that is not always the case (Belanger and Hiller 2006; Karwatzki et al. 2017). The discloser can be either aware of or unaware of the disclosure (Son and Kim 2008). Especially in the digital age, information of individuals can be disclosed without awareness (Belanger and Hiller 2006), such as by private organizations using cookies or clickstream technologies (Milne 2000a; Son and Kim 2008). Unaware disclosure is thus primarily linked to the digital age.

Although the first five dimensions that were mentioned only refer to self-disclosure, they can also be applied to disclosing information about others and unaware disclosure. Hence, disclosure can be considered along all seven dimensions, as illustrated in Table 3.

Dimension	Definition	Author(s)
Accuracy	Correctness of the disclosed information	Posey et al. (2010); Wheelless (1978); Wheelless and Grotz (1976)
Amount	Frequency and duration of disclosure	Posey et al. (2010); Wheelless (1978); Wheelless and Grotz (1976)
Awareness	Level of consciousness of the disclosure	Belanger and Hiller (2006); Karwatzki et al. (2017)
Depth	Degree of intimacy of the disclosed information	Posey et al. (2010); Wheelless (1978); Wheelless and Grotz (1976)
Intent	Willingness of the individual to disclose	Posey et al. (2010); Wheelless (1978); Wheelless and Grotz (1976)
Nature of information	Whether the disclosed information is about oneself or others	Biczók and Chia (2013)
Valence	Whether the disclosed information is positive, neutral or negative	Posey et al. (2010); Wheelless (1978); Wheelless and Grotz (1976)

Table 3. Dimensions of disclosure

So far, disclosure has been conceptualized and the seven dimensions have been depicted. The actual usage of disclosure in studies is often either done by asking for the intention to disclose information or the actual disclosure behavior. The intention to disclose refers only to the motivation of the individual to reveal personal information and not to the actual behavior. In fact, most studies in privacy research rely on the intention to disclose, with only a few exceptions researching on actual disclosure behavior (Smith et al. 2011). However, since intention does not always lead to behavior (Fazio and Roskos-Ewoldsen 2005), the focus should also be on actual disclosure behavior (Smith et al. 2011), i.e. on the actual revelation of personal information of the individual during the study itself (Alashoor et al. 2016) or on reported past disclosure of information, such as on SNS (e.g., Krasnova and Veltri 2010). Generally, reported past disclosure, such as on SNS, is usually not different from actual disclosure behavior (Hampton et al. 2012) and thus can be considered together with actual disclosure behavior.

Besides disclosing information, individuals can also protect their privacy by several different measures.

2.2.2 Privacy-Protection

To protect one's privacy, the individual must be aware of the disclosure of private information. If the individual is unaware of the disclosure, she cannot actively protect her privacy. Given such awareness, different measures can be taken to protect one's privacy. According to CPM, the most common used ones are refusal and misrepresentation (Child and Petronio 2011).

Refusal is that an individual can decline to disclose information to protect her privacy. If the disclosure is intended, she can decide not to do it and refuse the disclosure. If the disclosure is unintended, e.g. through technological advancements, then the individual can also undertake technological measures to refuse the disclosure of information (Son and Kim 2008). For example, in web tracking, where disclosure is unintended (Son and Kim 2008), individuals can install particular pieces of software to prevent web tracking and thus refuse the disclosure of information (Baruh et al. 2017).

With misrepresentation, individuals can protect their privacy by intentionally providing incorrect information. Even if incorrect disclosed information is traceable to the particular individual, it threatens their privacy less. If the misrepresentation of information renders it no longer traceable back to the individual, privacy is fully protected. This also applies to unintended disclosure, where the individual may be forced to provide personal information but intentionally misrepresents that information (Son and Kim 2008).

There are many other ways to protect one's privacy. For example, one can ask an organization to remove information that has been disclosed to that organization, such as by deleting the record from a database or removing an entry on a profile on a SNS. Individuals can also pressure organizations to stop disclosing private information by telling other individuals that an organization diminished their privacy, by contacting the organization directly to post a complaint or by complaining to the organization via third-party organizations (Son and Kim 2008). In the cases of SNS (Ernst et al. 2015), the individual can adjust their connectivity, e.g. by altering the number of linked friends (Lankton and Tripp 2013), terminating connections (Bulgurcu et al. 2010) or changing the privacy settings (Lankton and Tripp 2013). Generally speaking, individuals can often change software settings or install tools to protect their digital privacy. These measures can be applied individually or in combination, sequentially or simultaneously.

If an individual wants to protect herself, she must believe in that the conducted action will lead to the anticipated goal. Otherwise, the individual may resign in protecting herself (Feifel and Strack 1989). Recent research indicates that many individuals resign in protecting their privacy (Guo and Yu 2020).

Yet, independent of the level of resignation: When individuals come to a decision to disclose information or to protect their privacy, the sensitivity of the information plays a major role (Mothersbaugh et al. 2011).

2.2.3 Information sensitivity

The definitions of information sensitivity in privacy literature vary widely. Such definitions include an individual information attribute concerning the level of discomfort (Dinev et al. 2013; Li et al. 2011a), the perceived intimacy level of information (Lwin et al. 2007), potential psychological, physical or material loss (Moon 2000; Mothersbaugh et al. 2011), information value (Wacks 1989) or generally the negative consequences of information disclosure (Bansal et al. 2010). Some authors also equate information sensitivity with the type of information. Although different pieces of information can lead to different levels of sensitivity, there is no general level of sensitivity for a specific type of information (Milne 1997; Milne and Gordon 1993; Phelps et al. 2000; Weible 1993). The sensitivity of a piece of information depends more on the subjective evaluation of the sensitivity (Bansal et al. 2010) and the

situation the individual is in (Weible 1993). In general, most definitions of information sensitivity link it directly to negative factors, yet there is no generally agreed upon definition.

Prior literature also indicates that higher information sensitivity decreases the likelihood of information disclosure (e.g., Malhotra et al. 2004), and increases privacy concerns (e.g., Bansal et al. 2010) and privacy risk (Dinev et al. 2013). It has also been suggested that information sensitivity moderates the relationship between privacy concerns and information disclosure (Alashoor et al. 2015).

To understand, how information sensitivity but also other concepts have an effect on the management of privacy, different theoretical lenses can be applied.

2.3 THEORETICAL LENSES: PRIVACY PARADOX, PRIVACY CALCULUS AND PROTECTION MOTIVATION THEORY

The eleven papers constituting this dissertation employ three main theoretical lenses to understand the management of privacy: First, the privacy paradox is an unresolved occurrence in the privacy domain and has been gained much attention in the privacy domain (Kokolakis 2017; Smith et al. 2011). Second, the privacy calculus is the predominant theory in the privacy domain to explain why individuals disclose information (Dinev and Hart 2006; Smith et al. 2011). Third, the protection motivation theory (Rogers and Prentice-Dunn 1997) is the most often used theory in the privacy domain to explain why an individual desires to protect her privacy (Wirth 2018).

2.3.1 Privacy paradox

The privacy paradox states that although individuals are worried about their privacy, this level of worry has little effect on their level of disclosure (Kokolakis 2017; Norberg et al. 2007). The level of worry of an individual about her privacy when personal information is disclosed can be called privacy concerns (Son and Kim 2008). Privacy concerns are usually considered along four dimensions: the collection of, errors in, the secondary use of and unauthorized access to personal information (Smith et al. 1996). The concept using these four dimensions is called the concern for information privacy scale (Smith et al. 1996). This scale was further developed by Culnan and Armstrong (1999) as well as Dinev and Hart (2006). Another development of the scale led to the Internet users' information privacy concerns scale (Malhotra et al. 2004) and the Internet privacy concerns scale (Hong and Thong 2013). The Internet privacy concerns scale comprises six dimensions: collection, secondary usage, errors, improper access, control, and awareness.

However, it has been shown that the refined scale of Dinev and Hart (2006) is the only scale that does not lead to a priming effect by survey participants in comparison to other scales such as Hong and Thong (2013) (Alashoor et al. 2017). Therefore, in this dissertation, the refined scale of Dinev and Hart (2006) is used, alongside with their definition of privacy concerns: "*Concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent in particular*" (Dinev and Hart 2006, p. 64).

Privacy concerns serve as a central construct in privacy research. Since privacy is a multi-facet concept that is often based on perceptions and not on rational assessment, it is difficult to measure. Privacy concerns is thus often used as a proxy to measure privacy (Smith et al. 2011). Due to its central role in privacy research, privacy concerns have often been used as an antecedent of disclosure. Thereby, it is logical to state that the higher the privacy concerns of the individual, the less likely she should disclose. This is because if individuals are concerned about opportunistic behavior related to their personal information, they should try to reduce their level of concerns by protecting their privacy and refusing to disclose information. However, in reality this is often not the case. In fact, in several studies, it was shown that the level of privacy concerns does not have any effect on the level of disclosure. This

has been called the privacy paradox (for a review, see Kokolakis 2017). Several possible solutions to the privacy paradox have been discussed (Kokolakis 2017), the most prominent of which is the privacy calculus.

2.3.2 Privacy calculus

Generally speaking, individuals act to minimize negative and to maximize positive outcomes (van Eerde and Thierry 1996; Vroom 1964). In the privacy setting, according to the privacy calculus, an individual's decision to disclose personal information depends mainly on the balance between the perceived benefits of disclosure (hereafter benefits) and the perceived risks of privacy loss through disclosure (hereafter privacy risks) (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977). Whereas benefits relate to the positive outcomes through disclosure, privacy risks refer to the expectation that there will be adverse consequences when information is made public (Smith et al. 2011).

From a model-driven point of view, benefits have a positive effect and privacy risks have a negative effect on disclosure (see Figure 2). If the benefits outweigh the privacy risks, then maximization of positive outcomes is fulfilled, and individuals will disclose information. Likewise, if the privacy risks outweigh the benefits, then individuals will not disclose information to avoid opportunistic behavior. In terms of the privacy paradox, even if individuals are concerned about their privacy, they will disclose personal information as long as the benefits outweigh the privacy risks of disclosure.

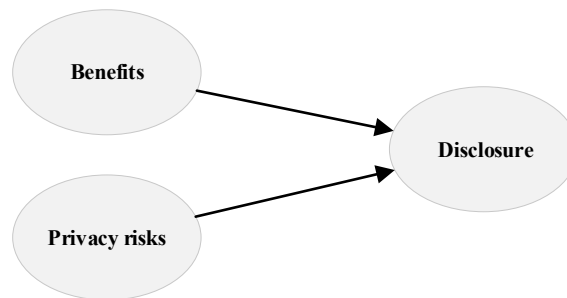


Figure 2. The privacy calculus (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977)

Benefits that relate to positive outcomes and privacy risks that relate to negative outcomes can be further analyzed.

2.3.2.1 Benefits and privacy risks

On the one hand, there are many benefits of disclosure that may influence the privacy calculus. The overview provided in Table 4 provides some examples from previous literature.

On the other hand, whereas there are several possibilities to depict benefits, privacy risks is depicted by the extent to which an individual thinks that there will be adverse consequences because others have access to her personal information (Karwatzki et al. 2018). However, there is a plethora of such adverse consequences. An overview is given by Karwatzki et al. (2017) in Table 5. While Karwatzki et al.'s (2017) study identifies potential adverse consequences, it does not investigate actual adverse consequence frequency. The third column of Table 5 therefore gives examples from practice and literature of adverse consequence that individuals have actually suffered.

Type of benefit	Definition	Author(s)
Expected positive community related outcomes	Judgement of individuals that they will probably benefit from communicating	Kordzadeh and Warren (2017)
Image enhancement	The extent to which the social image of an individual is enhanced	Choi et al. (2015)
Locatability	Taking advantage of positioning technologies gained through disclosure	Keith et al. (2012); Keith et al. (2013); Keith et al. (2015); Xu et al. (2009)
Monetary incentives	Financial rewards gained through disclosure	Acquisti et al. (2013); Acquisti and Grossklags (2005); Anderson and Agarwal (2009); Hui et al. (2007)
Perceived enjoyment	Having fun and enjoyment through disclosure	Brakemeier et al. (2016); Buckel and Thiesse (2013); Krasnova et al. (2012); Krasnova and Veltri (2010, 2011); Lankton and Tripp (2013)
Perceived usefulness	Belief that disclosure will increase one's performance	Brecht et al. (2019); Keith et al. (2010); Li and Sarkar (2010); Schreiner and Hess (2015)
Personalization	Content and services are provided based on the needs of the individual, which is in turn based on knowing about preferences of the individual	Chellappa and Sin (2005); Keith et al. (2012); Keith et al. (2013); Keith et al. (2015); Li and Unger (2012); Sheng et al. (2008); Sutanto et al. (2013); Xu et al. (2009); Xu et al. (2011b)
Relationships	Disclosure will lead to maintain, build and support relationships	Buckel and Thiesse (2013); Krasnova and Veltri (2010)
Self-enhancement	Disclosure will lead to shape the self-concept	Tam et al. (2002); Xu et al. (2003)
Self-presentation	Received benefits by improving one's self-concept in comparison to others	Buckel and Thiesse (2013); Krasnova and Veltri (2010)
Social adjustment	Establishing personal identity in a group through disclosure	Tam et al. (2002); Xu et al. (2003)
Time savings	More efficiency, less search costs and more accurate results when disclosing information	Tam et al. (2002); Xu et al. (2003)

Table 4. Overview of exemplary benefits in the privacy domain

Type of adverse consequence	Definition	Examples
Career-related	Negative impacts on one's career	<ul style="list-style-type: none"> • “Privacy mistakes is quickly becoming one of the top reasons people get fired” (Stevens 2017) • Individuals may not get hired because of information about them posted on social media (Acquisti and Fong 2019)
Freedom-related	Loss of freedom of opinion and behavior	<ul style="list-style-type: none"> • In response to mass surveillance, individuals less frequently use delicate terms such as homeland security and terrorism (Penney 2016) • Russia tried to influence the voting behavior of U.S. voters by posting content on SNS particular individuals (Howard et al. 2018)
Physical	Loss of physical safety	In intimate relationships, one partner uses disclosed information to physically violate the other partner (Dimond et al. 2011; Freed et al. 2017; Matthews et al. 2017).
Prosecution-related	Legal actions taken against an individual	<ul style="list-style-type: none"> • Individuals can have criminal records because someone who stole their identity committed crimes using their identity (Perl 2003) • Nearly 20 percent of all victims of identity theft (about 22 percent of all U.S. Internet individuals have been the victim of identity theft (statista.com 2018c)) have reported some form of criminal identity theft, e.g. warrants or criminal records (Identity Theft Resource Center 2016)
Psychological	Negative impact on one's peace of mind	<ul style="list-style-type: none"> • Mass surveillance can lead to anxiety, fatigue, and stress (Smith et al. 1992) • Cyberstalking can lead to anxiety and depression (Worsley et al. 2017)
Resource-related	Loss of resources	<ul style="list-style-type: none"> • Burglars use information available on SNS to plan their robberies (PWC Virginia) • Individuals lost \$16 billion due to fraud in combination with identity theft (Grant 2017)
Social	Change in social status	<ul style="list-style-type: none"> • 25 percent of individuals reported that their reputation has suffered due to a privacy loss (statista.com 2015b) • 59 percent of U.S. teens have been the victim of cyberbullying (Anderson 2018)

Table 5. Categories of adverse consequences induced by privacy risks (Karwatzki et al. 2017, p. 694) including examples

Although the interplay between benefits and privacy risks has been supported in many research

studies, some scholars have also challenged the privacy calculus.

2.3.2.2 Challenging the privacy calculus

The privacy calculus has been used and supported with many extensions in a variety of settings, including variables such as the situation the individual is in (Anderson and Agarwal 2011), information sensitivity (Kehr et al. 2015), privacy concerns and trust (Dinev and Hart 2006) and individual differences (Cichy et al. 2014). The privacy calculus has also been supported in different research settings, such as SNS (e.g., Cavusoglu et al. 2016), research about location information of individuals (Xu et al. 2009), or in the healthcare domain (Anderson and Agarwal 2009).

However, the privacy calculus has also been challenged. In several cases, individuals disclose information even when benefits do not outweigh privacy risks (Acquisti 2004; Dinev et al. 2015). One explanation is that the benefits and privacy risks are perceived as being higher or lower than they could be. A second explanation is that the effect of benefits and privacy risks on disclosure can be altered, potentially strengthening the effect of benefits and potentially weakening the effect of privacy risks (see Table 6).

The factors that can alter the perception of benefits and privacy risks include limited information, bounded rationality and psychological distortion (Acquisti 2004). *Limited information* means that individuals rarely have access to all necessary information and evaluate benefits and privacy risks based on limited information. This can lead to failures in the evaluation process. *Bounded rationality* is that even if individuals had access to necessary information, some would not be able to process that information correctly. Most individuals are not able to calculate and compare all the consequences associated with disclosure in relation to benefits and privacy risks. Even if individuals had access to all information and were able to process that information correctly, many people have some form of *psychological distortion* leading to a misperception of benefits and privacy risks (Acquisti 2004).

The factors that can alter the effect of benefits and privacy risks on disclosure include perceived relevance, perceived trust, privacy risks and mental states. *Perceived relevance* indicates that the effect of benefits on intention to disclose weakens when the information requested appears to be not relevant and the effect becomes insignificant when the information requested appears to be relevant (Sarathy and Li 2007). *Perceived trust* indicates that the effect of benefits on disclosure weakens when individuals' level of trust towards the company the information is disclosed to is high (Xu et al. 2003). Privacy risks weakens that effect of benefits on disclosure when privacy risks are high (Sun et al. 2015). *Mental states* can also alter the effect of benefits and privacy risks on disclosure. Mental states are cognitive conditions at a particular moment in time (Dane 2011). When individuals are more in a prevention-focused state, i.e. more focus on losses of disclosure, the effect of benefits on intention to disclose weakens, whereas the effect of privacy risks on intention to disclose strengthens (Brakemeier et al. 2016).

Explanation	Factor	Author(s)
Altering the perception of benefits and privacy risks	Limited Information	Acquisti (2004)
	Bounded Rationality	Acquisti (2004)
	Psychological Distortion	Acquisti (2004)
Altering the effect of benefits and privacy risks on disclosure	Perceived relevance	Sarathy and Li (2007)
	Perceived trust	Xu et al. (2003)
	Privacy risks	Sun et al. (2015)
	Mental state	Brakemeier et al. (2016)

Table 6. Explanations for a non-functionable privacy calculus

Despite these results, the privacy calculus still is the dominant theory in privacy research to explain disclosure (Dinev et al. 2015). To explain protection of privacy on the other hand, the protection motivation theory is the most prominent one.

2.3.3 Protection motivation theory

By definition, information must be disclosed in order to potentially threaten one's privacy, but such disclosure does not necessarily lead to diminished privacy (Wirth et al. 2019). The mechanisms individuals can undertake to protect their privacy (see section 2.2.2 above) and their motivations for doing so can be viewed through several different theoretical lenses, including the prominent protection motivation theory (see Figure 3) (Boss et al. 2015; Rogers and Prentice-Dunn 1997).

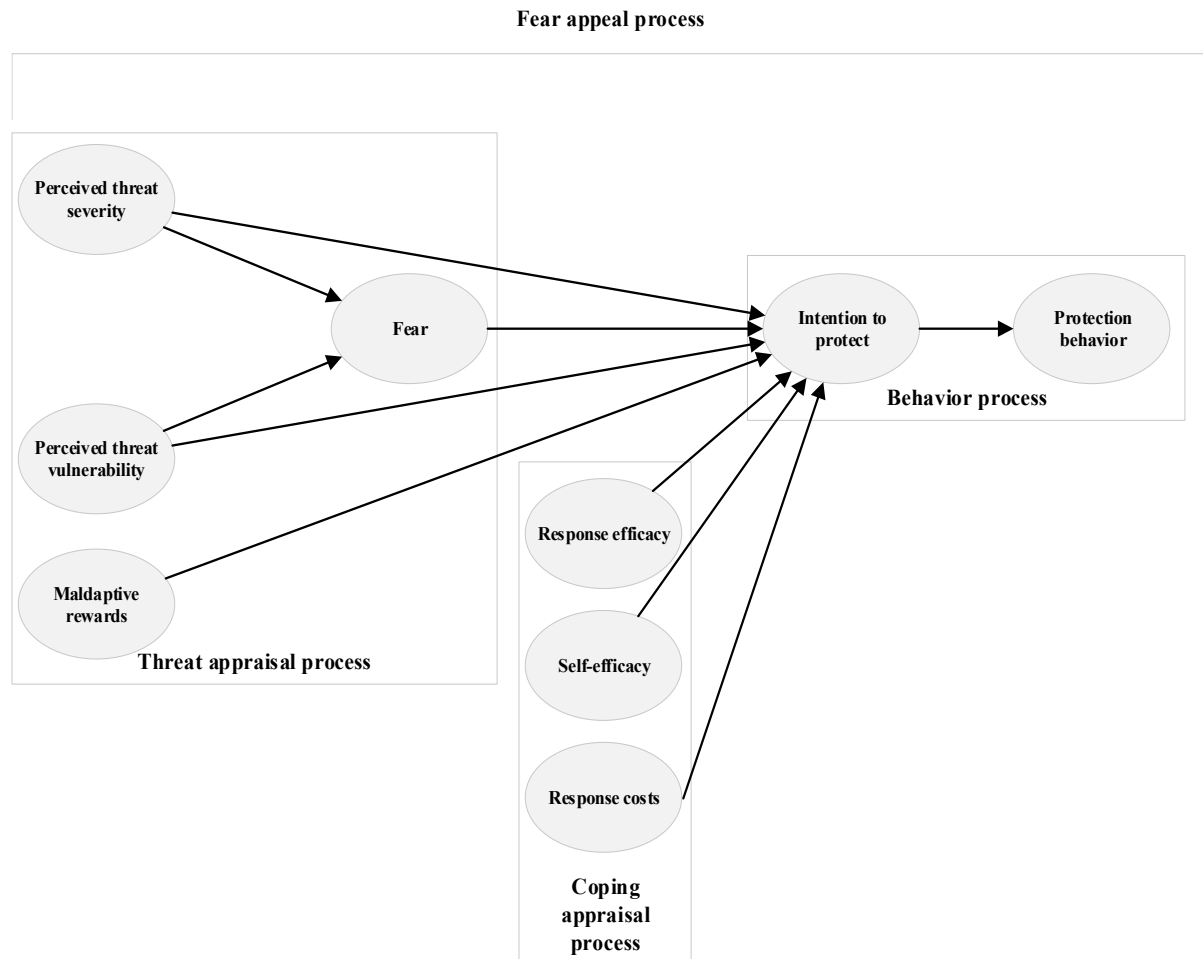


Figure 3. Protection motivation theory

In the privacy context, the protection motivation theory helps explain what leads an individual to protect herself against a source of danger which can cause loss of control over authentic personal information, resulting in harm to the individual (Floyd et al. 2000). The protection motivation theory consists of four processes to explain protection behavior (see Figure 3): The *threat appraisal process* through which individuals evaluate the degree to which the current issue is an actual threat. Here, individuals consider the severity of the threat, their own vulnerability to the threat, and the resulting fear caused by the threat. Also, they consider the maladaptive rewards of not protecting oneself against the threat. Then, individuals conduct the *coping appraisal process*, which involves evaluating the degree to which they are able to protect themselves against the threat. Here, they consider the response efficacy, their self-efficacy as well as the costs of responding to the threat. After having conducted both appraisals, the *behavior process* starts where individuals form a particular intention and adopt a particular protection behavior. In a study, all the mentioned processes are supposed to be influenced by the *fear appeal process*, which are factors that make the threat real and the protection measure acknowledged as an effective response to protect against the threat. Fear appeal is defined as a “*persuasive message designed to scare people by describing terrible things that will happen to them if*

they do not do what the message recommends” (Witte 1992, p. 329). When including a fear appeal into protection motivation in studies, scholars use it to manipulate individuals. A fear appeal is usually divided into both “high” and “low” fear appeals (Boss et al. 2015; Milne et al. 2000b). Such a fear appeal does not only affect the fear concept, nor only some of the relationships of the entire model. Rather, a fear appeal serves as a central moderator of the entire model (McClendon and Prentice-Dunn 2001).

With few exceptions (e.g., Acquisti 2004), the concepts and theories discussed above assume that individuals always take on a full cognitive load and reach fully-informed decisions. However, this assumption is often incorrect for various reasons, such as the influence of behavioral economics (Dinev et al. 2015).

2.4 BEHAVIORAL ECONOMICS

Most privacy research shares the tacit assumption that individuals behavior is based on economics theory, i.e. that individuals are able to make decision by effortful, deliberate information processing, when considering privacy-related perceptions and behaviors (Dinev et al. 2015). This reflects the neoclassical economics model, which, in the privacy context, assumes “*that responses to external stimuli result in deliberate analyzes, which lead to fully informed privacy-related attitudes and behaviors*” (Dinev et al. 2015, pp. 641–642).

However, that is often not the case. In fact, individuals often undertake privacy-related perceptions and behaviors with little such deliberation, taking simple heuristics and cognitive shortcuts, or are affected by extraneous factors such as information with no objective value in that context that should not logically influence the privacy-related perceptions and behavior. Prior research has neglected to account for such incomplete decision making and processing of information. However, especially in a privacy-related domain, this is important in explaining outcomes such as the privacy paradox, which cannot always be fully explained by relying on neo-classical models (Dinev et al. 2015).

Basically speaking, individuals’ can come to a decision by either taking a high-effort or a low-effort route (Petty and Wegener 1998). Although more recent psychological research points to the fact that the level of effort is on a continuum and is seldom a binary value (Petty and Wegener 1998), the binary perspective still helps to explain the effect of level of effort on privacy-related perceptions and behaviors. A high-effort process “*is elaborated, consciously determined, logical, and explainable*” (Dinev et al. 2015, p. 641). In comparison, a low-effort process “*involves relatively little cognitive effort or conscious awareness*” (Dinev et al. 2015, p. 641). The neoclassical economic models on which the majority of previous research relies assumes a high-effort process. However, since individuals often conduct privacy-related behavior spontaneously with little deliberation, the low-effort process should be considered when researching on privacy-related perceptions and behaviors (Dinev et al. 2015). In fact, psychology and behavioral economics studies confirm that behavior is often determined by a low-effort process (McConnell and Rydell 2014; Petty and Wegener 1998). The low-effort process can also result in suboptimal behaviors that actually contradict the values and beliefs of the individual (Ariely 2010).

In light of these considerations, Dinev et al. (2015) suggest that one needs to extend the view on privacy concerns as one of the main concepts in privacy research and the privacy calculus as one of the main theories in privacy research. In particular, the antecedents of privacy concerns, results of privacy concerns as well as the privacy calculus are affected by the *level of effort* as well as *peripheral cues, biases, heuristics* and *misattributions*. The level of effort is determined by limited cognitive resources, affect motivation and time constraints (Dinev et al. 2015). On the other hand, peripheral cues can refer to the *framing of message*, i.e. more positive or more negative; *biases* such as the optimistic “yes” bias or the anchoring-effect; *heuristics* such as implicit trust or *misattribution* which is the effect that

individuals incorrectly think that one event is caused by another (Bem 1967; Kahneman and Frederick 2002).

The level of effort directly moderates the relationships of many variables, such as the variables of the privacy calculus, antecedents of privacy concerns or outcomes of privacy concerns. High-effort processing will result in an outcome, consistent with the prior literature, which assumes such a high-effort processing. However, low-effort processing will moderate such relationships, weakening or strengthening them depending on the context (Dinev et al. 2015).

On the other hand, peripheral cues, biases, heuristics and misattributions will directly influence several concepts such as the level of privacy concerns, benefits, privacy risks or disclosure. Their relative level of influence will in turn be determined by the level of effort individuals put into their processing. In case individuals conduct high-effort processing, the impact of such extraneous concepts will be low and negligible. Yet, if the individual is conducting a low-effort processing, the influence of the extraneous concepts becomes larger and might even be predominant in the formation of perceptions and behaviors (Dinev et al. 2015).

In summary, most theories in privacy research assume that individuals always put high effort into their decision-making process. However, this is not always the case, which limits the applicability of theories in privacy research and indicate the need to account for the influence of peripheral cues, cognitive biases, heuristics and misattributions.

2.5 SUMMARY

Section two introduces the notions of digital age and information privacy and introduces the concepts, theoretical lenses and behavioral economics used in the eleven papers constituting this dissertation. The digital age and the explosive growth in IS use have changed the way privacy is considered. In this dissertation, privacy is considered from the cognate-based control perspective. The concepts of disclosure, privacy-protection and information sensitivity, the theoretical lenses privacy paradox, privacy calculus and protection motivation theory, and the behavioral economic reality that individuals do not always act with high effort when making privacy-related decisions are all essential in understanding how individuals manage their privacy.

The following section discusses the communication privacy management theory (CPM), which serves as the overarching structure of the remainder of this dissertation. Although it is also a theory, it serves primarily as a structural scheme for this dissertation, following the lead of other scholars (Farrell et al. 2014).

3 COMMUNICATION PRIVACY MANAGEMENT THEORY AND RESEARCH QUESTIONS

The CPM has its origins in research on the non-IS context. Its basic purpose was to explain how individuals manage their private information by disclosing or concealing private information inside their families. The basic premise of the CPM is that individuals maintain virtual boundaries around themselves to draw lines between public and private information. Based on these by the individual managed boundaries, personal information is disclosed or concealed (Petronio and Altman 2002). This view of the CPM corresponds to the cognate-based control perspective (Smith et al. 2011). Individuals whose privacy is maintained are able to control their privacy on their own by deciding on their own what and to whom personal information is disclosed or concealed.

The CPM is based on three elements distilled from five elements of an older version of the CPM (Petronio 2013; Petronio and Altman 2002). The three elements of the CPM are privacy ownership,

privacy control and privacy turbulence (see Figure 4). These elements are neither in a causal order, nor do they provide particular cause-effect relationships that explain the management of privacy. However, they provide an overview of elements an individual considers when managing her privacy. The CPM can serve as a basic scheme to research particular cause-effect relationships that determine an individual's management of privacy by applying further theoretical lenses.

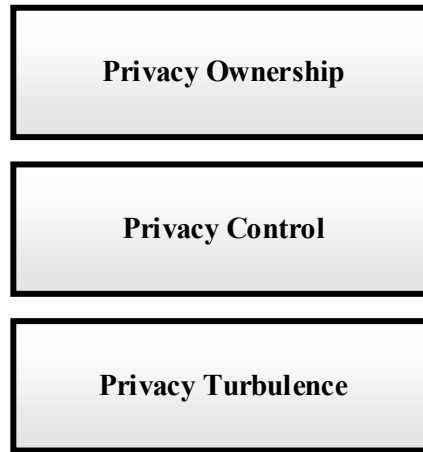


Figure 4. The three elements of the communication privacy management theory (Petronio 2013)

In explaining each of the three elements, a focus is on the *content of the element*, including a definition and related terms, and on the *interpretation of the element by the CPM*, including how the CPM argues that the element is applied by individuals in managing their privacy. This dissertation uses primarily the *content* of the three elements to consider how individuals manage their privacy. In addition, motivated by the theoretical background of this dissertation, it also extends the *interpretation* of each element by the CPM.

3.1 PRIVACY OWNERSHIP

Content: The privacy ownership element posits original owners and co-owners of information. Personal information of an individual belongs to that individual and thus that individual is called an *original owner*. On the other hand, private information co-ownership describes the situation when an individual gives one or more entities access to her personal information, making that other entity a *co-owner* (Petronio 2013; Petronio and Altman 2002). This entity may be another individual, the government, an organization, or a different entity (Karwatzki et al. 2017). When this takes place, the original owner no longer holds a single boundary around the personal information, but rather a collective boundary is formed with the co-owner(s) held by the original owner and the co-owner(s). This implies that the original owner must rely on the co-owner to maintain the collective boundary according to the original owner's needs and desires (Petronio 2013; Petronio and Altman 2002).

Interpretation by the CPM: Individuals believe that they alone own their personal, private information and that they alone are the original owners. They also trust that they have the right to withhold or to give others access to their personal information (Petronio 2013).

3.2 PRIVACY CONTROL

Content: The privacy control element refers to the degree to which individuals have control over whether they give others access to personal information or not. The control of information can vary and is based on the thickness of the virtual boundary. When this boundary is thick, individuals have a high degree of control over their personal information. When this boundary is thin, individuals have little control over their personal information, which is easily accessed through the thin virtual boundary (Petronio 2013; Petronio and Altman 2002).

Interpretation by the CPM: Individuals decide to give others access to their information based on rules determining when, how, with whom and in what way this access is granted. These rules are influenced by five criteria: 1) culture, 2) gender, 3) motivation, 4) context and 5) risk/benefits ratio. Cultural differences include, among others, individualistic vs. collectivistic cultures. The level of motivation is determined by liking, attraction or reciprocity. The context includes the social environment the physical settings, such as if the individual is in a room with one other individual or in a crowded train. The risk/benefits ratio is similar to the privacy calculus in that individuals weigh the benefits against the privacy risks of disclosure (Petronio and Altman 2002).

These criteria provide initial insights into cause-effect relationships that can explain how individuals manage their privacy and can serve as a starting point to understand the control of privacy. Since the CPM itself provides little detailed insight into cause-effect relationships, other theories that dive deeper into such cause-effect relationships are needed to understand the control of privacy.

3.3 PRIVACY TURBULENCE

Content: Although original owners as well as co-owners should be able to treat personal information the original owner wants to treat it, the practical reality is different. Information is often spread in a way the original owner would deny. When mutually collective boundaries do not match the expectations of the original owner, the co-owner may disclose information despite the denial of the original owner. In such situations, original owners no longer fully control their personal information and privacy turbulence can occur. There are many causes of privacy turbulences, including mistakes, misunderstandings or intentional violations, among others (Petronio 2013; Petronio and Altman 2002).

Interpretation by the CPM: The original owner will re-define the collective boundaries in case of privacy turbulence in an attempt to return to a state where the information is inside a boundary and handled the way the original owner wants it to be (Petronio 2013; Petronio and Altman 2002).

3.4 RESEARCH QUESTIONS

The overall research question of this dissertation is how individuals manage their privacy. To this end, the three elements of the CPM are utilized structurally, based on the definitions and terms of each element. Beyond the interpretation of the three elements by the CPM, the theoretical underpinning of this dissertation suggests that the interpretation of each element of the CPM may also be extended or viewed differently. Hence, to answer the overall research question, each of the interpretations of the CPM of each of the elements may have to be re-interpreted based on sub-research questions. Afterwards, these reinterpretations can be put together to answer the overall research question.

Element of the CPM	CPM content	CPM interpretation	Research question challenging interpretation
Privacy ownership	There can be original owners and co-owners of personal information.	Individuals believe that they own their personal, private information. They also trust that they have the right to protect their personal information or to give access to it.	How do individuals handle privacy ownership in the digital age?
Privacy control	Individuals can give access to personal information to others or not.	In deciding whether others may access information, individuals follow rules determined by five criteria.	What determines individuals' control of their own and others privacy?
Privacy turbulence	Original owners do not always fully control their personal information.	Original owner will resettle the collective boundaries in case of privacy turbulence.	How do individuals handle privacy turbulence in the digital age?

Table 7. Summary of the CPM and how the digital age influences the management of privacy

Table 7 provides an overview of the content and the interpretation of each element of the CPM together with sub-research questions which challenges the interpretation based on the theoretical background of this dissertation.

Privacy Ownership

Traditionally, original owners believe that they are the sole owners of their personal information (Petronio 2013; Petronio and Altman 2002). However, in the digital age, information can be disclosed without intent (see section 2.2.1) (Karwatzki et al. 2017). In this case, the original owner may no longer be sole owner of her personal information and may not be explicitly asked to disclose the personal information. Furthermore, recent literature indicates that in the digital age, individuals may have resigned in protecting their own privacy (see section 2.2.2) (Guo and Yu 2020). This may indicate a loss of privacy ownership. Hence, research question 1 asks to what degree the assumption that every original owner believes that she is the sole owner of her personal information needs to be reconsidered in the digital age:

Research question 1: How do individuals handle privacy ownership in the digital age?

Privacy Control

Traditionally, individuals think they alone control their privacy and grant others access to their information based on rules influenced by five criteria: culture, gender, motivation, context and risk/benefit ratio (Petronio and Altman 2002). However, previous literature identifies other criteria that may also influence how individuals control their privacy, such as behavioral economics (Dinev et al. 2015) or information sensitivity (Mothersbaugh et al. 2011) (see sections 2.2, 2.3 and 2.4). Furthermore, as access to information is shared, co-owners are also able to control the privacy of others (Biczók and Chia 2013). To get beyond the superficial view of the rules governing the control of privacy in the digital age, research question 2 asks how individuals control their own and others' privacy needs:

Research question 2: What determines individuals' control of their own and others' privacy?

Privacy Turbulence

Traditionally, privacy turbulence is caused by co-owners with unauthorized access to private information and is rectified by original owners re-defining collective boundaries to remove unauthorized access from co-owners (Petronio and Altman 2002). However, in the digital age, a wide range of co-owners have potentially unauthorized access to private information (see section 2.1.1.2) (Karwatzki et al. 2017). For example, new technologies give hackers easier access to personal information. Simultaneously, the digital age also affords individuals new ways to protect their privacy against unauthorized access, for example, by installing technical tools that block hackers from gaining access to their private information (see section 2.2.2). Research question 3 thus asks how the concept of privacy turbulence needs to be considered in the digital age:

Research question 3: How do individuals handle privacy turbulence in the digital age?

The following section outlines the methodology and data analysis techniques used by the eleven papers constituting this dissertation to answer these sub-research questions and with them the overall research question.

4 METHODOLOGY AND DATA ANALYSIS

To answer the overall research question, this dissertation presents eleven papers that implement various methodologies, depending on the nature of the individual research question. The first part of this section explains the choice of methodologies and discusses each in terms of the *parameters* used to classify the methodology, namely the research approach, the research method, the data collection technique and the duration. Each parameter has particular *instances*, which show how each parameter

can be classified. The second part of this section presents the data analysis, explaining the detailed instances of data analysis techniques used in the eleven papers.

	Parameter	Instances				
Methodology (section 4.1)	Research approach	Quantitative			Qualitative	
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles
	Duration	Cross-sectional			Multiple snapshots	
Data analysis (section 4.2)	Data analysis	Structural equation modeling	Instrument development	Logistic regression	t-Test for independent samples	Interview coding

Table 8. Overview of the methodology and data analysis of this dissertation

An overview of the methodologies and data analysis is given Table 8. This table shows the different parameters as well as the corresponding instances. Table 8 should be read like a morphological box. For each parameter, at least one instance is selected in one of the eleven papers⁴. The instances of parameters are not interreliant. For example, just because the research is quantitative it does not mean that only literature reviews and surveys may be chosen.

More details on the methodology is given in section 4.1, followed by insights into data analysis in section 4.2. In section 4.3, a summary of the methodologies and data analysis techniques used in this dissertation is given. In the appendix (see section 8.2) of this introductory paper, overviews of the combinations of methodologies and data analysis applied in the eleven papers are provided, applying Table 8.

4.1 METHODOLOGY

A methodology can be differentiated by four different parameters: The research approach, the research method, the data collection technique as well as the duration (Chen and Hirschheim 2004). A research approach (or research design) can be quantitative – with an emphasis on quantitative data – or qualitative – with an emphasis on qualitative data (Recker 2013). The research method is the particular strategy followed to answer the focal research question (Recker 2013). Data collection techniques are the ways information is collected in line with the research method (Harrison and Wells 2000). Finally, the duration of research can be cross-sectional or include multiple snapshots (Chen and Hirschheim 2004). All four parameters are explained in more detail below.

4.1.1 Research approach

The research approach can be quantitative or qualitative. Whereas quantitative research has an emphasis on quantitative data, usually numbers, qualitative research has an emphasis on qualitative data, usually words (Recker 2013). Specifically, quantitative research analyzes numerical data to describe the relationship between factors (Chen and Hirschheim 2004). The results of such analyzes are considered strong scientific evidence of how a phenomenon works. This approach adheres to a positivist philosophy, which means the study posits a realist and objectivist ontology including the assumption

⁴ In a morphological box, usually only one instance per parameter may be selected. However, in several of the papers, multiple methodologies or data analysis techniques have been implemented. In such a case, more than one instance per parameter is selected.

that theories can be falsified (Recker 2013). Most of the papers comprising this dissertation take a quantitative research approach (**Papers II-IX** and **Paper XI**).

In contrast, qualitative research describes and helps understanding the situation behind the factors (Chen and Hirschheim 2004). This approach helps flesh out the context in which a phenomenon is located (Recker 2013). Qualitative research, which usually analyzes text or words are especially helpful in clarifying the boundary between phenomena and their context, and to understand complex, multifaceted, or even hidden phenomena. Qualitative research provides more comprehensive insights and is often considered interpretive in nature. Qualitative research is by nature often more subjective than quantitative research (Recker 2013). **Papers I** and **X** follow a qualitative research approach. Also based on the research approach, a particular research method can be chosen.

4.1.2 Research method

A research method “*is a term that describes the strategy of inquiry used to answer a specific research question*” (Recker 2013, p. 36). There are many different research methods. Rather than attempting to be exhaustive, this introductory paper introduces the most relevant research methods used in the eleven papers comprising this dissertation which are needed to understand how the answers to the research questions posed by the papers were determined.

4.1.2.1 Literature review

Literature reviews are used to grasp the breadth of a topic and to establish the current state of knowledge about that topic. A literature review summarizes the literature in a field without collecting or analyzing primary data (Paré et al. 2015). Previous research typically guides the literature review (Paré et al. 2015; Webster and Watson 2002). Typically, the scope of publication outlets, keywords, publication date and search fields (e.g. title or full text) are defined. After the initial search, the results are analyzed based on established selection criteria, which may entail reading the title, abstract or keywords. Then each selected article is read and articles that do not meet particular criteria are dismissed. Forward and backward searches are typically undertaken to identify studies not identified by the initial search. Following Webster and Watson (2002), a concept-centric approach is recommended to classify the literature.

In **Paper I**, a review of literature on privacy was conducted with the particular goal of identifying dependent variables, research methods, theories, research settings, and durations in privacy research in the domain of IS. Since this literature review applied to the IS domain, the scope of publication outlets was limited to the AIS basket of eight journals (AIS 2011) and ICIS and ECIS proceedings, the two major IS conferences (vhb-jourqual 2016). No earliest publication date was set. The search then included titles, abstracts and keywords for the sole keyword “privacy” (Li 2011b). Of the 308 articles resulting from the initial search, a closer reading left 84 relevant articles. A subsequent backward and forward search identified 58 additional relevant articles. In total, **Paper I** analyzed 142 articles. For this dissertation, the literature review has also been updated to also gather the current state of knowledge, leading to a final number of 182 analyzed articles (see section 8.1 in the appendix for more details). The goal of the ensuing descriptive literature review is collect, codify and statistically analyze the frequency of topics, methods or theories to produce quantitative results (Paré et al. 2015). In keeping with previous research (Onwuegbuzie and Frels 2016), since the analysis follows a qualitative research approach, literature reviews are classified as qualitative, even though the results have a more quantitative nature.

Papers II-XI and **Paper XI** also contain literature reviews to identify relevant research gaps.

4.1.2.2 Survey

Surveys are used to gather primary data, typically through questionnaires (Chen and Hirschheim 2004). Surveys are useful for collecting data about the characteristics, actions, perceptions, attitudes or

opinions of a large group (Alavi and Carlson 1992). Surveys are useful when the research question is about “how and why” something is happening, and they are typically considered in quantitative research (Recker 2013).

Surveys are generally used to explore, describe or explain. Exploration means becoming more familiar with a previously unknown topic. Description means portraying the opinion, behavior or attitudes of the large group about a certain topic. Explaining means testing theories and causal relationships between theoretical constructs. The basis for such relationships is usually grounded on theory and how and why there should be such a relationship. Typically, a relationship between two theoretical constructs and the directionality of this relationship are tested. This provides evidence not only of a link between theoretical constructs, but also the reasons for the link (Recker 2013). This dissertation uses surveys only to *explain* occurrences and not to explore or to describe them.

Papers II–VII and **Paper IX** of this dissertation use surveys. Table 9 provides an overview of the research objectives and the number of valid participants for each paper using a survey. Different samples of participants were surveyed depending on the specific research question. One way to recruit participants is through Amazon Mechanical Turk (mTurk), an online crowdsourcing market (OCM) which pays individuals money to conduct tasks. mTurk has been successfully validated by previous research (Steelman et al. 2014) and it is considered as good as or superior to other databases (Lowry et al. 2016). mTurk has also been used successfully in privacy settings (e.g., Bellekens et al. 2016; Pu and Grossklags 2015). In all papers comprising this dissertation that surveyed individuals through mTurk, several of the following guidelines suggested by previous research were implemented. *Previously completed tasks*: participants are only accepted if they have successfully completed a high number of tasks (Steelman et al. 2014). *Trap questions*: participants are only accepted if they correctly answer questions designed to ensure they are reading the content rather than clicking randomly, e.g. ‘please click on ‘strongly agree’’ (Lowry et al. 2016). *Location of participants*: participants are only accepted if they live in the U.S., since this yields the most reliable results (Steelman et al. 2014). *Reverse coded items*: participants are only accepted if their answers to reverse coded survey items are sensible and logically consistent with regularly coded survey items (Weijters and Baumgartner 2012). For example, if a participant evaluates a set of statements about perceived risk of disclosing information as high on a 7-point Likert scale, their response to not perceiving risk of such discloser should be low on the same scale.

Paper	Research objective	Final number of participants
Paper II	How and why individuals justify mass surveillance	135
Paper III	How and why resignation may lead to a non-working privacy calculus	166
Paper IV	How and why subjective norm may affect the privacy calculus	1,466
Paper V	Explaining the effect of laziness on the privacy paradox	188
Paper VI	How and why different levels of personality traits and especially mindfulness affect the perception of technostress	126 (study 1), 408 (study 2)
Paper VII	How and why mindfulness affects threat appraisal and coping appraisal	175
Paper IX	How and why the extended concept of information sensitivity explains the protection of information by co-owners	155

Table 9. Research objective and final number of participants of papers that implemented surveys

The following describes how and why surveys were conducted for each paper.

In **Paper II**, the goal was to explain how and why individuals justify mass surveillance, making a survey a particularly suitable method. Participants were recruited from mTurk. 141 participants took part in the initial survey, and the final dataset consisted of 135 participants.

In **Paper III**, the aim was to find out how and why resignation leads to a non-working privacy

calculus, making a survey a suitable method. Participants were recruited from mTurk. Of the 180 participants who took part in the survey, 166 surveys remained after applying the guidelines described above.

In **Paper IV**, the question was how and why subjective norm affect the privacy calculus. As the aim here is to explain something, a survey is a suitable method. To gather survey participants, the 25,700 current followers of a woman with an Instagram profile were informed about the academic study and invited to take part in the survey. A total of 1,466 participants answered the survey fully.

In **Paper V**, the study was conducted to explain the effect of laziness on the privacy paradox in the domain of SNS and Facebook in particular, indicating that a survey was a suitable method. This study includes three surveys. The first survey assessed the reliability and validity of a newly developed construct laziness. 28 participants from mTurk participated in that study. The second and third surveys were used to collect data to test the research model. Since this research model follows a multiple snapshot approach (see section 4.1.4) (Chen and Hirschheim 2004), two surveys were necessary. Survey participants were found in two ways. First, people who had registered on the University of Bamberg website to voluntarily take part in future surveys were invited. Second, participants of an annual survey about working conditions by the Chair of the Department of Information Systems and Services, conducted together with a project partner, were asked, whether they wish to be invited by email to participate in future studies (Weitzel et al. 2017c)⁵. The project partner is a human resources organization that provides services for organizations and employees. The contact with the project partner was established in the course of studies undertaken about working conditions, and data collected through these surveys was also allowed to be used in scientific research. Participation was incentivized by raffling off technical products among study participants. In total, 1,265 people were invited to participate in the surveys.

243 participants took part in both surveys. After removing individuals who do not use Facebook and who provided unrealistic information such as being online for more than 24 hours a day or claiming to have an unrealistic number of Facebook friends, the total was 188 participants.

In **Paper VI**, the aim was to explain how and why different levels of personality traits and especially mindfulness affect the perception of technostress, making a survey a suitable method. For this paper, two surveys were conducted, one in an organization and a second via mTurk. In the first survey, participants who work at a large organization with 3,500 employees and a sales volume of around 500 million euros were sought. A total of 126 employees submitted valid responses to the survey. A total of 408 participants submitted valid responses to the second survey on mTurk. The results from the organization survey and the mTurk survey were statistically comparable, confirming that mTurk yields reliable results.

In **Paper VII**, the aim was to determine how and why mindfulness affect threat appraisal and coping appraisal, which makes a survey suitable. To gather participants for the survey, the same procedure as in **Paper V** was followed, but the participants were different because the survey was taken a different year. This time, the pool consisted of 1,639 potential survey participants. After invalid responses and duplicates were removed, the survey invitation was sent to 1,615 email addresses. Participation was incentivized by raffling off technical products among study participants. In total, 371 participants took part in the survey, 175 participants of whom were exposed to a high fear appeal and selected as the final

⁵ This annual survey about working conditions consists of the study Recruiting Trends and the study Bewerbungspraxis. Both were first published in 2004 and from then on annually, with the author of this dissertation having been involved in all studies since 2015: Weitzel et al. (2015a, 2015b, 2015c), Weitzel et al. (2016a, 2016b, 2016c, 2016d, 2016e, 2016f, 2017a, 2017b, 2017c, 2017d, 2017e), Weitzel et al. (2018a, 2018b, 2018c, 2018d, 2019a, 2019b, 2019c, 2019d), Weitzel et al. (2020a, 2020b, 2020c, 2020d, 2020e). In total, since then, 23,312 candidates took part in the Bewerbungspraxis and 14 case studies were conducted as part of the Recruiting Trends.

survey participants (see also information on fear appeal in **Paper XI** in section 4.1.2.3).

In **Paper IX**, the goal was to determine to what degree an extended concept of information sensitivity explains protection of information by co-owners. A survey is a suitable method to research this issue. Survey participants were solicited on mTurk and excluded participants who do not use Facebook, which is the context of this study, resulting in 155 valid responses.

Surveys may also be complemented with experiments in an online setting and are then called online survey experiments. These are explained next.

4.1.2.3 Online survey experiment

Generally, experiments are suited to identify cause-effect relationships (Recker 2013). Three terms are important here: treatment (Recker 2013), experiment design and factorial design (Broota 1989). The two basic types of experiments are laboratory experiments and field experiments, both of which can be conducted on- or offline (Karahanna et al. 2018). An online survey experiment is an experiment in a laboratory setting that is conducted online. An explanation for this categorization is given in the following, by introducing the particular terms in more detail.

Treatment: The treatment is the operationalization of the independent variable. In experiments, participants are divided into at least two groups. In a true experimental design, participants are randomly assigned to the groups and in a quasi-experimental design, participants are not randomly assigned (Recker 2013). Each group receives a different treatment, which means that the experimenter manipulates a certain element of the experiment differently for each group (Recker 2013). For example, to find out if the color of a software influences the usage of that software, the experimenter could divide the participants into two groups and the color of the software is the treatment. One group is given red software and the second group is given blue software. In this case, red and blue are the particular operationalizations of the independent variable.

Experimental design: The experimental design is either subject-between or subject-within. In subject-between design, each participant is assigned to one treatment (Broota 1989). In the example above, each participant is assigned to only one of the two groups and is thus given either the red or the blue software. In comparison, a subject-within design means that every participant receives all treatments (Broota 1989). In the above-mentioned example, each participant would be given the red software and then, later, the blue software.

Factorial design: Factorial design describes how many treatments the experiment contains. A one-factorial design includes one factor with two treatments, such as the example above. The uni-factorial design also includes one factor, but more than two treatments, such as if red, blue and green software are included. The multi-factorial design includes more than one independent variable (Broota 1989), such as color and menu font.

Laboratory and field experiments: Independent of the treatment, the experimental design and the factorial design, experiments can either be conducted in the laboratory or in the field. In a laboratory experiment, an artificial setting is built up (Recker 2013). The advantage is that internal validity is high because the variables of interest can be tightly controlled (McGrath et al. 1982). The disadvantage is that artificial settings are often unrealistic and the external validity (generalizability) is low (Karahanna et al. 2018; McGrath et al. 1982). In a field experiment, the experiment takes place in a real-world setting (Recker 2013), ideally in the participant's naturally occurring environment. The advantage is that the experiment is very realistic. The disadvantage is that the internal validity is often low. The external validity depends upon the pool of participants (Karahanna et al. 2018).

Online laboratory and online field experiments: Both types of experiments can be conducted online. This means that the laboratory experiment is moved out of the laboratory to an online setting. Participants are recruited over the Internet and take part in the laboratory experiment online. Even though participants may be in their natural environment, it is still a laboratory experiment because the setting is artificial. The advantage is that a much larger pool of potential participants is accessible in a shorter time, which strengthens the external validity of the experiment. The disadvantage is that since the participants are not in the laboratory, the internal validity may be weaker (Karahanna et al. 2018).

Field experiments can also be conducted online. Participants are again recruited online, but the actual experiment is not undertaken in an artificial setting, but rather in the field. An advantage of online field experiments is that log files may be available to uncover previously unobserved behaviors of participants, such as installing a software they use in their everyday life. This software can include log-files which can be analyzed (Karahanna et al. 2018).

Online survey experiment: A survey experiment also includes a treatment, an experimental design and a factorial design. The treatment is included in the survey itself, e.g. by manipulating its form, content or other components. The experimental design can either be subject-between or subject-within, and different kinds of factorial designs are possible. The participants of the survey are assigned randomly to the particular group (Gaines et al. 2007). Generally, survey experiments attempt to maximize internal and external validity (Barabas and Jerit 2010). An online survey experiment is then a survey experiment conducted online. This term is used to ensure clarity, since the term survey experiment alone does not indicate whether it is held online or offline, such as by telephone or live in public. Likewise, the term online experiment does not indicate whether or not a survey includes a treatment.

In **Paper VIII** an online survey experiment was conducted to determine the degree to which an anchor (Tversky and Kahneman 1974) affects the amount and the accuracy of disclosure. Since the goal was to identify a cause-effect relationship, an experiment is a suitable research method. For the paper, four online survey experiments with participants from mTurk were implemented. Each study included a survey published online, each of which included a treatment. For example, in one study, participants were asked to type information about their last holidays into a text field. The treatment was whether the text field was big or small. The experimental design was subject-between, such that every participant only experienced one treatment. A one-factorial design was chosen, such that only two groups for each study were needed. Since all four studies were conducted online in a web-based system, this was an online survey experiment. In total, 528 participants from mTurk, applying the guidelines mentioned above, took part.

In **Paper XI**, another online survey experiment in the domain of email tracking was conducted. The goal was to find out if participants' responses vary depending on the strength of a fear appeal (Boss et al. 2015). Since the objective was to identify a cause-effect relationship, an experiment was a suitable research method. A fear appeal is a "*persuasive message designed to scare people by describing terrible things that will happen to them if they do not do what the message recommends*" (Witte 1992, p. 329). The fear appeal is included in the survey, making the experiment a survey experiment. In this study and in line with previous research (Boss et al. 2015), the fear appeal was either high or low. The fear appeal thus represents the treatment, which was included directly in the survey. A subject-between design was chosen, such that participants were either confronted with a high or with a low fear appeal. Since the fear appeal was either high or low, it is a one-factorial design. As the study was conducted online, this is an online survey experiment. The participants of this study were from the same pool of participants for **Paper VII**, but this time responses from participants exposed to a high fear and to a low fear appeal were included. In total, 371 participants (175 exposed to a high fear appeal and 196 exposed to a low

fear appeal) were included.

4.1.2.4 Online field experiment

As stated earlier, field experiments can also be conducted online (Karahanna et al. 2018). A potential advantage is that log files might be available that can reveal previously unobserved participant behaviors. Generally, field experiments also contain a treatment, an experimental design and a factorial design. In comparison to laboratory experiments, they take place in a real-world setting, which distinguishes them from laboratory experiments.

In **Paper XI**, besides the online survey experiment, an online field experiment was conducted, again using fear appeal as a treatment in the survey, making the design one-factorial. The difference here is that the dependent variable was observed in the field. Participants in **Paper XI** were sent emails with a hidden image that made it possible to track them. Based on the fear appeal the participants were treated with, log files revealed who protects themselves against tracking and who does not. A field experiment requires a field context in the task (Harrison and List 2004). In this case, participants did not know that there was a task being monitored, which was the participants' behavior to protect against email tracking or not. This behavior was outside the survey but in their natural environment, constituting a field context and making the experiment a field experiment. Since the treatment was online, it is an online field experiment (Harrison and List 2004; Karahanna et al. 2018). In compliance with the law, recipients were also informed in a footer that the email contained a tracking element and an opt-out link was included. None of the participants used the opt-out link. The participants of this study were the same 371 participants who participated in the online survey experiment described in the previous section.

4.1.2.5 Case study

In a case study, a phenomenon can be investigated in depth in its natural setting. Usually, it is a contemporary phenomenon in a real-life domain. Case studies are common when the boundaries between the phenomenon and the context are unclear (Recker 2013). The case study itself can have several design types including one or more phenomena (cases) with one or more units of analyzes (e.g. participants) (Yin 2014).

In **Paper X**, a case study was conducted to better understand the degree to which individuals' levels of privacy concerns vary depending on the relationship with the co-owner causing these privacy concerns. This was an embedded case, which means it focused on one case (level of privacy concerns) and several units of analysis (participants). Since the level of privacy concerns is contemporary (Smith et al. 2011) and since the role of context in determining the level of privacy concerns was unclear, case study research is a suitable research method. Case study participants with a basic knowledge of technology were selected, who had experience with privacy concerns and who may have a strong relationship with co-owners of their private information (e.g. friends) and, through technology, an absent relationship with co-owners (e.g. governmental agencies). It was determined that students were suitable participants and advertised publicly at the University of Bamberg. In total, the case study was conducted with eleven participants.

4.1.3 Data collection techniques

Each of the research methods can use different data collection techniques to gather suitable data.

4.1.3.1 Questionnaires

Questionnaires are the medium between the researcher and the participant answering the questionnaire. The aim of a questionnaire is to gather information that will enable the researcher to answer the research questions of her study. Therefore, the required data must be collected as accurately as possible. Throughout the questionnaire, the researcher includes the questions to which she needs answers, to then answer her research question (Brace 2014).

The questions in a questionnaire should always be asked the same way to all participants, including the sequence of questions and how the questions are formulated. In this regard, a questionnaire is different from an interview (see following section). The survey experiment is an exception to this rule because the treatment may alter the content of the survey. Participants can either respond to questionnaires themselves or say their responses to an interviewer face-to-face, via telephone or via video conference. Self-completion questionnaires can be paper-based or web-based (Brace 2014). Questionnaires are the usual way to gather data in a survey (Chen and Hirschheim 2004) and all of the papers comprising this dissertation conducting surveys contain web-based self-completion questionnaires. **Papers II-IX** and **Paper XI** use such web-based self-completion questionnaires driven by Limesurvey software.

4.1.3.2 Interviews

Interviews are the most common data collection technique in qualitative research. They can be conducted face-to-face, via telephone or via video conference. As with surveys, interviews can be descriptive, explanatory or exploratory. Furthermore, interviews can be unstructured, semi-structured and fully structured. In most cases, interviews are semi-structured. Semi-structured interviews are flexible, which means that the interviewer can adapt her questions flexibly depending on the respondent's answers. The interviewer typically has a set of questions to ask, but may ask them in a different sequence or with a different focus in each interview (Recker 2013). A common special interview technique is the critical incident technique, in which interviewees are asked to describe experiences in a particular setting (Flanagan 1954).

In **Paper X**, interviews were held in order to understand stakeholders directly involved in a situation (Forte et al. 2009; Kolfshoten et al. 2012; Sarker et al. 2013). The interviews lasted about 20 minutes and were recorded and later transcribed using Microsoft Word and VLC Player software.

4.1.3.3 Past literature

The past literature is the cumulative knowledge base in a scholarly field. Past literature can be analyzed to identify research gaps and determine the current state of knowledge on a topic (Recker 2013). A review of past literature is suitable to bring the research question into focus and for establishing a theoretical basis for the research study (Okoli and Schabram 2010). A fully structured literature review can summarize or synthesize the existing literature in a particular field and reveal particular research gaps (Schryen 2015). A structured literature review can serve as the main research method in a study, leading to a pure review article (Paré et al. 2015). Since the literature review takes place in a scientific domain, the literature to be used is also of scientific nature.

In this dissertation, past literature has been used in almost every paper to either present a structured review article (**Paper I**) or to identify research gaps (**Papers II – IX** and **Paper XI**).

4.1.3.4 Log files

Log files are files of records that can be appended to indefinitely and read back sequentially or randomly. When opening log files, one can access information prior to a previous point in time (Finlayson and Cheriton 1987). Usually, a log file contains a list of actions that have occurred with or through the technology and are generated automatically by the technology (Elhiber and Abraham 2013).

Log files were used in **Paper XI** as part of an online field experiment. To find out if participants of the study were trackable via email or not, a tracking image was included in emails sent to the participants. Google Analytics technology was used to create log files based on the tracking image.

4.1.4 Duration

A research project varies in terms of the duration of data collection. Most research studies collect

cross-sectional data (Chen and Hirschheim 2004). Cross-sectional data is collected as a snapshot at a particular point in time (Orlikowski and Baroudi 1991). Cross-sectional research is especially suitable when the relationship between the independent and dependent variable is independent of time (Zheng et al. 2014). *Multiple snapshots* refer to the second possibility of duration in a research study. With multiple snapshots, the study is also of cross-sectional nature. However, it involves more than one single-data collection. Examples refer to different experiments, various treatments or additional subjects (Chen and Hirschheim 2004).

Papers II, III, IV, VII, IX and X report on cross-sectional research. Here, one single study at one point of time has been conducted. **Paper V, Paper VI, Paper VIII and Paper XI** analyze data collected from multiple snapshots. In **Paper V** and **Paper VI**, surveys were conducted at two different points of time with the same pool of participants. In **Paper VIII**, four different experiments with different subjects to research on the same phenomenon were created, however, at the same point of time. In **Paper XI**, a survey was conducted at the first point of time and log files were generated at a second point of time.

This section has discussed what research method was chosen and how data with different durations was collected. To analyze the data, different techniques were applied in the eleven papers comprising this dissertation, which are explained next.

4.2 DATA ANALYSIS

To analyze the data, the following techniques were applied in the eleven papers comprising this dissertation: structural equation modeling, instrument development, logistic regression, the t-test for independent samples, and interview coding.

4.2.1 Structural equation modeling

To test hypotheses or to explore patterns in data, first-generation techniques such as factor analysis and regression analysis were used. Over the last decades, second-generation techniques have overcome many limitations of these first-generation techniques. Second-generation techniques enable unobservable variables to be measured indirectly through directly observable indicators. With second-generation techniques, multivariate analysis now makes it possible to handle multiple variables simultaneously. Structural equation modeling (SEM) (Hair et al. 2017) are multivariate second-generation statistical tools that complement, among others, multiple regression and ANOVA methods. They are used primarily to analyze data and test hypotheses which assume a relationship between variables (Bagozzi and Yi 2012).

SEM includes partial least squares SEM (**PLS-SEM**) and covariance-based SEM (**CB-SEM**), each of which has its own goals and certain different aspects. Since PLS-SEM was applied in most papers comprising this dissertation, the references to SEM in the following sections focus on PLS-SEM. More details on the difference between both approaches are given in section 4.2.1.1 (Hair et al. 2017).

To test hypotheses, SEM relies on several concepts: Latent variables (also called constructs) reflect the central variables in the theoretical model. These latent variables are unobservable but can be measured indirectly through generally multiple indicators, which serve as a proxy (Hair et al. 2017). For example, privacy risks cannot be measured directly because there is no standard and observable measurement for privacy risks. Instead, several indicators are used to measure privacy risks such as “In general it would be risky to give personal information to this Website” or “My personal information could be inappropriately used by this Website” (Xu et al. 2011a). Participants then answer to these indicators usually on a Likert scale from “Strongly agree” to “Strongly disagree”. The combination of these indicators is a proxy for measuring the latent variable privacy risks. The relationship between a latent variable and its indicators is called **measurement model**, which is explained in section 4.2.1.2.

A measurement model may include latent variables measured by reflective indicators or latent variables measured by formative indicators. A combination of reflective or formative measured latent variables in one study is possible, however, each latent variable is measured either reflectively or formatively. In particular, latent variables measured by reflective indicators are measured indirectly by indicators that represent the corresponding latent variable. They all reflect the meaning of the latent variable and should thus be highly correlated with each other. Furthermore, since they all reflect the same meaning, they are interchangeable and removing one indicator should usually not affect the reflected latent variable. In contrast, formative indicators cause the latent variable. They are not interchangeable, and each formative indicator captures one aspect of the latent variable. Hence, removing one formative indicator also alters the meaning of the latent variable (Hair et al. 2017). In this dissertation, only reflective indicators are used, which is why no further details on the differentiation is provided.

Furthermore, there are also relationships between latent variables, which are the causal relationships hypothesized in the research study. A latent variable causing another latent variable is called an independent variable, and the latent variable caused by the independent variable is called a dependent variable. A variable can also be an independent and a dependent variable at the same time when it is caused by one independent variable and also causes another dependent variable. The interplay between latent variables is called **structural model**, which is explained in section 4.2.1.3 (Hair et al. 2017).

In a structural model, the independent variable and the dependent variable may have a direct relationship. However, a so-called mediator may intervene in that direct relationship and the relationship might be altered by a so-called moderator. More details on **mediation and moderation** are given in section 4.2.1.4.

Furthermore, latent variables can either be first-order constructs or higher-order constructs. Usually, first-order constructs are used. However, higher-order constructs may be used to capture more abstract concepts. Higher-order constructs are a composite of first-order constructs, whereby the first-order constructs are dimensions of the higher-order construct (Hair et al. 2017). More details on **higher-order constructs** are given in section 4.2.1.5.

Finally, the results may not only be dependent on the constructs themselves but also on the measurement method. The variance that is caused by this measurement method is called **common method bias** (Aguirre-Urreta and Hu 2019). More details on this are given in section 4.2.1.6.

4.2.1.1 Difference between PLS-SEM and CB-SEM

As mentioned above, two types of SEM are PLS-SEM and CB-SEM. Whereas CB-SEM is more suitable in an environment where an established theory is tested, PLS-SEM better fits a research context where the theory is less developed and the research model predicts and explains (Hair et al. 2017; Rigdon 2012).

PLS-SEM and CB-SEM differ in several ways. One key difference is the objective target. CB-SEM is used to reproduce the variance-covariance matrix, i.e. the relationships between the variables. In contrast, PLS-SEM is used to predict the data matrix that reflects the values from the participants, i.e. to explain the dependent variable. Therefore, PLS-SEM is also considered a variance-based approach to SEM (Hair et al. 2017; Weiber and Mülhhaus 2014). Another difference refers to the measurement model. Whereas PLS-SEM is able to treat both reflective and formative measurement models even in the same research model, CB-SEM is only applicable to reflective measurement models. To assess the quality of a research model, PLS-SEM uses only partial quality criteria (Weiber and Mülhhaus 2014). Although there are already global quality criteria in place, they should be used with extreme caution because they are still in the development phase (Hair et al. 2019). In contrast, CB-SEM uses global

quality criteria to assess the overall model fit. Furthermore, regarding sample size, whereas PLS-SEM is suitable for small sample sizes, CB-SEM is suitable for large sample sizes (Weiber and Mühhlhaus 2014). See Table 10 for an overview.

Criterion	PLS-SEM	CB-SEM
Objective target	Prediction of data matrix	Reproduction of the empirical variance-covariance matrix
Measurement model	Reflective and formative	Reflective
Quality criteria	Partial quality criteria	Global quality criteria
Sample size	Small	Large

Table 10. Differences between PLS-SEM and CB-SEM based on Weiber and Mühhlhaus (2014)

Scholars have made various recommendations on when to choose which approach. Generally, PLS-SEM is better suited than CB-SEM when the research focus is more predictive and exploratory, when the model is complex and has many indicators and constructs, and when latent variable scores will be used in subsequent analyzes, e.g. in higher-order constructs (Hair et al. 2017).

PLS-SEM was applied in **Papers II, III, V and IX** because they are exploratory and predictive. For example, **Paper II** uses system justification theory, which has never been applied in IS-research before. **Paper V** establishes laziness as a new, specific construct in IS research and incorporates it into the privacy paradox. Furthermore, **Papers VI and VII** include mindfulness as a hierarchical component and the latent variable scores are used in subsequent analyzes, making PLS-SEM the suitable approach. **Paper XI** includes many constructs and indicators, so PLS-SEM is again the suitable approach. SmartPLS 3 was used to apply PLS-SEM.

CB-SEM was applied in **Paper IV**, where the research model combines two established theories. Hence, the focus was more on theory testing rather than conducting exploratory research, making CB-SEM the suitable approach. SPSS 25 and AMOS 25 were used to apply CB-SEM.

In summary, PLS-SEM and CB-SEM are both good techniques to analyze data through SEM. When the focus is exploratory, PLS-SEM is more suitable and when the focus is on theory testing, CB-SEM is more suitable. Therefore, since both has been done in this dissertation, also both approaches have been implemented in this dissertation. Independent of PLS-SEM or CB-SEM, in both cases, the measurement model and the structural model need to be assessed.

4.2.1.2 Assessing the measurement model

Before the structural model can be assessed, i.e. before the hypotheses can be tested, the validity and reliability of the applied measurements need to be checked (Hair et al. 2017). Reliability refers to the consistency of a measurement (Bollen 1989), in the sense that it is stable and repeatable with different persons or on different occasions (Drost 2011; Nunnally 1978). Validity refers to whether the item measured is the item the researcher intended to measure (Bollen 1989). The criteria considered to check measure in regard to validity and reliability vary depending on whether reflective or formative indicators are used (Hair et al. 2017). Since this dissertation only uses reflective indicators, the following criteria only refer to reflective indicators, i.e. a reflective measurement model. Furthermore, the overall model fit is only applicable in CB-SEM. An overview is given in Table 11.

Criterion	Definition	Measure	Recommended threshold	Author(s)
Content validity	The extent to which the instrument is representative of the construct	Valid constructs from previous literature or own operationalization	-	Haynes et al. (1995)
Discriminant validity	The extent to which concepts differ from each other	Fornell-Larcker criterion	Square root of AVE > Inter-construct correlation	Fornell and Larcker (1981)
		HTMT _{0.85} and HTMT _{0.90}	For HTMT _{0.85} < 0.85 For HTMT _{0.90} < 0.90	Henseler et al. (2014)
Convergent validity	The extent to which a construct correlates with another construct	Convergent validity on construct level	AVE > 0.5	Hair et al. (2017)
		Indicator reliability	Indicator loading > 0.707	Hair et al. (2017)
Construct reliability	The degree of internal consistency	Cronbach's Alpha	> 0.70	Hair et al. (2017)
		Composite reliability	> 0.70	Hair et al. (2017)
Overall model fit (only CB-SEM)	The difference between the covariance matrix from the hypothesized model and the covariance matrix from the sample	CFI	> 0.95	Hu and Bentler (1999)
		RMSEA	< 0.06	Hu and Bentler (1999)
		SRMR	< 0.08	Hu and Bentler (1999)
		χ^2/df	< 3	Hair (2010)
		NFI	> 0.9	Bentler (1990)

Table 11. Criteria, measures and thresholds to assess reflective measurement models, based on Hair et al. (2017) and Hair (2010)

Content validity: *Content validity is the degree to which elements of an assessment instrument are relevant to and representative of the targeted construct for a particular assessment purpose* (Haynes et al. 1995, p. 238). The elements refer to the indicators of SEM and the construct is the latent variable. Hence, with content validity, the indicators should best represent the corresponding latent variable and not some other variable. To ensure content validity, the papers applying SEM use already established items from previous literature (**Papers II-VII** as well as **Paper IX** and **Paper XI**). In addition, all items used in the particular study were discussed with academic colleagues.

In **Paper V**, laziness was included in the research model. Since laziness has not been used in previous IS studies, no items existed, and so new items had to be developed. The process for the development of these items is described in section 4.2.2.

Discriminant validity: Discriminant validity tests the degree to which the latent variables differ from each other and do not measure the same underlying concept. The two most common approaches to ensure discriminant validity are the Fornell-Larcker criterion (Fornell and Larcker 1981) and the heterotrait-monotrait ratio (HTMT) of the correlations of the latent variables (Henseler et al. 2014). The Fornell-Larcker criterion is true when the square root of the average variance extracted (AVE) is greater than the highest cross-loading of one construct with all other constructs. If this is the case, then the construct shares the highest amount of variance with its indicators rather than with any other construct (Hair et al. 2017). The HTMT is defined by two values in relation to each other: the mean of the correlations of items across constructs and the mean of the average correlations for the items measuring that same construct. If HTMT is high, then discriminant validity might be problematic (Hair et al. 2019). The HTMT indicates discriminant validity when the HTMT value is below 0.85 or below 0.90 (Henseler et al. 2014). Recent publications argue that the Fornell-Larcker criterion cannot always recognize discriminant validity, so scholars recommend including HTMT in studies applying SEM to ensure discriminant validity (Hair et al. 2019).

In this dissertation, the papers applying SEM (**Papers II-VII** as well as **Paper IX** and **Paper XI**) considered the HTMT or the Fornell-Larcker criterion to ensure discriminant validity.

Convergent validity: Convergent validity is “the extent to which a measure correlates positively

with alternative measures of the same construct” (Hair et al. 2017, p. 112). Two criteria are important in ensuring convergent validity. First, *convergent validity on the construct level*. In this case, an AVE of over 0.5 shows that the indicators explain at least half of the variance of the corresponding construct. This criterion was met in all papers of this dissertation (**Papers II-VII** as well as **Paper IX** and **Paper XI**). Second, *indicator reliability* represents convergent validity on the outer loadings. High indicator loadings indicate that the indicators have much in common, which is captured by the latent variable. At least these indicators should be significant. Furthermore, particular loadings representing “*how much of the variation in an item is explained by the construct and is described as the variance extracted from the item*” (Hair et al. 2017, p. 113) are required. Since a latent variable should explain at least 50 percent of an indicator’s variance, the value of the loading should be at least 0.707 because the square root of 0.50 is 0.707. Items below 0.707 but still above 0.4 may be included if excluding the item would decrease the composite reliability. Items below 0.4 must be excluded. In all of the papers comprising this dissertation, only indicators fulfilling these criteria were considered reliable items and were included (**Papers II-VII** as well as **Paper IX** and **Paper XI**).

Construct reliability: The reliability or internal consistency of a latent variable is assessed using two criteria. First, Cronbach’s Alpha measures the intercorrelation between the indicators. This value should exceed 0.70. Second, composite reliability measures the reliability of a latent variable. This value should also exceed 0.70. In all papers (**Papers II-VII** as well as **Paper IX** and **Paper XI**), at least one of the two criteria was applied and yielded satisfactory results.

Overall model fit: The overall fit of a model is usually only calculated in CB-SEM. Even though it can be calculated in PLS-SEM, it is not recommended (Hair et al. 2017; Hair et al. 2019). Determining the overall model fit in CB-SEM indicates the degree to which the covariance matrix from the hypothesized model differs from the covariance matrix derived from the sample. If this difference is non-significant, then overall model fit is indicated. Overall model fit is evaluated using several criteria. The most common is the χ^2 divided by the degrees of freedom. Since this test has some limitations, other criteria are usually considered as well, including the comparative fit index (CFI), the normed fit index (NFI) (Weiber and Mülhauß 2014), the standardized root mean square residual (SRMR) and root mean square error of approximation (RMSEA) (Hu and Bentler 1999). All of these measures indicate the degree to which the hypothesized model differs from the sample model. An overview of all fit criteria, including the recommended thresholds, is given in Table 11.

If the measurement model proves valid and reliable, the structural model can then be evaluated.

4.2.1.3 Assessing the structural model

The structural model depicts the underlying theoretical assumptions with hypotheses reflected by the interconnected latent variables. By assessing the structural model, one can evaluate the predictive capabilities of the model and whether the hypothesized relationships between the latent variables are supported or rejected. Several criteria are used to assess the structural model. An overview is given in Table 12.

Criterion	Definition	Evaluation / Recommended threshold	Author(s)
Sign and magnitude of relationships	A change of one unit in the independent variable changes the dependent variable by the size of the value of the relationship between both variables when everything else remains constant.	The value is between -1 and +1. The closer the value is to 0, the weaker the relationship is. The closer it is to -1 or +1, the stronger it is.	Hair et al. (2017)
Significance level of relationships	The maximum probability that is allowed to mistakenly reject a true null hypothesis.	A p-value needs to be below a α -value to be statistically significant; α -values are usually 0.05, 0.01 or 0.001.	Hair et al. (2017)
Coefficient of determination (R^2 values)	The predictive power and the entire amount of variance in the dependent variable that is explained by all independent variables linked to it.	Depends largely on the research domain. Rules of thumb: > 19 percent: weak > 33 percent: moderate > 67 percent: substantial	Chin (1998); Hair et al. (2017)
Effect size (f^2)	The impact of an independent variable on the dependent variable if the independent variable is omitted.	Direct effect: > 0.02: small > 0.15: medium > 0.35: large	Cohen (1988)
		Moderating effect: > 0.005: small > 0.01: medium > 0.025: large	Kenny (2015)

Table 12. Criteria, definitions and evaluation of criteria to assess the structural model, based on Hair et al. (2017)

Sign and magnitude of relationships: The relationships between the latent variables reflect the hypotheses. In PLS-SEM, the relationships between latent variables are standardized and have a value between -1 and +1. A value close to -1 reflects a strong negative relationship, whereas a relationship close to +1 reflects a strong positive relationship. The closer the relationship is to 0, the weaker the relationship is (Hair et al. 2017). The value represents how much a change in the independent variable affects the dependent variable. A change of one unit in the independent variable changes the dependent variable by the size of the value of the relationship between both variables when everything else remains constant (Hair et al. 2017).

Significance level of relationships: Generally, a value close to +1 or -1 will likely be significant and a value which is close to 0 will likely be insignificant. Nonetheless, the significance still needs to be tested. A significant relationship is one which is different from 0 in the population (Hair et al. 2017). In other words, that relationship is not based on coincidence, but rather represents a relationship in the entire population. A relationship that is non-significant means that the relationship is based solely on coincidence. The statistical significance is indicated by the p-value (Rasch 2014).

Whereas the hypothesized relationship is called “alternative hypothesis”, the hypothesis that states that the relationship is merely based on coincidence is called “null hypothesis”. A significance level represents the maximum probability allowed to mistakenly reject a true null hypothesis. In other words, assuming that a relationship is occurring in the population even though in fact it is not. This significance level is represented by the α -value. For example, a α -value of 5 percent indicates that the probability that the null hypothesis has mistakenly be rejected may not be above 5 percent (Rasch 2014).

Usually, α -values are on a level of 5 percent, 1 percent and 0.1 percent. A relationship is statistically significant if the p-value is smaller than the α -value. The smaller the p-value, the stronger the significance as long as it is below the α -value (Rasch 2014). To calculate the p-value, in PLS-SEM, bootstrapping is applied. With bootstrapping, subsamples of the original sample are randomly drawn with replacement and the model is estimated using these subsamples. Usually, this procedure is repeated up to 5,000 times (Hair et al. 2017).

Coefficient of determination (R^2 values): The coefficient of determination is the most common measure in PLS-SEM to evaluate the structural model. It represents the predictive power and shows the entire amount of variance in the dependent variable explained by all independent variables linked to it. The value can range between 0 and 1. Acceptable values vary strongly, depending on the complexity of the model and the general context, but a general rule of thumb is that R^2 values above 19 percent are considered weak, above 33 percent are considered moderate and above 67 percent are considered substantial (Chin 1998; Hair et al. 2017).

Effect size (f^2): It is sometimes desirable to know the extent to which R^2 changes when an independent variable is omitted, such as when investigating the impact of a particular independent variable on the dependent variable. To measure that impact, the effect size (f^2) can be used. Effect sizes for direct effects above 0.02 are considered small, above 0.15 are considered medium and above 0.35 are considered large (Cohen 1988). Effect sizes for moderating effects (see section 4.2.1.4) above 0.005 are considered small, above 0.01 are considered medium and above 0.025 are considered strong (Kenny 2015). Whereas the sign and magnitude of the relationships, its significance and the coefficient of determination are standard procedures in every PLS-SEM approach, the effect size is not always useful. In this dissertation, the effect size was considered in **Papers III, IV, V, and VI**.

4.2.1.4 Mediation and moderation

In a structural model, the independent variable and the dependent variable may have a direct relationship (see Figure 5). However, a so-called mediator can intervene in that direct relationship, and a so-called moderator can alter the relationship.

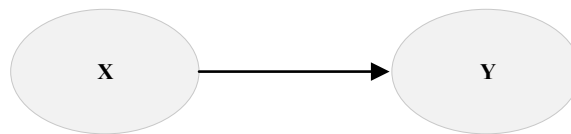


Figure 5. Direct relationship

Mediation: In a structural model, a latent variable may serve as an independent variable, as a dependent variable or as both. If the latent variable is both and the relationships are significant, then it is also called a mediator. In that case, the independent variable (X) has an effect on the dependent variable (Y) through the mediating variable (M) (Hair et al. 2017) (see Figure 6). One example of mediation is when excessive television watching (X) increases the watcher's weight (Y). This alone is not plausible. However, it becomes plausible if this relationship is mediated by concepts like "less exercise" (B). In other words, individuals who watch television excessively (X) are more likely to less exercise (M) which is likely to lead to weight gain (Y).

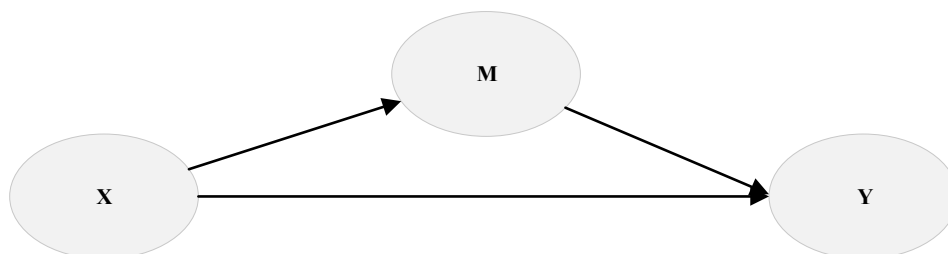


Figure 6. Mediating relationship

More formally, an increase in X will lead to an increase in M which will then subsequently lead to an increase in Y. This is also called an indirect effect. The mediation can either be partial or full. The mediation is full if the direct relationship between X and Y is insignificant as soon as M is included and the relationship between X and M as well as M and Y is significant. The mediation is partial if the

relationship between X and Y remains significant, even after including M (Hair et al. 2017).

To determine the significance of the relationship between X and M as well as M and Y, both p-values are calculated, and the confidence interval must not cut 0 (Hair et al. 2017). Previously, the Sobel test was most frequently used to test mediation. However, since this test requires normal distribution and unstandardized path coefficients, and cannot handle small sample sizes, this test is not applicable anymore, especially in PLS-SEM (Hair et al. 2017). An alternative, especially for PLS-SEM, is to bootstrap the distribution of the sample of the indirect effect (Preacher and Hayes 2008). This approach works well with small sample sizes and abnormal distribution of the sample (Hair et al. 2017). It is therefore the recommended approach in PLS-SEM.

A mediation analysis with bootstrapping was undertaken in **Paper XI**.

Moderation: A relationship may also be moderated. In this case, the effect of the independent variable (X) on the dependent variable (Y) is increased or decreased by a moderating variable (M) (Hair et al. 2017) (see Figure 7). For example, if a participant has extensive knowledge about a topic (X), this leads probably to strong results on an exam about this topic (Y). However, if the individual is very nervous during the exam (M) then this relationship is moderated, and the relationship is weakened.

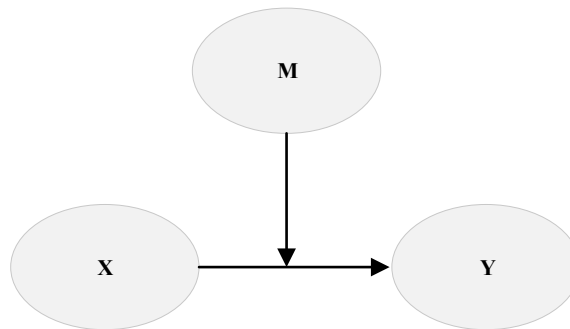


Figure 7. Moderating relationship

The moderator can be on a continuous scale, as it would be in this example, or it can be a categorical variable (Hair et al. 2017) such as gender, which is often included as a moderator in IS studies (Venkatesh et al. 2003). Categorical moderators are especially common in multi-group analyzes, where the entire research model can be moderated and a research model is compared across the instances of the categorical variable (Hair et al. 2017).

A moderation with continuous and categorical variables was undertaken in **Papers III, V, IX and XI**.

4.2.1.5 Higher-order constructs

Latent variables can either be first-order constructs or higher-order constructs. First-order constructs, which are latent variables with a set of indicators, are commonly used. However, to also capture more abstract or complex concepts, higher-order constructs may be used. Higher-order constructs are a composite of first-order constructs, in which the first-order constructs are dimensions of the higher-order construct. Using higher-order constructs makes the entire structural model more parsimonious because there are fewer structural relationships (Hair et al. 2017).

Higher-order constructs are usually second-order constructs, which means the higher-order construct consists of several first-order constructs which are reflected or formed by the corresponding indicators. To evaluate higher-order constructs in PLS-SEM, when the higher-order construct is purely reflective, the two-stage approach and the repeated indicators approach can be applied. In the repeated indicators

approach, all indicators of the lower-order constructs are assigned to the higher-order construct. In addition, the indicators remain indicators of the lower-order construct and are thus used twice. Then, when the measurement model is evaluated, the loadings of the indicators of the lower-order constructs serve as indicator loadings. Also, the relationships between the lower-order constructs and the higher-order construct serve as indicator loadings for the higher-order construct (Hair et al. 2017). In comparison, the two-stage approach builds on the repeated indicators approach. First, all indicators of the lower-order constructs are assigned to the higher-order construct. Here again, the indicators remain indicators of the lower-order constructs and are thus used twice. Second, the latent variable scores are calculated and used as indicators of the second-order construct. The first-order constructs with its indicators are removed from the research model. Hence, the second-order construct then looks like a first-order construct with indicators representing the first-order constructs (Hair et al. 2017).

A higher-order construct in form of a second-order construct was implemented in **Paper VI** and **Paper VII**.

4.2.1.6 Common method bias

In all quantitative studies, the results may not only be dependent on the constructs themselves but also on the measurement method. The variance caused by this measurement method is called common method bias (CMB) (Aguirre-Urreta and Hu 2019). In particular, it is defined as “*variance that is attributable to the measurement method rather than to the constructs the measures represent*” (Podsakoff et al. 2003, p. 879). The measurement method may refer to different aspects such as the content of items, the type of the scale, the response format, or the general context (Fiske 1982) and is one of the most often cited concerns in research studies in the IS domain (Schwarz et al. 2017).

If CMB is an issue, the outcomes can bias the entire research study in terms of biased validity, reliability and values of the relationships between constructs. This in turn will affect the testing of hypotheses. The results are Type I (assuming that there is a significant relationship even though there is none) or Type II (assuming that there is no relationship even though there is a significant relationship) errors. Furthermore, incorrect conclusions about the explained variance in the dependent variable are possible (Aguirre-Urreta and Hu 2019). Hence, CMB can significantly affect the entire research study. CMB may result when the same respondents provide answers for both the independent and the dependent variable, when the research context is the same, when items are similar or due to characteristics of the items (Podsakoff et al. 2003). There are both techniques to prevent CMB and techniques to detect it.

Preventive techniques are used to minimize or avoid CMB by optimizing the collection of data (Aguirre-Urreta and Hu 2019). CMB can be prevented by using different respondents for the independent and dependent variable, by temporally separating the measurements of a data collection and by using different methodologies for each type of data collection (Podsakoff et al. 2003).

Detective techniques alert the researcher that CMB is present (Aguirre-Urreta and Hu 2019). The most widely used detective technique is the Harman’s single factor test. It is conducted by “*examining the results of an exploratory factor analysis and checking whether the first extracted factor explains more than 50 percent of the variance*” (Aguirre-Urreta and Hu 2019, p. 46). If this is the case, then CMB is likely present. However, since it has been shown that the Harman’s single factor test does not always detect CMB, other techniques can be applied (Aguirre-Urreta and Hu 2019). One technique is to measure the effect of a single unmeasured latent method factor (ULMC). This “*involves adding a first-order factor with all of the measures as indicators to the researcher’s theoretical model*” (Podsakoff et al. 2003, p. 894). Then all other constructs are transformed into single-order constructs, i.e. every indicator of every construct is transformed into a single-item construct which points to the construct it had been

an indicator of. In addition, that construct is still assigned to all corresponding items. Then the ratio of the variance extracted including the CMB factor is compared with the variance extracted without the CMB factor. This ratio is compared with previous studies to then detect CMB (Liang et al. 2007). It has been shown that this test also does not always detect CMB (Chin et al. 2012). Further detective techniques include checking the correlation matrix. Since CMB results in extremely high correlations, low correlations indicate that CMB is not present (Pavlou et al. 2007).

In this dissertation, in all quantitative papers (**Papers II-VII** as well as **Paper IX** and **Paper XI**), techniques to prevent and/or detect CMB have been applied. The results indicate that CMB was not present.

4.2.2 Instrument development

All of the papers comprising this dissertation which employed SEM relied on items from previous literature to ensure content validity. One exception is **Paper V**, in which the concept of laziness was added to the research model. Since laziness had not been previously used in previous IS literature, no items were available and so they had to be developed. Following the lead of other scholars (Agarwal and Prasad 1998; Bala and Venkatesh 2016; Ragu-Nathan et al. 2008), the following steps were followed:

First, items were developed based on previous literature and discussions with academic colleagues. *Second*, survey participants assigned the newly developed items to the corresponding construct and were confronted with other similar items and corresponding constructs. Items assigned correctly by at least 61 percent were included (Landis and Koch 1977; Nahm et al. 2002). *Third*, to provide statistical evidence that these items belong together, an exploratory factor analysis (EFA) and a confirmatory factor analysis (CFA) were performed (Ragu-Nathan et al. 2008). In CFA, a fixed number of factors is provided, whereas in EFA, no number is provided, and an algorithm determines the number of factors. The goal is to show the extent to which the newly developed items are grouped together by both types of factor analysis. Criteria used throughout the CFA and the EFA are similar to those used to assess the overall model fit in CB-SEM (see Table 11), including comparative fit index (CFI), standardized root mean square residual (SRMR) and root mean square error of approximation (RMSEA) (Hu and Bentler 1999). EFA and CFA are conducted using another survey including the focal construct and other similar constructs. *Fourth*, to assure construct reliability, measures similar to those used for the measurement model are applied, including composite reliability (CR) and Cronbach's Alpha (Nunnally 1978). *Fifth*, the average variance extracted (AVE) of the newly developed construct is evaluated to ensure discriminant validity. In addition, maximum shared squared variance (MSV) and average shared squared variance values (ASV) need to be accounted for (Hair et al. 2014). See Table 13 for an overview of all criteria, including the definition and recommended threshold of each criterion.

Criterion	Definition	Recommended threshold	Author(s)
ASV	Comparing AVE with the average squared shared variance	< AVE	Hair et al. (2014)
AVE	How much of the variance of the construct is explained	> 0.50	Hair et al. (2017)
CFI	An incremental fit index	> 0.95	Hu and Bentler (1999)
CR	Internal consistency	> 0.70	Hair et al. (2017)
Cronbach's Alpha	Internal consistency	> 0.70	Hair et al. (2017)
MSV	Comparing AVE with the maximum squared shared variance	< AVE	Hair et al. (2014)
RMSEA	Model misfit – closeness of fit of the model in relation to the degrees of freedom	< 0.06	Hu and Bentler (1999)
SRMR	The average standardized residual covariance	< 0.08	Hu and Bentler (1999)

Table 13. Criteria to evaluate newly developed items

In **Paper V**, these steps were followed to develop new items for laziness. All criteria met or exceeded

the recommended values.

Structural equation modeling and instrument development refer to items that measured latent variables on a continuous scale. However, a variable may also be directly measured and may also be binary and not on a continuous scale, in which case logistic regression is used to evaluate the results (Peng et al. 2002).

4.2.3 Logistic regression

To analyze results when the independent variable is continuous and the dependent variable is binary, PLS-SEM is possible (Hair et al. 2017) but not recommended because of its nearity, normality and continuity (Peng et al. 2002). In such a case, logistic regression is more suitable. This calculation method shows how one or more continuous independent variables affect a binary dependent variable. The logistic regression calculates odds ratios, which display a value representing the probability that the dependent variable will change if the independent variable increases by one unit (Peng et al. 2002).

Several steps are taken to ensure the validity of the logistic regression. First, to determine the significance of the overall model, a χ^2 test is conducted. Then the significance of the relationship of the independent variable and the dependent variable is measured using the wald- χ^2 test and the corresponding level of significance. To ensure goodness-of-fit, Nagelkerke's R^2 (Nagelkerke 1991) is calculated (Peng et al. 2002). Furthermore, confidence-intervals can be evaluated to find out if the odd-ratios are significant, which is the case when the confidence interval does not cut 0 (Bewick et al. 2005). If all criteria are fulfilled, then the overall logistic regression model is valid, and the results are significant.

The actual odds ratios are displayed by the value $\text{Exp}(B)$ which is at least 0. If this value is 1, then the probability that the dependent variable will change is 0. If the value is smaller than 1, then the probability that the dependent variable will change is decreased by $|\text{Exp}(B) - 1|$. If $\text{Exp}(B)$ is larger than 1, then the probability that the dependent variable will change is increased by $\text{Exp}(B) - 1$ (Peng et al. 2002). For example, consider the probability that an individual will either use a software to protect her privacy, depending on her own assessment of privacy risks on a continuous scale. If $\text{Exp}(B)$ equals 1, then the probability that privacy risks will affect her usage of the software is zero. If $\text{Exp}(B)$ is 0.7, then the probability that she will use the software if privacy risks is increased by one unit, is decreased by 30 percent. If $\text{Exp}(B)$ is 1.6, then the probability that she will use the software, if privacy risks is increased by one unit, is increased by 60 percent.

Logistic regression was conducted in **Paper XI**. In this study, the dependent variable was whether or not individuals protected themselves against email tracking. The independent variable was their intention to protect themselves against email tracking. The behavior was measured via log files and was binary, whereas the intention was measured by a questionnaire with a 7-point Likert scale and was quasi-continuous. This indicates that logistic regression was a suitable analysis technique. The odds-ratios enabled calculation of the probability that individuals show actual protection behavior if their intention to do so changes by one unit.

The data analysis techniques discussed thus far aim to identify the relationships between concepts. A less sophisticated technique to analyze data is to simply find out if two concepts differ from each other using a t-test.

4.2.4 t-Test for independent samples

The t-test can be applied to investigate whether the mean values of two samples differ systematically from each other. This makes it possible to find out whether two groups show actual differences or whether this difference is based on chance. This, in turn, shows if the two populations from which the

samples were drawn are also different. A population here is the main unit of people who possess a certain characteristic. Since it is seldom possible to look at an entire population, samples representing a subset of a population are used (Adeyemi 2009; Rasch 2014).

The alternative hypothesis in studies is usually that the mean values of the populations differ. The null hypothesis in turn indicates that the means do not differ (see section 4.2.1.3 for further explanation of the alternative and the null hypothesis) (Hair et al. 2017). The t-test can now be applied to determine the likelihood that the null hypothesis is erroneously rejected, and the alternative hypothesis is accepted. This is done by examining the mean values of the samples. The t-test outputs a t-value for this purpose, which can be used to determine whether a difference in mean values is significant or not by relying on a t-table (see also significance of relationships in section 4.2.1.3) (Adeyemi 2009).

To perform a t-test, three conditions should be met: The characteristic under investigation should be interval-scaled, it should be normally distributed in the population and the variances of the populations from which the samples originate should be equal. While the t-test is somewhat robust to violations of these conditions, the samples must be larger than 30 and should be reasonably uniform in size. In addition, for an independent t-test, the values of one sample must not affect the values of the other sample. For a dependent t-test, the values are dependent on each other (Rasch 2014).

Several independent t-tests were conducted in **Paper VIII**. In four studies, the participants were divided into two groups and quantitative, interval-scale data was collected. The mean values of the data from two groups were then compared in each of the four studies, applying an independent t-test. The number of participants was fairly consistent across the groups and there were more than the recommended number of 30 participants. Since both groups were independent of each other, the t-test is the correct analysis technique here. To conduct t-tests, SPSS 25 was used.

4.2.5 Interview coding

The data analysis techniques presented above focus on quantitative approaches. One paper contained in this dissertation took a qualitative approach, using a case study as the research method to collect data via interviews. Once data is collected, it must be analyzed or coded (Corbin and Strauss 1990).

Following coding guidelines (Corbin and Strauss 1990) ensures that the interpreted results are valid and reliable. These coding guidelines are separated into open, axial and selective coding. First, in open coding, “*conceptually similar events/actions/interactions are grouped together to form categories and subcategories*” (Corbin and Strauss 1990, p. 12). This step compares events/actions/interactions with each other by evaluating similarities and differences. Categories and potentially subcategories are identified as dimensions of the focal category. This provides an overview of the topic and reveals broad patterns along particular dimensions among the data. For example, a researcher may identify privacy risks as a category in an interview and privacy risks to oneself or privacy risks to others as subcategories (Corbin and Strauss 1990).

Second, in axial coding, “*categories are related to their subcategories, and the relationships tested against data*” (Corbin and Strauss 1990, p. 13). This step refines and further develops the categories and subcategories identified in the open coding step, identifying relationships between the subcategories and the corresponding categories. The objective is to understand the conditions influencing the category, the category’s context or the category’s consequences. In the example above, the researcher might identify that privacy risks to oneself have a strong effect on subsequent behavior, whereas privacy risks to others have only a weak effect on subsequent behavior (Corbin and Strauss 1990).

Third, in selective coding, “*all categories are unified around a "core" category, and categories that need further explication are filled in with descriptive detail*” (Corbin and Strauss 1990, p. 14). Such a

core category is the main analytic idea running throughout the data or all action/interaction it is about. A core category can also explain differences between categories identified through axial coding. Core categories can either be based upon the categories identified or on a more abstract concept (Corbin and Strauss 1990). The core category in the example above may be privacy risks.

To increase reliability, it is advisable that multiple researchers conduct all three steps so that intercoder-reliability, i.e. how similarly different researchers code interview items, can be evaluated. When different conclusions are reached, the findings are discussed until agreement is reached on how to code an interview segment or a unit of analysis (Campbell et al. 2013).

One way to determine the units of analysis for the coding procedure is to select clear text units, such as words, sentences, paragraphs or pages. Another way is to apply “units of meaning” to code the content of the interview independent of the text units (Campbell et al. 2013). Using units of meaning is appropriate in more exploratory research (Garrison et al. 2006) because any portion of a text may be a unit of analysis, ranging from a single word in one part of the interview to segments from multiple, nonsequential paragraphs in another part of the interview (Campbell et al. 2013).

Coded interviews were analyzed in **Paper X**. In this case, open, axial and selective coding was conducted, following guidelines developed by Corbin and Straus (Corbin and Strauss 1990). To increase reliability, two researchers coded the data and differences were discussed until agreement was reached. Since the study was of exploratory nature, “units of meaning” were used as the units of analysis, which is in line with previous research (Campbell et al. 2013). The text was coded using the software MAXQDA 11.

4.3 SUMMARY

To summarize, in the papers comprising this dissertation, different methodologies with different data analysis techniques were applied. Most of the research was quantitative, using surveys as the research method and questionnaires as the data collection technique. In most of the papers, the data was analyzed using PLS-SEM, but several other data analysis techniques were also applied. Table 8 is used in the appendix to illustrate the combinations of methodology and data analysis applied in each paper.

By applying a certain methodology and a corresponding data analysis technique, results could be obtained for each of the 11 papers. These are presented next.

5 RESULTS

In this section, the results of each of the eleven papers of this dissertation are presented. After summarizing the main findings of the literature review, the remainder of the section follows the structure of the CPM. In the final subsection, a summary is given, where the results of the 11 papers in each element are combined.

5.1 PAPER I: DEPENDENT VARIABLES IN THE PRIVACY-RELATED FIELD: A DESCRIPTIVE LITERATURE REVIEW⁶

IS research into how individuals manage their privacy has focused on diverse issues. This descriptive literature reviews identifies the dependent variables used in this field to give an overview what has been discussed in the privacy-related field. Furthermore, it discusses the findings of previous studies to determine gaps in existing related research (Paré et al. 2015; Webster and Watson 2002). In addition to identifying dependent variables, this survey of the 142 articles considered most current and relevant

⁶ Wirth, J. 2018. “Dependent Variables in the Privacy-Related Field: A Descriptive Literature Review,” in *Proceedings of the 51st Hawaii International Conference on System Sciences*, T. Bui (ed.), Waikoloa Village, Hawaii

allows to make five additional overall observations. For this introductory paper, the literature review has also been updated to also cover more recent findings, including 40 additional articles such that in sum, 182 articles were analyzed⁷. The key results have not changed:

First, from 2006 on there is a steady increase in studies focusing on SNS. In comparison, research in other research settings, such as healthcare or location-based settings, decreased over the same period. *Second*, the dependent variables can be categorized as either behavior-related or psychology-related. Intention to disclose is the most commonly used behavior-related dependent variable, followed by actual disclosure behavior, which includes observations of actual behavior as well as self-reported past behavior in SNS settings. However, psychology-related dependent variables have also been used, the most common of which are privacy concerns and willingness to pay / willingness to sell. *Third*, the privacy calculus is the most commonly used theory to explain disclosure of information and the protection motivation theory is most commonly used to explain the protection of privacy. However, other theories, such as the CPM, have also been used in IS-related privacy research. *Fourth*, surveys are the most used research methods. Experiments have only been used half as frequently as surveys. The majority of research studies are cross-sectional, considering only one point of time, rather than longitudinal. *Fifth*, research into actual disclosure behavior has inconsistent results. For example, three studies show a non-significant effect of privacy concerns on actual disclosure behavior, whereas four other studies show a significant negative effect. This corresponds to a non-resolved privacy paradox.

The literature review contributes in the following significant ways. First, although intention is often the best predictor of actual behavior, it does not always result in that particular behavior. As a result, many scholars recommend focusing on actual behavior as well. Second, the privacy paradox remains unresolved, which confirms previous research studies (Kokolakis 2017) and underscores the need to understand this phenomenon. Third, to uncover new possibilities and research avenues, it is recommended to expand beyond commonly used dependent variables and research settings to include other equally revealing dependent variables and research settings.

In summary, **Paper I** presents the findings of a literature review on privacy in the domain of IS, pointing to the benefits of studying actual behavior, the need to better understand the privacy paradox, and the value of including dependent variables beyond disclosure.

5.2 PRIVACY OWNERSHIP

Paper II and **Paper III** attempt to answer the research question to what degree privacy ownership has changed in the digital age.

5.2.1 Paper II: Justification of mass surveillance: a quantitative study⁸

Mass surveillance results in reduced privacy which can have disadvantages such as a loss of freedom of opinion and behavior (Karwatzki et al. 2017; Penney 2016). Despite these potential disadvantages, more individuals accept mass surveillance than reject it (PeWResearchCenter 2013; Reddick et al. 2015). It is important for both governmental agencies, who benefit from continuing mass surveillance (McAskill 2015), and individuals, who suffer the loss of privacy due to mass surveillance (Siner 2014), to understand the factors that drive individual justification of mass surveillance.

The research model is based largely on the system justification theory (SJT), which posits that

⁷ For this introductory paper, the literature review has been extended to also cover more recent findings, including 40 additional articles. These findings do not change the key results. A more detailed analysis is given in the appendix (section 8.1).

⁸ Wirth, J., Maier, C., and Laumer, S. 2019. "Justification of Mass Surveillance: A Quantitative Study," in *Proceedings of the 14th International Conference on Wirtschaftsinformatik*, T. Ludwig and V. Pipek (eds.), Siegen, Germany.

individuals justify, i.e. defend, warrant and bolster, an existing system based on, among others, the perceived need for order and stability and the perceived dangerousness of the world (Jost et al. 2004; Jost and Hunyady 2005; van der Toorn et al. 2015). Moreover, the SJT assumes that individuals whose lack of access to sufficient resources makes them powerless are more likely to justify the system causing their powerlessness, principally because doing so helps them maintain a positive image about their situation.

Based on a comprehensive literature review through which gaps in research applying the SJT in the mass surveillance context were identified, the research model also considers privacy-related concepts such as perceived security, which might be increased by mass surveillance (Dinev et al. 2008), or individuals' notion that they have nothing to hide from others (Solove 2007, 2011). In this research context, powerlessness is conceptualized as a loss of privacy control because mass surveillance reduces the power one has over one's own privacy.

To test the research model, a quantitative research approach with a survey as the research method has been conducted and evaluated the results following a PLS-SEM approach. The results reveal that the research model explains 56.6 percent of the variance of justification of mass surveillance and that the effect of privacy control on justification is not significant. The results support all other remaining hypotheses (see Figure 8). It is concluded that the justification of mass surveillance is driven significantly by the perceived need for order and stability, perceived dangerousness of the world, perceived security as well as the concept of having "nothing to hide".

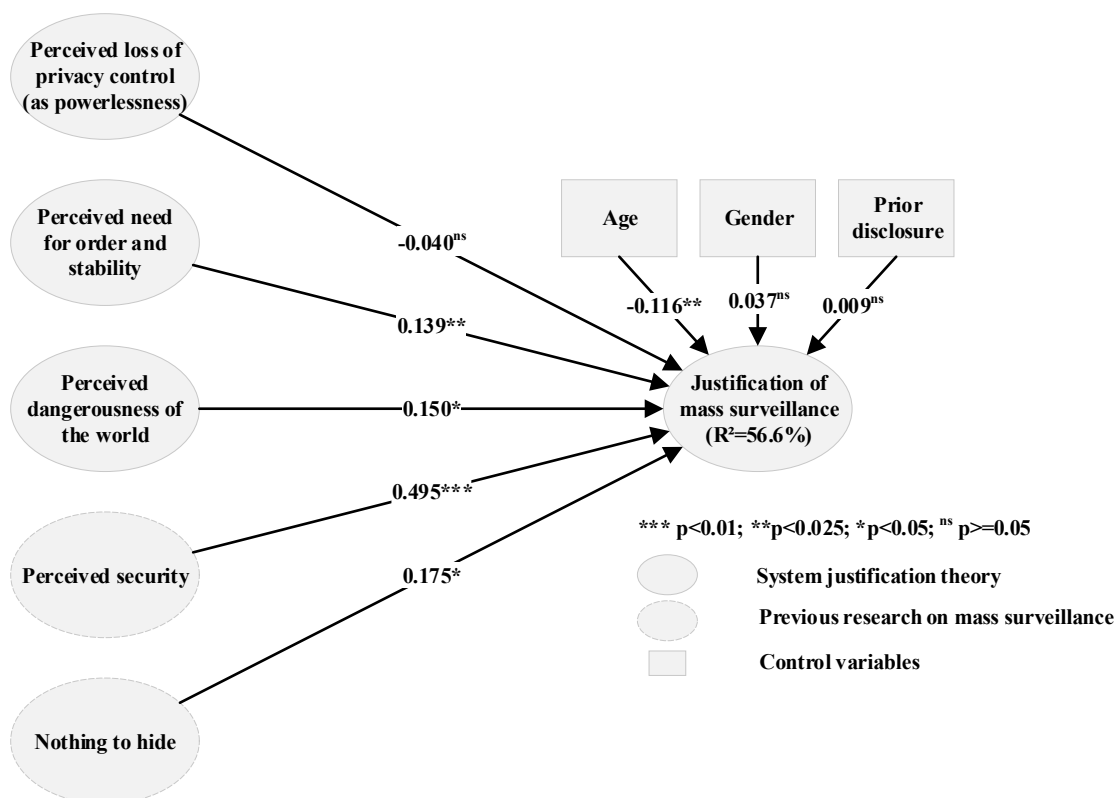


Figure 8. Results of Paper II

The results of **Paper II** implicate that mass surveillance is a system in the sense of the SJT. Scholars researching the justification of mass surveillance can therefore also rely on SJT in their future research studies. This makes the SJT, which has usually been applied in political science (Jost et al. 2004), available in the IS domain. Furthermore, not all individuals consider mass surveillance purely negative, as has been largely assumed by previous research (Solove 2007). This study also finds that loss of

privacy has no impact on the justification of mass surveillance. In other words, individuals are not particularly worried about the loss of privacy resulting from mass surveillance. Moreover, many individuals think that mass surveillance can help increase their security and make the world less dangerous. This has research design implications for scholars tempted to consider mass surveillance only from a negative perspective.

In summary, **Paper II** investigates why individuals justify mass surveillance. To fill a research gap identified in a literature review, it is drawn on the SJT as a basis for a research model complemented by additional concepts from privacy research. The research model is tested by applying a PLS-SEM approach. The results show that the justification of mass surveillance is mainly determined by perceived security and privacy control has no effect on the justification of mass surveillance. These findings imply that mass surveillance is not considered as purely negative by individuals and that the SJT is suitable to be applied in IS research.

5.2.2 Paper III: The influence of resignation on the privacy calculus in the context of social networking sites: an empirical analysis⁹

Resignation is a reaction to events such as threats in which individuals accept the threat and take no actions to change it (Feifel and Strack 1989). Previous research indicates that resignation could alter the effect of benefits and privacy risks on disclosure (Acquisti 2004; Guo and Yu 2020; Hoffmann et al. 2016; Spiekermann et al. 2001). **Paper III** investigates the implications for the privacy calculus caused by resignation, i.e. of individuals' giving up on protecting their privacy.

To research on this issue, a research model has been developed based on the privacy calculus, including resignation as a moderator of both the effects of benefits and privacy risks on disclosure. A literature review has been conducted, which shows that resignation has not yet been considered as such a moderator by previous privacy research. The research model hypothesizes that if individuals have resigned in protecting their privacy, the effects of benefits on disclosure will be strengthened and the effects of privacy risks on disclosure will be weakened.

To test the research model, a quantitative research approach has been conducted with a survey as the research method. The results were evaluated by a PLS-SEM approach. The results show that resignation moderates the effects of both benefits and privacy risks on disclosure. Specifically, the effect of benefits on disclosure is strengthened by resignation and the effect of privacy risks on disclosure is weakened by resignation (see Figure 9).

These results help explain why individuals sometimes disclose information even though the benefits are low and the privacy risks are high (Acquisti 2004): Resignation of individuals leads to a stronger effects of the benefits and to a weaker effects of the privacy risks. Scholars applying the privacy calculus (Dinev and Hart 2006) need to consider the level of resignation. The higher the level of resignation among participants, the less the privacy calculus appears to be applicable. This study also contextualizes resignation as a common reaction of individuals in the privacy domain (Hoffmann et al. 2016), making the concept useful to scholars in the privacy domain.

⁹ Wirth, J., Maier, C., and Laumer, S. 2018. "The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: an Empirical Analysis," in *Proceedings of the 26th European Conference on Information Systems*, P. Bednar, U. Frank and K. Kautz (eds.), Portsmouth, UK.; A previous version has been presented and discussed at the 12th Pre-ICIS Workshop on Information Security and Privacy in Seoul, South Korea: Wirth and Maier (2017).

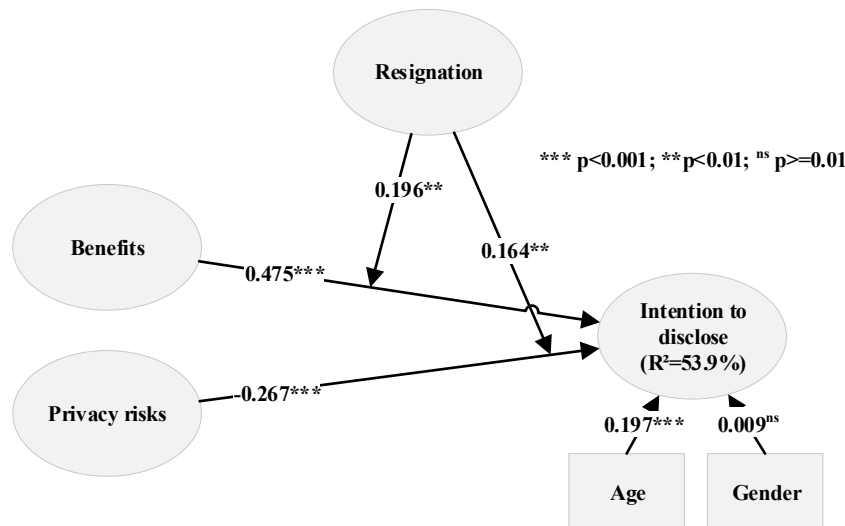


Figure 9. Results of Paper III

In summary, **Paper III** presents the result of a quantitative study of the effect of resignation on the privacy calculus. The research model builds on the privacy calculus and includes resignation as a moderator. The results support the hypotheses, suggesting a significant moderating effect of resignation on the influence of both benefits and privacy risks on disclosure. The results implicate that, in the privacy domain, resignation helps explain why individuals sometimes disclose information even though the benefits are low, and the privacy risks are high.

5.3 PRIVACY CONTROL

The privacy control element of the CPM describes how an individual decides to either disclose or to conceal personal information. The associated research question asked by this dissertation is what determines individuals' control of their own and others' privacy. The six papers that aim to answer this research question are **Papers IV, V, VI, VII, VIII and IX**.

5.3.1 Paper IV: Subjective norm and the privacy calculus: explaining self-disclosure on social networking sites¹⁰

Paper IV provides an additional explanation for why individuals may disclose information despite low benefits and high privacy risks. For example, it was shown that individuals are more likely to pay to protect their privacy when others who are important to them expect them to do so (Schreiner and Hess 2015). This so-called subjective norm has been shown to generally influence decisions of individuals (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975). The effect of subjective norms has already been indicated in the privacy domain (Heirman et al. 2013). **Paper IV** investigates the effect of subjective norm on the privacy calculus.

Based on the theory of reasoned action (TRA) (Fishbein and Ajzen 1975, 2010) and the privacy calculus (Dinev and Hart 2006), an extended research model has been created with benefits, privacy risks and subjective norm, determining disclosure. A literature review shows that subjective norm has already been part of previous privacy research but has not been included in the privacy calculus. A research model is thus developed. Here, it is hypothesized that subjective norm has a positive effect on disclosure. In other words, individuals are more likely to disclose if they think that others who are important to them expect them to do so and because they think the expected behavior is viewed as

¹⁰ Wirth, J., Maier, C., and Laumer, S. 2019. "Subjective Norm and the Privacy Calculus: Explaining Self-Disclosure on Social Networking Sites," in *Proceedings of the 27th European Conference on Information Systems*, P. Johannesson, P. Ågerfalk and R. Helms (eds.), Stockholm & Uppsala, Sweden.

appropriate by other important referents (Triandis 1980). The individuals also hope to be considered more favourably by important referents (Moore and Benbasat 1991).

To investigate the research model, a quantitative research approach with a survey as the research method has been conducted. The results were evaluated by a CB-SEM approach. The results show that 18.6 percent of the dependent variable could be explained. Furthermore, by calculating f^2 values, it was shown that subjective norm has the strongest effect on disclosure (0.11), followed by benefits (0.07) and privacy risks (0.00).

The results implicate that subjective norm can outweigh the effects of benefits and privacy risks. Hence, generally, the basic premises of the privacy calculus could be overridden by subjective norm. When applying the privacy calculus (Dinev and Hart 2006) scholars should thus consider the level of subjective norm and calculate for its effects. Participants with high levels of subjective norm will be more driven by that level of subjective norm than by benefits and privacy risks. More generally, the results implicate that other concepts may override the effect of the privacy calculus on disclosure. Although the privacy calculus is the main dominant theory in privacy research (Smith et al. 2011), these results implicate that there are also other concepts that may better explain disclosure.

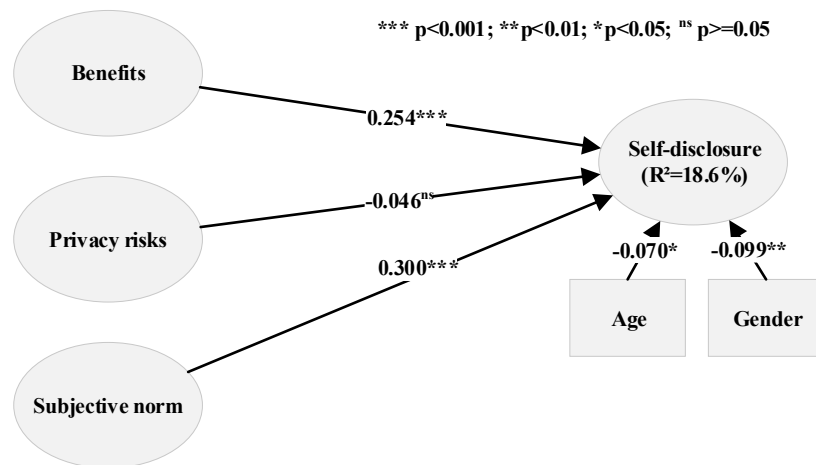


Figure 10. Results of Paper IV

In summary, subjective norm is included into the privacy calculus to better explain disclosure of information. The results show that subjective norm has a stronger effect on disclosure than benefits or privacy risks. This implicates that subjective norm should be considered when performing research using the privacy calculus.

5.3.2 Paper V: Laziness as an explanation for the privacy paradox: An empirical investigation with multiple snapshots¹¹

In privacy research, there is a so-called privacy paradox that individuals disclose information even though they are highly concerned about their privacy. Scholars have called for more research into the role of personality traits in the privacy paradox to better understand this paradox (Bélanger and Crossler, 2011). One such personality trait is laziness (Abramson et al. 1978; Watkins et al. 2009), which has been mentioned as potentially important in the privacy domain (Kwong 2015; Spencer 2014).

To test the effect of laziness on the privacy paradox, a research model has been developed, integrating laziness with privacy concerns and disclosure from the privacy paradox (Kokolakis 2017). Furthermore,

¹¹ Wirth, J., Maier, C., Laumer, S., and Weitzel, T. "Laziness as an explanation for the privacy paradox: An empirical investigation with multiple snapshots", submitted to Internet Research, 2nd round; A prior version has been presented and discussed at the 20th DIGIT Workshop, Fort Worth, TX, USA: Wirth et al. (2015).

privacy risk is included as it is one of the most salient beliefs in privacy related research (Malhotra et al. 2004). To avoid confusion between disclosure intention and disclosure behavior (Smith et al. 2011), this research model uses actual retrospective self-disclosure behavior of the individuals. Also, a literature review has been conducted, showing that laziness has not been included in privacy research before.

To evaluate the research model, a quantitative approach with survey as the research method has been conducted. The results are evaluated by PLS-SEM. Furthermore, since the construct of laziness does not exist in privacy research, it was conceptualized and operationalized.

The results (see Figure 11) show that the explained variance of self-disclosure without the moderator is 19.6 percent, and 21.6 percent including the moderating effect. A multi-group analysis was carried out, to better understand the moderating effect of laziness. Groups were divided into “high lazy” and “low lazy” individuals. The results show that the influence of privacy concerns on self-disclosure is non-significant when individuals are “high lazy”. However, among “low lazy” individuals, the influence of privacy concerns on self-disclosure becomes negative and significant. These results support the hypothesis regarding the moderating effect of laziness. Hence, laziness influences the privacy paradox in that the privacy paradox exists when individuals are “high lazy” and does not exist when individuals are “low lazy”.

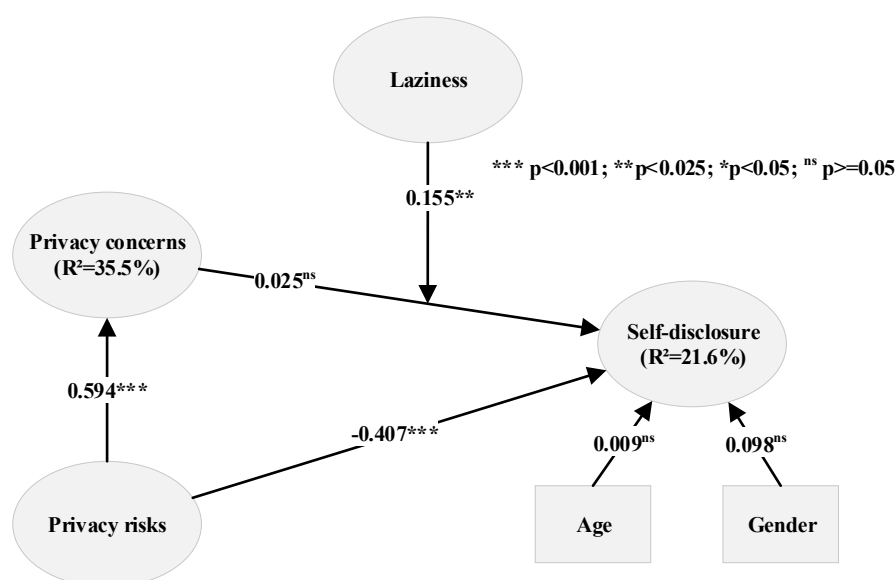


Figure 11. Results of Paper V

The results of **Paper V** contribute to the literature by showing that the personality trait laziness can help in better understanding the privacy paradox. Scholars, who have relied on the privacy calculus as the main explanation of the privacy paradox (Dinev and Hart 2006; Smith et al. 2011) should also take into account the level of laziness. If participants are “high lazy” the privacy paradox will be more likely to occur than if individuals are less lazy. Furthermore, laziness is conceptualized, defined and operationalized to make it useful in further studies.

In summary, **Paper V** researches on the effect of laziness on the privacy paradox. After conceptualizing and operationalizing laziness, the results show that if individuals are “high lazy” the privacy paradox applies more than if individuals are “low lazy”. This deepens the understanding of the privacy paradox.

5.3.3 Paper VI: Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples¹²

Recent studies show that technostress decreases well-being and individual performance (Maier et al. 2015), underlying the importance of understanding the factors that lead individuals to perceive technostress. Building on research theorizing personality as a factor influencing technostress (Ayyagari et al. 2011), this study considers the role of three hierarchical levels of personality (Thatcher et al. 2018): 1) broad traits, 2) stable, context-specific traits and 3) dynamic, context-specific traits.

A literature review identifies relevant research gaps and guided the choice of salient personality traits from the three hierarchical levels of personality for the research model: neuroticism, personal innovativeness in IT (PIIT) and IT mindfulness. Especially the dynamic, context-specific trait IT mindfulness has received increasing recent research attention (Thatcher et al. 2018), including a focus on the relationship between mindfulness and the level of the stress hormone cortisol (Brown et al. 2012; Brown and Ryan 2003; Shapiro et al. 2011). The research model hypothesizes that techno-stressors are influenced by all three personality traits, with IT mindfulness having the highest explanatory power.

To evaluate the research model, a quantitative approach with survey as the research method has been conducted. Data of the survey was collected by two different samples via two different points of time and was tested by conducting a PLS-SEM approach. The results confirm that all three personality traits influence the perception of technostress and that IT mindfulness has the strongest impact (see Figure 12).

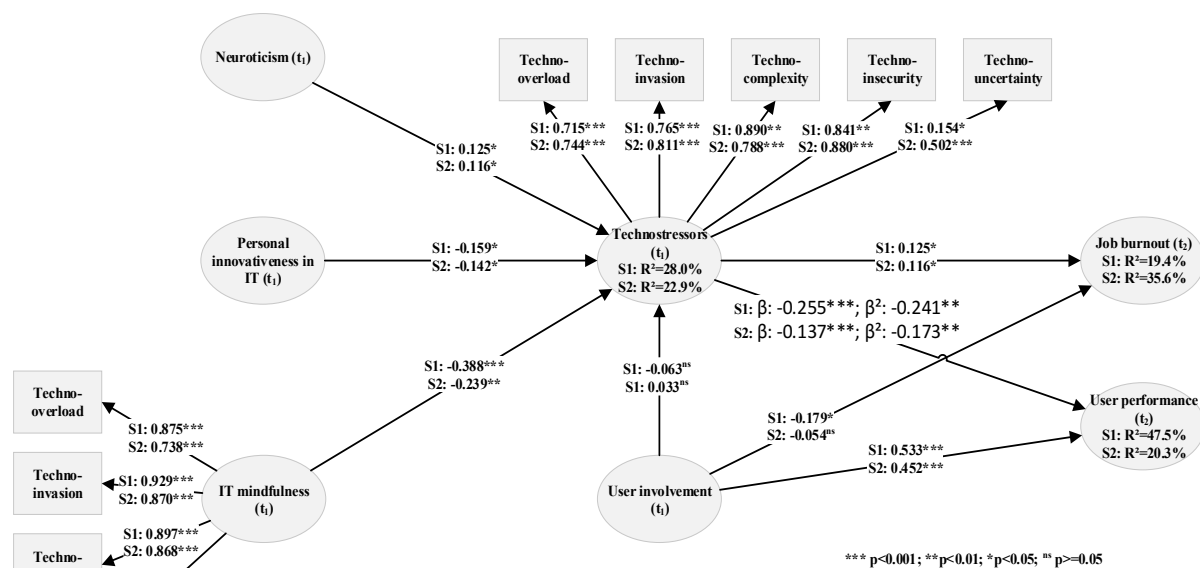


Figure 12. Results of Paper VI

Note: Rectangles are dimensions, ellipse are constructs; S1 means sample 1 and S2 means sample 2; Neuroticism, PIIT, IT mindfulness, techno-stressors and user involvement are collected in survey 1 (indicated by t1), job burnout and user performance are collected in survey 2 (indicated by t2)

The main contribution of this study with respect to general IS research is that the dynamic, IS-specific

¹² Maier, C., Laumer, S., Wirth, J., and Weitzel, T. 2019. "Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples," *European Journal of Information Systems* (28:5), pp. 496–522. A prior version has been presented and discussed at the 38th International Conference on Information Systems in Seoul, South Korea: Maier et al. (2017).

trait IT mindfulness has the strongest influence on techno-stressors. These results underscore the influence of narrow and dynamic traits on beliefs and behaviors related to IS research in general. This finding complements previous research in the area of psychology, suggesting that the explanatory power of broad traits can be increased by focusing on more narrow traits (Paunonen and Ashton 2001).

In summary, this research focuses on the effect of three different kinds of personality traits, with a focus on IT mindfulness as a dynamic, context-specific trait. The results show that IT mindfulness has the strongest explanatory power on perception of technostressors. This implicates that research should rather focus on such dynamic, context-specific traits rather than on broad traits.

5.3.4 Paper VII: The effect of mindfulness on threat appraisal and coping appraisal: an empirical analysis¹³

Research in the field of IS suggests that individual's motivation to protect their privacy is generally governed by privacy motivation theory, which asserts that their motivation depends on their appraisal of the privacy threat and their appraisal of their ability to cope with it (Rogers and Prentice-Dunn 1997). If the individual expects the privacy threat to cause severe harm or expenses, the motivation to protect against that privacy threat is greater than if she expects the privacy threat to cause only minor damages. Furthermore, if the individual considers herself to have the necessary capabilities to protect against the threat she will be more likely to do so (Mousavizadeh and Kim 2015; Rogers and Prentice-Dunn 1997). Thus, determining what leads to certain appraisals is instrumental in understanding why individuals are sometimes more and sometimes less motivated to protect their privacy. It should be noted that extant privacy-related research focuses mainly on appraisal outcomes and not on what leads to certain appraisals (Anderson and Agarwal 2010; Boss et al. 2015; Chen and Zahedi 2016). Research in the field of psychology suggests that individual mindfulness directly influences certain types of appraisal (Epel et al. 2009; Garland et al. 2011; Weinstein et al. 2009). This research study considers mindfulness as an antecedent of threat appraisal and coping appraisal in the domain of privacy.

A conducted literature review reveals that mindfulness has not yet been considered by privacy research. In this study, it is built on the protection motivation theory and extended by including mindfulness, adapted to the particular context (Thatcher et al. 2018). Specifically, both mindfulness in terms of threat appraisal and mindfulness in terms of coping appraisal is considered. It is then hypothesized that when an individual is mindful of both, she is more likely to consider and recognize threats to her privacy and to consider and recognize actions that will protect her from the threat. To test these hypotheses, a research model combining the protection motivation theory, mindfulness on threat appraisal and mindfulness on coping appraisal is created.

To evaluate the research model, a quantitative research approach with PLS-SEM has been followed, using a survey as the research method. In line with protection motivation theory, test subjects were exposed to a high fear appeal (Boss et al. 2015) and email tracking was the underlying context (Xu et al. 2018). The fear appeal was a frightening message detailing the dangers of email tracking and describing how to protect against those dangers.

The results show that mindfulness on threat appraisal has a positive effect on threat appraisal, and mindfulness on coping appraisal has a positive effect on coping appraisal. Most of the anticipated hypotheses are supported (see Figure 13).

This finding contributes by showing that both threat appraisal and coping appraisal can be partly

¹³ Wirth, J., Maier, C., Laumer, S., and Weitzel, T. "The effect of Mindfulness on Threat Appraisal and Coping Appraisal: An Empirical Analysis", manuscript in preparation for submission; A prior version has been presented and discussed at the the 38th International Conference on Information Systems in Seoul, South Korea: Wirth et al. (2017).

explained by the level of mindfulness. Scholars researching the PMT, including threat appraisal and coping appraisal, should thus also consider the individuals' level of mindfulness. Different levels of mindfulness might help explain different levels of threat appraisal and coping appraisal among the participants. Furthermore, mindfulness supports the fear appeal, which triggers the threat appraisal and the coping appraisal, among other effects. Hence, if scholars aim to increase the level of threat appraisal and coping appraisal among their participants, they should select individuals who are mindful of both.

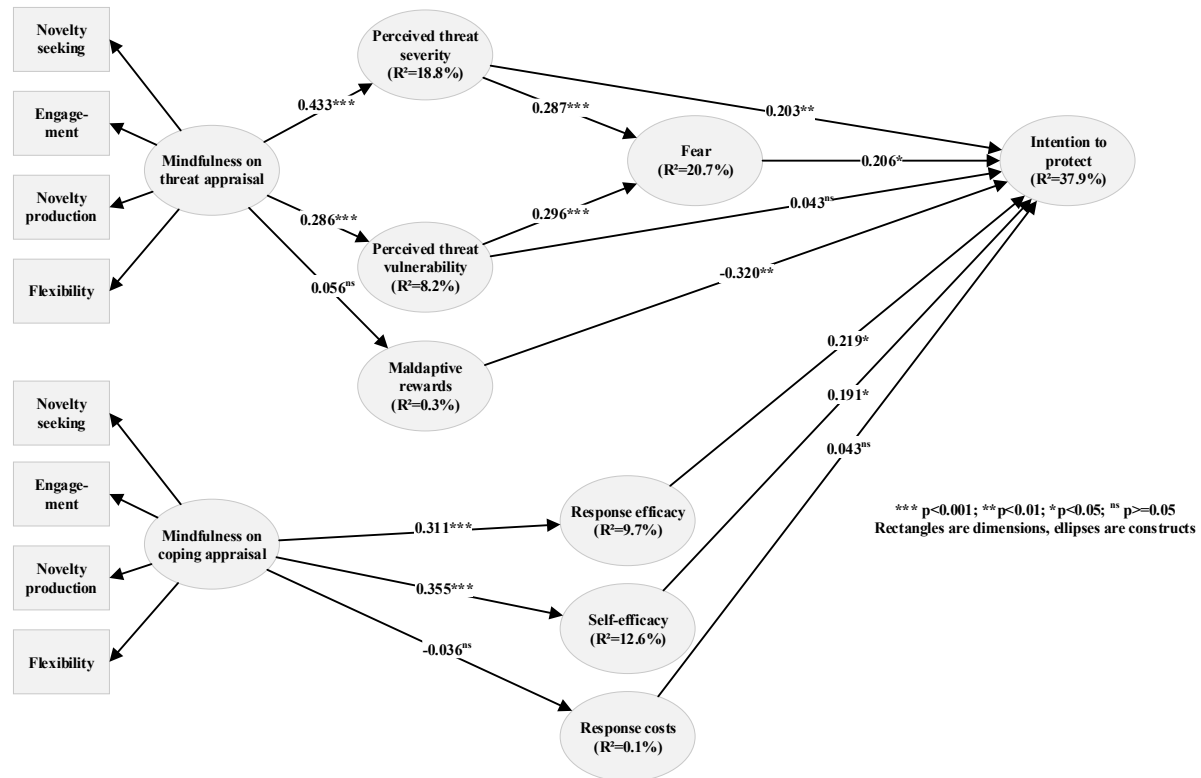


Figure 13. Results of Paper VII

In summary, this research contextualizes mindfulness to the domain of the protection motivation theory in the context of privacy. The results support most of the hypotheses, indicating a positive effect of mindfulness on threat appraisal and on coping appraisal. Its contributions include that scholars should consider the level of mindfulness when applying the protection motivation theory.

5.3.5 Paper VIII: Anchoring influences actual disclosure: four studies on the amount and accuracy of information disclosure¹⁴

One way that individuals can control their privacy is to alter the *amount* and *accuracy* of the information they disclose (Posey et al. 2010; Son and Kim 2008). Despite extensive previous research assuming that individuals invest high effort into privacy control, there is also evidence that individuals often invest little effort into that decision (Dinev et al. 2015). It has then been shown that factors related to behavioral economics, such as cognitive biases, can distort decision-making (Ariely 2010; Bodenhausen et al. 2001; Cialdini 2010; Kahneman et al. 1982; Tversky and Kahneman 1974). One such cognitive bias is the anchoring-effect, which potentially influences all decisions (Furnham and Boo 2011; Kahneman et al. 1982). According to the anchoring-effect, individuals are unable to dismiss some type of information when making decisions (Tversky and Kahneman 1974). **Paper VIII** investigates

¹⁴ Wirth, J., Maier, C., Laumer, S., and Weitzel, T. "Anchoring Influences Actual Disclosure: Four Studies on the Amount and Accuracy of Information Disclosure", manuscript in preparation for submission

how the anchoring-effect influences both the amount as well as the accuracy of disclosure (Acquisti et al. 2017; Mussweiler and Strack 1999; Tversky and Kahneman 1974).

Two literature reviews were conducted, revealing gaps in research on the amount and accuracy of disclosure as well as the inclusion of the anchoring-effect in privacy research in general. To fill these research gaps, four studies have been conducted: Study 1 and study 2 focus on the amount of actual disclosure and study 3 and study 4 on the accuracy of actual disclosure. For example, study 1 uses the size of a textbox as an anchor, hypothesizing that individuals confronted with a large textbox will disclose more words than individuals confronted with a small textbox. Study 3 examines the accuracy of information disclosed when the individual is not sure about the correctness of information. In this case, individuals were asked how many online-accounts they have, which is something an individual might not be fully sure of. Individuals were also asked for the last two digits of their cellphone number, which serve as the anchor. It is then hypothesized that the accuracy of disclosed information the individual is uncertain about is influenced by this anchor.

To evaluate the four studies and the hypotheses, a quantitative research using an online survey experiment has been conducted and tested with t-tests. The results show that the anchoring-effect influences the amount and, partly, the accuracy of information. Specifically, when individuals are influenced by an anchor, they are likely to disclose more information or less information, depending on the anchor. In addition, the information they disclose is likely less accurate, depending on the anchor.

The results implicate that cognitive biases need to be taken into account when doing research on privacy. This supplements the call of Dinev et al. (2015) to conduct more research on cognitive biases in the privacy domain. Furthermore, when doing research on the amount of actual disclosure, the anchoring-effect needs to be considered. This research contributes by showing that factors other than e.g. only the privacy calculus (Dinev and Hart 2006), such as the anchoring-effect, need to be considered to better understand the control of privacy. In addition, the accuracy of disclosed information is influenced by the anchoring-effect. Specifically, when individuals provide inaccurate information (Wheless and Grotz 1976) without knowing it is incorrect, they can be influenced by the anchoring-effect. Future studies on the accuracy of disclosed information should thus consider the potential influence of an anchor.

In summary, this research study builds on the fact that individuals often only put low effort into their decisions and are thus prone to cognitive biases such as the anchoring-effect. The results show that also when individuals disclose information, they are influenced by anchors. These results implicate that scholars should take into account cognitive biases and specifically the anchoring-effect in privacy studies.

5.3.6 Paper IX: Perceived information sensitivity and interdependent privacy protection: a quantitative study¹⁵

It has been shown that information sensitivity plays a major role when individuals disclose information about themselves (Mothersbaugh et al. 2011). Previous research has mainly considered negative consequences for the original owner. However, based on the CPM (Petronio 2013), privacy control is also about co-owners. In this study, the concept of information sensitivity is extended to understand the degree to which co-owners consider the sensitivity of information in terms of negative consequences for themselves and for the original owner when handling information of original owners.

A literature review has been conducted that shows that information sensitivity has not been well

¹⁵ Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2019. "Perceived information sensitivity and interdependent privacy protection: a quantitative study," *electronic markets* (29:3), pp. 359–378

defined and lacks the perspective of the co-owner. To fill this gap, this study reconceptualizes and redefines information sensitivity to account for the original owner and the co-owner. It is now called “perceived information sensitivity” and is defined as “*an individual’s assessment of information belonging to him/herself or any other individual based on perceived negative consequences for him/herself or any other individual due to the loss of an individual’s privacy with regard to the information*”.

To research this concept of perceived information sensitivity, a research model has been developed. It includes with two perspectives: the perspective of the co-owner considering negative outcomes of disclosure for herself (“perceived information sensitivity for the co-owner”), and the perspective of the original owner considering negative outcomes for the original owner (“perceived information sensitivity for the original owner”). The research model also includes perceived enjoyment as a benefit for the co-owner, as well as motivation to comply, which is the incentive the co-owner feels to follow the requests of the original owner (Ajzen 2006; Fishbein and Ajzen 1975). The dependent variable is the intention of the co-owner to protect the privacy of the original owner. It is then hypothesized that both concepts of perceived information sensitivity negatively influence the dependent variable, that perceived enjoyment will also have a negative effect and that motivation to comply will have a positive effect. Furthermore, two moderating effects are included, hypothesizing that the effect of perceived information sensitivity for the co-owner on the dependent variable will be negatively moderated and the effect of perceived enjoyment will be positively moderated. To test the research model, a quantitative approach with a survey as the research method has been conducted. The results are evaluated by a PLS-SEM approach.

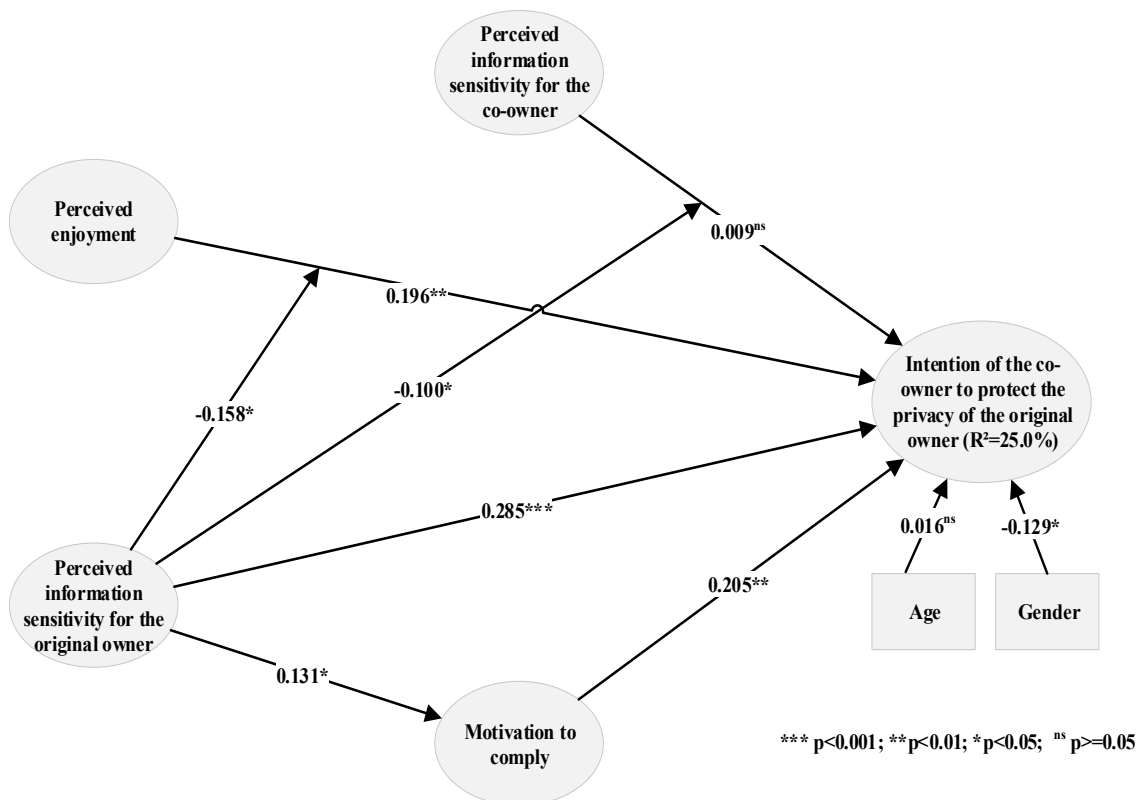


Figure 14. Results of Paper IX

The results support most of the hypotheses (see Figure 14). Overall, the dependent variable is explained by 25.0 percent. The effect of perceived information sensitivity for the co-owner on the dependent variable is non-significant. However, that non-significant effect is explained and significantly moderated by perceived information sensitivity for the original owner.

The main contribution of this study is that it extends perceived information sensitivity, laying the groundwork for future research to define it clearly. This study also reveals the concealment of information as a privacy-protection mechanism. The dependent variable has been measured by asking if co-owners refrained from disclosing, i.e. whether they concealed personal information of the original owners. Previous research ignored this possible dependent variable, focusing instead primarily on original owners protecting their own privacy (Son and Kim 2008).

In summary, this study redefines and extends perceived information sensitivity to account for the perspective of the co-owner. The results show that this extended concept better explains the intention of the co-owner to protect the privacy of the original owner. These results implicate that information sensitivity needs to be extended and should be more clearly defined by future research.

5.4 PRIVACY TURBULENCE

Privacy turbulence occurs when co-owners have unauthorized access to information. In response, original owners may restore the collective boundaries to remove co-owners with that unauthorized access (Petronio and Altman 2002). This study investigates how privacy turbulence is handled by individuals in the digital age. Two papers aim to answer that research question (**Paper X** and **Paper XI**).

5.4.1 Paper X: Strength of ties as an antecedent of privacy concerns: a qualitative research study¹⁶

Previous research indicates that individuals' concern about their privacy varies, depending on who might gain unauthorized access to their personal information. In particular, in how far the level of concern varies depends on the relationship between the original owner and the co-owner. Research indicates that relationships can be described in terms of the strength of tie between people (strong, weak or absent tie) (Granovetter 1973; Xu et al. 2011a). This study researches the degree to which original owners' strength of tie with the unauthorized co-owner affects the level of concern of original owners about their privacy.

Since this research study is exploratory, it lacks a research model. Rather, a qualitative research approach has been undertaken with a case study research method, applying the theory of strength of ties (Granovetter 1973) to the privacy setting. The objective of the study was to better understand how strength of tie between original owners and unauthorized co-owners affects the original owners' level of privacy concerns. To execute the case study, interviews have been conducted. The interviews were evaluated by open, selective and axial coding (Corbin and Strauss 1990). The results indicate that weak ties are associated with greater privacy concerns, whereas strong and absent ties are only associated with privacy concerns under certain circumstances, such as when the information is sensitive and when individuals are generally concerned about their privacy.

The main contribution of this study is that the strength of tie is closely associated with the level of privacy concerns. Since privacy concerns are of great interest in privacy research, this study contributes to previous research (Smith et al. 2011) by pointing to strength of ties as a likely antecedent of privacy concerns. This confirms and extends previous research which states that privacy concerns is dependent on the audience (Stanton and Stam 2002) or an external agent (Xu et al. 2011a). Hence, scholars considering privacy concerns should take the overall setting into account by considering the relationship between the original owner and the potential co-owner gaining unauthorized access to the personal information of the original owner. The results indicate that the strength of ties between the two

¹⁶ Wirth, J. 2017. "Strength of Ties as an Antecedent of Privacy Concerns: A Qualitative Research Study," in *Proceedings of the 23rd Americas Conference on Information Systems*, D. Strong and J. Gogan (eds.), Boston, MA, USA.

individuals or entities will influence the level of privacy concerns of the original owner. This information will also facilitate reproducibility and the ability to compare multiple studies.

5.4.2 Paper XI: Drivers of email tracking privacy protection behavior: a two-wave quantitative study¹⁷

Email tracking violates individual privacy (Englehardt et al. 2018) and is prevalent: 99 percent of newsletters use tracking technology (Brunet 2017) and about every fifth conversational email is tracked (Merchant 2017). By tracking an email, the sender can collect information about whether, when and where an email has been opened (Bender et al. 2016; Brunet 2017; Fabian et al. 2015; Merchant 2017). Despite this invasion of their privacy, studies indicate that most individuals do not protect themselves against email tracking (Xu et al. 2018). This study aims to identify what factors influence email tracking protection behavior. To do so, it applies the protection motivation theory, which suggests that appealing to individuals' fear motivates them to protect themselves against email tracking. A fear appeal is a message intended to increase individuals' fear of a threat while also providing information on how to protect against the threat.

Based on the protection motivation theory, a research model has been built (Rogers and Prentice-Dunn 1997). After having conducted a literature review, the literature review reveals that the protection motivation theory has not been used fully or correctly in the privacy domain because concepts or relationships have been omitted, added or changed. In line with previous research (Aurigemma and Mattson 2019) the protection motivation theory is contextualized to the context of email tracking and the full nomology of the protection motivation theory is applied (Boss et al. 2015). A high and a low fear appeal were included. The high fear appeal included a severe warning regarding email tracking and also clear instructions on how to protect against it. The low fear appeal only indicated that tracking in general may be dangerous and only superficially described how to protect against it.

To evaluate the research model quantitatively, a PLS-SEM approach was used whereas the research method was an online survey experiment. To better understand the behavior, an online field experiment was also conducted to assess actual email tracking behavior among study participants by analyzing log-files. These findings were included in the research model by applying logistic regression.

The results are evaluated twice: Once for participants with the high fear appeal treatment and once for participants with the low fear appeal treatment. The results show that most of the hypotheses are supported. In particular, the relationships between the threat appraisal, coping appraisal and behavior process are more often significant in the hypothesized direction in the high fear appeal domain than in the low fear appeal domain. Regarding the effect of intention on behavior, a non-significant effect was found for individuals with a high fear appeal and the effect became significant for participants with a low fear appeal. The results indicate that behavior is influenced by the fear appeal in general because participants of the study more actively protected themselves against email tracking after being confronted with either a low or high fear appeal (see Figure 15).

¹⁷ Wirth, J., Maier, C., Laumer, S., and Weitzel, T. "Drivers of Email Tracking Privacy Protection Behavior: A Two-Wave Quantitative Study", manuscript in preparation for submission

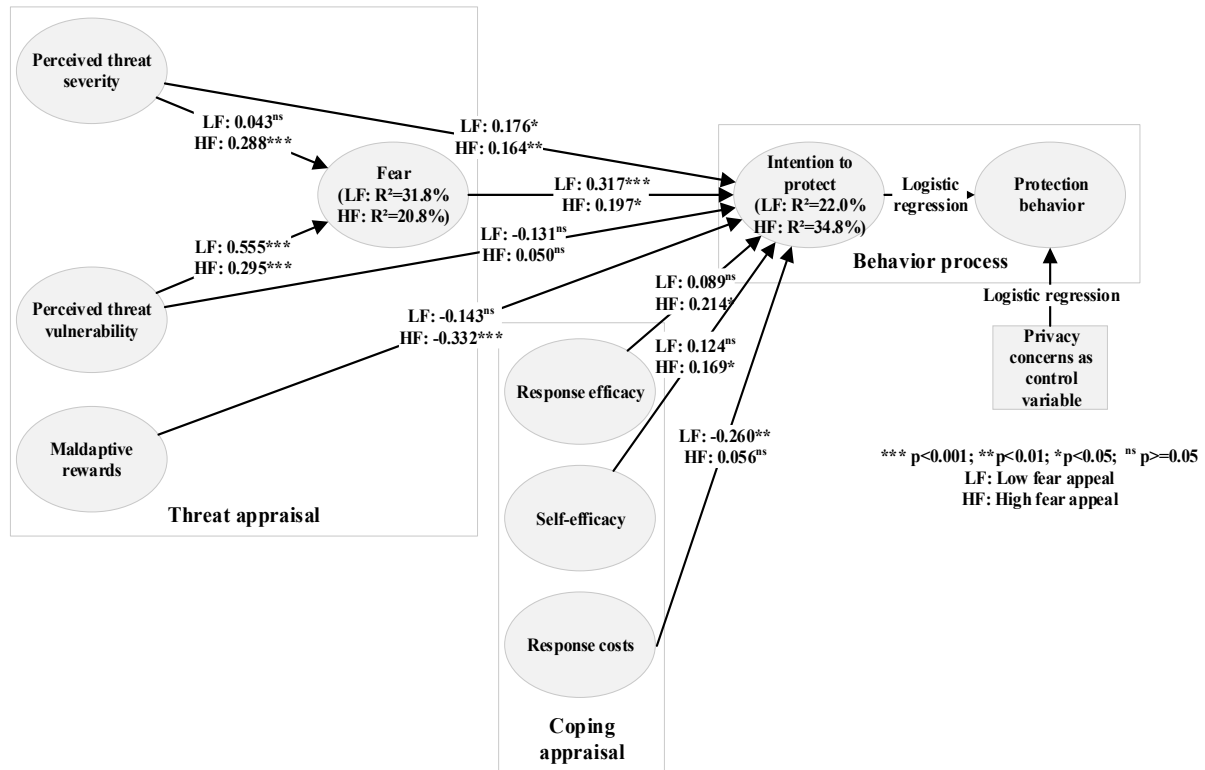


Figure 15. Results of Paper XI

These results show that a fear appeal helps in promoting email tracking protection behavior. This confirms the protection motivation theory (Rogers and Prentice-Dunn 1997) in this context and thus contributes to the email tracking literature (Englehardt et al. 2018) by giving guidance on how to motivate individuals to protect against email tracking. The results also indicate that the protection motivation theory is generally more applicable in a high fear appeal context. This implies that future research in the privacy domain should consider fear appeals by including a high and a low fear appeal in their studies and evaluating the difference, or by including at least a high fear appeal to ensure the maximum applicability of the protection motivation theory.

In summary, **Paper XI** applied the full nomology of the protection motivation theory to investigate its applicability in the email tracking context. While the study confirms the anticipated relationships when participants faced a high fear appeal or a low fear appeal, the relationships were stronger in a high fear appeal context. These results implicate that scholars should generally account for the fear appeal and should also include all relationships from the full nomology of the protection motivation theory.

5.5 SUMMARY OF THE RESULTS

This section summarizes the eleven papers comprising the remainder of this dissertation. **Paper I** provides an overview of privacy research, identifying several research gaps of which some are closed by the remaining **Papers II – XI**, which are structured in terms of privacy ownership, privacy control and privacy turbulence, following the CPM. Furthermore, most other papers include a separate literature review for the particular research problem that is considered in the focal study. In the following, the results for every element are summarized.

Privacy Ownership. The focus of **Paper II** is the collection of personal information by governmental agencies without permission from the individual. This paper finds that individuals often justify this collection, raising the question of who owns that personal information. The paper identifies factors influencing the justification of mass surveillance, finding that loss of privacy control has no

effect on the justification of mass surveillance. **Paper III** focuses on individuals' level of resignation which is strongly influenced by new technological advancements. When individuals are resigned with regard to privacy protection, they no longer trust that they have the sole right to grant or deny access to their personal information.

Privacy Control. **Paper IV** shows that individuals' privacy control behavior is influenced by subjective norm, including the opinion of important referents. **Paper V**, **Paper VI** and **Paper VII** consider the influence of salient individual differences on how individuals control their privacy. **Paper VIII** gives insight into behavioral economics, questioning neo-classical assumptions and theoretical lenses in privacy research and how individuals control their privacy. Finally, **Paper IX** shows that information sensitivity plays a major role, not only in terms of how original owners control their own privacy, but also how co-owners control original owner's privacy. Taken together, these papers illustrate that individuals' control of privacy is influenced by their social environment, their individual differences and cognitive biases, as well as the level of information sensitivity for both the original owner and the co-owner.

Privacy turbulence. **Paper X** shows that the relationship, i.e. strength of tie, between an original owner and an unauthorized co-owner causing privacy turbulence influences the original owner's level of privacy concerns. **Paper XI** finds that appealing to individuals through fear positively influences their decision to protect their privacy using technology in case of privacy turbulence. Since the technological advances of the digital age make it possible to collect personal information without the original owner's awareness, the findings support the merits of increasing individuals' awareness of such collection as a step toward their decision to protect their privacy.

These results have several contributions to research and practice which are discussed next. Furthermore, the overall research question as well as the three corresponding sub-research questions are answered in the following section.

6 DISCUSSION

This section outlines discusses how the results of the papers comprising this dissertation contribute to privacy literature and practice, answers the overall research question, identifies the limitations of the studies and derives avenues of potentially fruitful future research.

6.1 CONTRIBUTIONS TO LITERATURE

Broadly speaking, the contributions are structured following the three elements of the CPM. In some cases, the implications for an element are also based on papers generally assigned to a different element. Each element contains a table summarizing the CPM content, the CPM interpretation, the relevant research question (see section 3.4) challenging that interpretation, and an answer to that research question. Collectively, these insights will help answer the overall research question which answer is given in section 6.2.

6.1.1 Privacy ownership

The results of **Paper II** and **Paper III** imply that the interpretation of privacy ownership as outlined by the CPM is not always applicable in the digital age. Moreover, privacy ownership also affects privacy control. An overview is given in Table 14.

CPM content	CPM interpretation	Research question challenging interpretation	Answer to research question
There can be original owners and co-owners of personal information	Individuals believe that they own their personal, private information. They also trust that they have the right to protect their personal information or to give access to it.	How do individuals handle privacy ownership in the digital age?	In the digital age, individuals no longer always believe they are the sole owners of their personal information. They are sometimes resigned in terms of protecting their privacy, lacking the trust that only they have the right to determine who has access to their personal information.

Table 14. Answer to the first research question regarding privacy ownership

6.1.1.1 Privacy ownership needs to be reinterpreted in the digital age

According to the CPM, individuals believe they are the sole owners of their personal information and trust that they have the right to protect or to give access to their personal information. Once they have granted access, original owner trust that they have the right to decide whether to revoke the status of co-owners or make others new co-owners (Petronio 2013).

This changes as mass surveillance is made possible through the digital age, as described in **Paper II**. In this case, an individual often does not actively give access to her data and she is frequently not asked for permission to access it (Karwatzki et al. 2017). The CPM suggests that the individual should respond to an unauthorized breach of ownership by objecting to this unsolicited access. In reality, however, most individuals do not object. In fact, a majority supports mass surveillance (Reddick et al. 2015). This indicates that the individual no longer believes that she is the sole owner of her information. Not objecting to another entity gaining unsolicited access to personal information makes that entity an owner as well.

Paper II supports this conclusion, showing that increased security allegations tend to lead to increased justification of mass surveillance. Interestingly, the results also show that a loss of privacy does not affect justification of mass surveillance which supports the results of **Paper X** such that individuals are less concerned about their privacy if some unknown entity is having access to their information. If the individual considered herself the sole owner of her personal information, this relationship should be negative. However, even though a majority of individuals think that mass surveillance reduces privacy control (Strauß 2017), this relationship is non-existent. This result indicates that the explanation is that the individual no longer considers herself to be the sole owner. The results also indicate that the reason for this consideration is that the individual sees benefits of mass surveillance in terms of improved security or making the world less dangerous.

It is important to distinguish that the entity conducting mass surveillance is not an authorized co-owner. An authorized co-owner has been authorized by the original owner. This authorization can also be revoked by the original owner at any time. However, in the case of mass surveillance, the original owner does not give authorization and cannot revoke it. Rather, the entity conducting mass surveillance provides itself with access to the information, decides which information is to be accessed and what is done with it. This does not speak in favour of an authorized co-owner, but of an additional owner.

Paper III also questions the interpretation of the CPM regarding privacy ownership. This study builds on previous research showing the importance of resignation in privacy research (e.g., Hoffmann et al. 2016). This paper first shows that resignation can exist in the privacy domain. If that is the case, also as shown by recent studies (Guo and Yu 2020), individuals can resign to the fact that others can control who has access to their information such that they can no longer protect their privacy. With this, they can no longer trust that only they have the right do so. This contradicts the interpretation of the CPM regarding privacy ownership.

Taken together, the findings of **Paper II** and **Paper III** suggest that privacy ownership should be

reinterpreted in the digital age and the interpretation of the CPM should not be viewed as generally valid. In the digital age, individuals often no longer believe they are the sole owners of their private information and often no longer trust that they have the sole right to give access to or protect their personal information. In certain circumstances, they may also consider others to be owners and have less confidence in their right to decide alone who has access to their personal information.

This does not make the first element of the CPM useless in the digital age, or does the CPM lose its value as a scheme to understand the management of privacy in the digital age. The privacy ownership concepts of original owners and co-owners remain intact. However, the findings of this dissertation demand a reinterpretation of the content.

6.1.1.2 Privacy ownership influences privacy control

As individuals lose sole control over ownership of and access to their private information in the digital age, the results of **Paper III** show that the basic premise of the privacy calculus (Dinev and Hart 2006) changes. Hence, a change in privacy ownership directly affects privacy control as well.

These results from **Paper III** contribute to privacy literature. The reinterpretation of privacy ownership has a direct impact on privacy control. This extends previous research which indicates that privacy ownership has an effect on the belief of the individual that she is also allowed to control her privacy (Petronio 2013). The results of **Paper III** extend this view by showing that the way how individuals control their privacy is different, when privacy ownership changes. Scholars should therefore not only look at privacy control but should also look at privacy ownership at the same time. If they do not do so, situations may arise where one element is not understood because another has changed. For example, by looking at privacy ownership in **Paper III**, the privacy calculus and thus privacy control could be better understood.

6.1.2 Privacy control

The privacy control element of the CPM explains how individuals decide to either disclose or to conceal information. The CPM identifies five criteria for defining the rules determining privacy control (Petronio and Altman 2002). However, the results of **Papers III, IV, V, VI, VII, VIII and IX** show how this view on criteria needs to be extended and how other theories need to be considered differently (see Table 15).

CPM content	CPM interpretation	Research question challenging interpretation	Answer to research question
Individuals can give access to personal information to others or not.	In deciding whether others may access information, individuals follow rules determined by five criteria.	What determines individuals' control of their own and others privacy?	There are criteria not included in the CPM that influence individuals' control of privacy: Individual differences, the level of subjective norm, the level of resignation, the sensitivity of the information to be disclosed and how much effort individuals put into their decision making. These concepts are interwoven and affect other theories, such as the privacy calculus.

Table 15. Answer to the second research question regarding privacy control

6.1.2.1 Laziness and mindfulness extend the understanding of the privacy paradox and the protection motivation theory

Paper V, Paper VI and Paper VII give further insights into the privacy paradox (Kokolakis 2017; Norberg et al. 2007) and the protection motivation theory (Boss et al. 2015; Rogers and Prentice-Dunn 1997).

In particular, **Paper V** provides a further explanation of the privacy paradox (Kokolakis 2017) beyond the privacy calculus (Dinev and Hart 2006) and behavioral economics (Acquisti and Grossklags

2003, 2005; Dinev et al. 2015), pointing to laziness as an additional factor. The results show that the privacy paradox is influenced by laziness. That means that scholars, researching on the privacy paradox should take into account the laziness of individuals. If individuals are “high lazy” then the privacy paradox is more likely to occur than among “low lazy” individuals. Hence, if scholars want to avoid the privacy paradox or might want to exclude laziness as an explanation, they should focus on participants who are “low lazy”.

Furthermore, the results of **Paper VI** show that dynamic, context-specific traits generally have greater explanatory power than broad personality traits. This complements previous research suggesting that the explanatory power of broad traits can be increased by focusing on more narrow traits (Paunonen and Ashton 2001). In particular, it was shown that IT mindfulness, a dynamic, context-specific trait, helps explain beliefs and behavior. This has also confirmed recent research, pointing at the importance of mindfulness in general and the need to adapt it to the particular context of the research setting (Thatcher et al. 2018). In **Paper VII**, mindfulness is then adapted to the domain of privacy and applied to better understand the protection motivation theory. In particular, mindfulness is established as an antecedent of threat appraisal and coping appraisal, showing that the more mindful an individual is, the higher both appraisals are. This paper thus helps explain why individuals can appraise the same threat differently and exhibit different behaviors regarding their privacy-protection. More mindful individuals are more likely to perceive a threat to their privacy as dangerous but are also more likely to be able to cope with that threat. In applying the protection motivation theory, scholars should account for the level of mindfulness of study participants to ensure that the theory is workable. If participants have low levels of mindfulness, the level of threat and coping appraisal must be more increased to make the protection motivation theory more functionable than if the individuals have high levels of mindfulness (Boss et al. 2015; Rogers and Prentice-Dunn 1997).

6.1.2.2 Resignation and subjective norm as further explanations for a non-functionable privacy calculus

One of the criteria set out by the CPM to define rules to control privacy is the risk/benefit ratio (Petronio 2013), which directly points to the privacy calculus (Dinev and Hart 2006). However, previous research has shown that the privacy calculus does not apply in certain circumstances. For example, individuals sometimes disclose information even though the benefits do not outweigh privacy risks. Several particular explanations have been provided, such as cognitive biases, incomplete information or mental states of the individual (Acquisti 2004; Brakemeier et al. 2016). **Paper III** and **Paper IV** provide additional explanations for a privacy calculus that does not work. **Paper III** shows that resignation in terms of privacy protection strengthens the effect of benefits and weakens the effect of privacy risks. Similarly, **Paper IV** shows that the effect of subjective norm on disclosure is stronger than the effects of benefits or privacy risks.

The results of **Paper III** and **Paper IV** directly contribute to the most used theoretical lens – the privacy calculus (Dinev and Hart 2006) – and thus to the broader privacy domain. The results of **Paper III** imply that the basic premise of the privacy calculus loses validity when individuals have resigned in terms of protecting their privacy. Scholars should thus refrain from applying the privacy calculus if participants are highly resigned in protecting their privacy and should rather focus on other theories to explain disclosure.

This also extends previous explanations for why the privacy calculus sometimes fails, including insufficient access to information, bounded rationality, or distortion due to psychological factors (Acquisti 2004). Yet, even if an individual had access to all necessary information, had all the mental capabilities and had no psychological distortions, **Paper III** suggests that when the individual is resigned, she might still disclose information despite low benefits and high privacy risks.

Furthermore, the results of **Paper IV** suggest that when subjective norm is high, the privacy calculus can lose explanatory power. Hence, scholars should also focus on the subjective norm of their participants. If subjective norm is high, then the basic premises of the privacy calculus might still apply but have less effect on the participants than their level of subjective norm. In such a case, scholars may either drop the relationships of benefits and privacy risks or focus on other theories which either then diminish the effect of subjective norm or where subjective norm might again be the dominant antecedent.

In addition, previous explanations (Acquisti 2004; Brakemeier et al. 2016; Dinev et al. 2015; Sarathy and Li 2007) have considered the alteration of benefits and privacy risks or the alteration of the effect of benefits and privacy risks on disclosure. **Paper IV** provides the additional explanation that other concepts can overlie the effect of benefits and privacy risks on disclosure. Scholars are called to identify additional factors which may diminish the effects of benefits and privacy risks on disclosure.

6.1.2.3 Individual differences need to be considered by the CPM

Another criteria the CPM sets out that can influence the definition of rules to control privacy is gender (Petronio 2013). Gender is an individual difference (Eysenck and Eysenck 1985). However, the results of **Papers V, VI and VII** identify other such individual differences need to be considered, including laziness and mindfulness. **Paper V** demonstrates the direct influence of laziness on how individuals control their privacy, and **Paper VII** builds on the results of **Paper VI**, showing how the appraisal of threats and how to cope with the threats (Rogers and Prentice-Dunn 1997) is better understood by considering mindfulness.

Taken together, these results imply that the CPM's assertion that privacy control is determined by five criteria (Petronio 2013; Petronio and Altman 2002) insufficiently explains the control of privacy. Rather, the interpretation of privacy control should be extended to account for individual differences (Eysenck and Eysenck 1985). That does not nullify the content of the privacy control element, nor does it invalidate the interpretation of that element by the CPM itself. Rather, in applying the CPM's criteria to the definition of rules to control privacy, scholars should also consider individual differences.

6.1.2.4 The criteria for rules in the CPM are interdependent

More recent research has shown that criteria of the CPM are interdependent (Petronio 2013). The results of **Paper IV, Paper V and Paper VII** contribute to this research stream.

Paper IV demonstrates the effect of subjective norm (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975) on the privacy calculus. Subjective norm has been considered as part of the social environment which is in turn part of the context (Petronio and Altman 2002). The results indicate that subjective norm is more important in explaining disclosure than benefits or privacy risks. This contributes to the CPM because it shows that the context has a direct effect on the risk/benefit ratio. Previous research has rather focused on the influence of motivation on the risk/benefit ratio (Petronio 2013). When individuals are in a context where subjective norm is high, then the effects of benefits and privacy risks (which are reflected by the risk/benefit ratio) diminishes. As mentioned in the previous section, **Paper V** and **Paper VII** demonstrate that individual differences should be considered alongside the other criteria for rules in the CPM. At the same time, individual differences also affect the privacy paradox and the protection motivation theory.

In summary, these results confirm and extend previous research (Petronio 2013) that it is insufficient to focus on just one criterion or on several criteria independently that determine rules to control privacy. Rather, scholars are called to theorize the mutual, interdependent effects of criteria. For example, when scholars focus on the risk/benefit ratio, they also need to take into account the social environment and

how that social environment affects the risk/benefit ratio. With such considerations, scholars can better explain privacy control.

6.1.2.5 Perceived information sensitivity needs to consider original owners as well as co-owners

Most privacy research takes the perspective of the original owner controlling her own privacy. The CPM asserts, however, that when the original owner discloses information, there is a co-owner (Petronio 2013) who also has the responsibility and ability to control the privacy of the original owner. Hence, to understand privacy control in CPM, one also needs to understand how co-owners behave.

As confirmed by **Paper X**, perceived information sensitivity is an important concept in understanding privacy-related decisions (Mothersbaugh et al. 2011). However, **Paper IX** shows that perceived information sensitivity is not well-defined and must be expanded to include the co-owner viewpoint, i.e. how does a co-owner perceive the sensitivity of information not only for herself, but also for the original owner.

These results contribute to the broader privacy domain in two basic ways. First, perceived information sensitivity is redefined considering multiple perspectives, as “*an individual’s assessment of information belonging to him/herself or any other individual based on the perceived negative consequences for him/herself or any other individual due to the loss of an individual’s privacy with regard to the information*”. Such a definition has been lacking in the literature and should lead to a clearer understanding of perceived information sensitivity, its determinants and effects. For example, whereas some research studies have only focused on perceived intimacy level affected by perceived information sensitivity (Dinev et al. 2013), this definition also includes possible negative impacts not only on the individual disclosing information, but also on other affected individuals. This enables perceived information sensitivity to be applied in more realistic settings, where individuals consider the negative consequences of perceived information sensitivity for themselves and for others. Furthermore, research is often simply stating that perceived sensitivity of information varies according to the type of information (e.g., Malhotra et al. 2004), which is insufficient to make sure to grasp the full concept of information sensitivity (Milne 1997; Milne and Gordon 1993). Such research might have to be reconsidered through the lens of the new definition and by actually measuring the sensitivity of information.

Second, the protection of information of the original owner by the co-owner is explained. **Paper IX** identifies two categories that determine the co-owner’s decision: 1) issues that concern the co-owner herself (perceived enjoyment and perceived information sensitivity for the co-owner, dependent on several moderating effects), and 2) issues that concern the original owner (the level of perceived information sensitivity for the original owner and the level of motivation to comply as determinants). Previous research focusing primarily on the original owner and not the co-owner neglects the first category and with this explains less what leads a co-owner to protect the privacy of the original owner. In contrast, the extended concept of perceived information sensitivity better explains the protection of information of the original owner by the co-owner. Scholars applying perceived information sensitivity in studies including co-owners besides the original owner should therefore draw on the extended concept.

6.1.2.6 Privacy control is influenced by behavioral economics

To understand privacy control, the previous contributions have focused on different concepts and extensions of the CPM or other theoretical lenses. These contributions focused on individuals who put high effort into their decision making process, in line with most other previous research (Dinev et al. 2015). This does not have to be necessarily wrong since individuals can put high effort into their

decisions. However, individuals often put low effort into their decision making process (Dinev et al. 2015), exposing their decisions more strongly to distortionary behavioral economics effects such as cognitive biases (Ariely 2010; Bodenhausen et al. 2001; Cialdini 2010; Kahneman et al. 1982; Tversky and Kahneman 1974).

Paper VIII investigates the role of the anchoring effect as such a cognitive bias. The results underscore the importance of recognizing that individuals are not always fully rational agents and are often subject to cognitive biases. Scholars should include such biases e.g. as control variables or as hypothesized concepts in their research models. To do so, they should also account for the level of cognitive effort the participants make in the study, such as by applying the cognitive reflection test (Frederick 2005) (see **Paper VIII**). If cognitive effort is high, then behavioral economics will have a weaker effect than when cognitive effort is low. Ideally, scholars should adopt a theoretical basis which acknowledges that individuals do not always invest great cognitive effort in their decision making.

Specifically, **Paper VIII** demonstrates that the anchoring-effect (Furnham and Boo 2011; Kahneman et al. 1982) should be considered when researching on amount and accuracy of disclosure (Posey et al. 2010; Wheelless 1978; Wheelless and Grotz 1976). The results demonstrate that both amount and disclosure can be influenced by an anchor. Scholars should therefore attempt to eliminate or account for anchors in research studies where cognitive effort levels on the part of participants is low and where disclosure is aimed to be explained. The results of previous studies on actual disclosure (e.g., Berendt et al. 2005; Choi et al. 2018; Joinson et al. 2010) may be deepened by considering possible anchoring-effects and other cognitive biases.

6.1.3 Privacy turbulence

The privacy turbulence element of the CPM explains that privacy can also be harmed in unforeseeable ways. **Paper X** and **Paper XI** focus on privacy turbulence in the digital age. The results demonstrate that in the digital age, new unauthorized co-owners such as hackers have entered the stage. Such co-owners lead to different levels of privacy concerns. Individuals might even be unaware of disclosure and thus of their privacy turbulence. Arousing fear is one way to make individuals aware of the privacy turbulence and to motivate them to resettle their boundaries (see Table 16).

CPM content	CPM interpretation	Research question challenging interpretation	Answer to research question
Original owners do not always fully control their personal information.	Original owners will resettle the collective boundaries in case of privacy turbulence.	How do individuals handle privacy turbulence in the digital age?	In the digital age, new unauthorized co-owners have entered the stage. Original owners have different levels of privacy concerns, depending on such unauthorized co-owners. In addition, original owners may be unaware of disclosure of information. Fear can then raise awareness and help motivate original owners to resettle their boundaries.

Table 16. Answer to the third research question regarding privacy turbulence

6.1.3.1 Privacy turbulence depends on who the co-owner is

Privacy turbulence is when an unauthorized co-owner has access to personal information of the original owner (Petronio 2013). Previous research has not considered how privacy turbulence varies depending on the relationship between the original owner and the unauthorized co-owner (Karwatzki et al. 2017). **Paper X** closes this research gap by showing that privacy concerns differ depending on the co-owner. This confirms the CPM's delineation of owner and co-owner in privacy research (Petronio 2013; Petronio and Altman 2002) and emphasizes the importance of co-owners due to their growing number of potential unauthorized co-owners in the digital age such as hackers or unauthorized organizations (Karwatzki et al. 2017). Given the importance of privacy concerns in privacy research

(Smith et al. 2011), the results point to the need for continued research into the role of the relationship between original owners and co-owners as an additional antecedent of privacy concerns.

Specifically, scholars in privacy research should clearly name potential authorized and unauthorized co-owners and the type and strength of their relationship, rather than not mentioning or inaccurately describing them (e.g., Awad and Krishnan 2006). This will lead to a clearer understanding of how privacy concerns are developed and yield more consistent results.

6.1.3.2 Fear helps in reframing collective boundaries

Paper VII applied the protection motivation theory to determine to what extent threat appraisal and coping appraisal are influenced by the level of mindfulness. **Paper XI** also applies the protection motivation theory to determine what drives original owners to protect themselves against privacy threats. The results show fear increases the probability that individuals will protect themselves against privacy threats. These results contribute in several ways.

First, in **Paper XI**, email tracking (Xu et al. 2018) was selected as a technology that can threaten individuals' privacy by disclosing information potentially without the awareness of the original owner (Bender et al. 2016). This example goes beyond the CPM, which assumes that individuals are aware that they are disclosing information. Therefore, the results imply that the unaware disclosure which is prevalent in the digital age (e.g., Belanger and Hiller 2006) require that the CPM be extended to include unaware disclosure by the original owner. Furthermore, scholars applying the CPM to study cause-effect relationships in privacy must clarify whether the disclosure in their study is unaware or aware. If disclosure is unaware, they need to either extend the CPM or rely on a different theory.

Second, the results of **Paper XI** show that frightening individuals can motivate them to readjust their collective boundaries. This contributes to the privacy domain in general by emphasizing the role of fear: If scholars want to move individuals to protect their privacy to end privacy turbulence, they can frighten them. It follows that scholars whose aim is it to find ways how participants can protect their privacy after it has been in turbulence, need to control for the level of fear of their participants. As the results of **Paper XI** and the protection motivation theory in general indicate (Rogers and Prentice-Dunn 1997), the level of fear is an influencing concept of protection behavior. In identifying other determinants, fear will still need to be accounted for.

Third, previous research in the privacy domain has failed to use all of the concepts and relationships of the protection motivation theory. As demonstrated by **Paper XI**, all concepts and relationships of the protection motivation theory need to be considered in privacy research, especially including the fear appeal. The results confirm the application of high fear appeal in the manner suggested by previous research (Boss et al. 2015; Rogers and Prentice-Dunn 1997) increases the effectiveness of the protection motivation theory. If scholars do not include a high fear appeal, they should at least provide a rationale for why they included a low fear appeal or did not include any fear appeal. One such rationale is demonstrated in **Paper VII**, where mindfulness is not meant to replace the fear appeal but can still trigger the threat appraisal and coping appraisal process.

6.1.3.3 Privacy turbulence influences privacy control

The CPM states that in case privacy turbulence happens, individuals will resettle their collective boundaries and with this will resettle the way how they control their privacy. However, both elements are usually still considered independent of each other, without giving details how privacy turbulence will affect privacy control (Petronio 2013; Petronio and Altman 2002). The results of **Paper X** and **Paper XI** contribute to this issue by providing more particular insight into how privacy control changes in case of privacy turbulence.

Paper X shows how privacy concerns emerge as the result of privacy turbulence, which may then subsequently affect the way how individuals control their privacy (Smith et al. 2011). Furthermore, **Paper XI** shows how privacy turbulence can result from unaware disclosure. In addition, when the individual becomes aware, they are more likely to reframe their collective boundaries and thus also adjust their privacy control. As **Paper XI** shows, the level of awareness of privacy turbulence influences how individuals control their privacy. Hence, in this way, privacy turbulence influences privacy control.

6.2 ANSWERING THE OVERALL RESEARCH QUESTION

The overall research question of this dissertation is how individuals manage their privacy in the digital age. In considering each element of the CPM in the context of the digital age, the theoretical background of this dissertation revealed the need to reinterpret or extend the elements of the CPM (Petronio 2013), giving rise to a different sub-research question pertaining to each element. As discussed in detail above, individuals may no longer consider themselves the sole owners of personal information and may no longer trust that they alone have the right to decide who has access to their personal information. Furthermore, privacy control is not only determined by the five mentioned criteria by the CPM but also by criteria such as individual differences, the level of subjective norm, the level of resignation, the sensitivity of the information to be disclosed and how much effort they put into their decision making. These concepts are interdependent and interwoven, such that e.g. the effects of benefits and privacy risks depend on the level of resignation. Finally, privacy turbulence is more complex and prevalent in the digital age, involving new co-owners and varying levels of privacy concerns, based on the relationships between the original owner and the co-owner and on whether the original owner is aware or unaware of the disclosure of information.

In order to understand privacy ownership in the digital age, it is important to understand why individuals may accept entities collecting personal information about them. In order to understand privacy control in the digital age, it is important to understand what motivates the disclosure or concealment of information. And in order to understand privacy turbulence in the digital age, it is important to understand how individuals behave when they are no longer solely in control of privacy decisions or aware of unauthorized co-ownership. These answers to the three sub-research question help in answering the overall research question of this dissertation: Individuals manage their privacy in the digital age by considering possible other owners of information, by considering multiple concepts that determine their decision to conceal or to disclose information, by considering who the entity is and their relationship with the entity that potentially caused privacy turbulence and, once aware of privacy turbulence, by trying to restore effective privacy control if sufficiently motivated to do so. This answer to the overall research question demonstrates that the management of privacy is a difficult and complex task (Petronio 2015).

In addition to individuals, organizations and states also benefit by understanding how individuals manage their privacy in the digital age. Organizations rely on the personal information of individuals (Dinev et al. 2006; Posey et al. 2017) and the state also justifies its laws based on how individuals manage their privacy (Kokolakis 2017). Such implications will be discussed in the section below.

6.3 IMPLICATIONS FOR PRACTICE

In addition to its implications for literature, this dissertation also has several practical implications.

6.3.1 Individual resignation may render laws ineffective

In the digital age, many individuals no longer believe they can protect their private information. An example of this resignation is when people view mass surveillance by the government as inevitable and beyond their control or assume that private companies such as Google already know everything about them. Privacy protection laws designed to empower individuals to protect their privacy, such as the

EU's General Data Protection Regulation (GDPR), may thus be viewed ineffective in the face of such resignation. The state that makes such laws because it believes its citizens want it to, should therefore address the level of resignation among its citizens. For example, by not only initiating laws but also showing that they are effective. Or by showing individuals possible solutions to protect their privacy in general, in order to lower the level of resignation.

6.3.2 Social networks could convince individuals that important referents want them to disclose

Organizations, and especially social networks, depend on individuals revealing their personal information. Network providers that generally take advantage of the current state of theory, would try to aim to show potential customers how they will benefit from joining and actively participating in the social network while minimizing their perception that doing so may pose a risk to their privacy. This may be a correct approach - but an additional approach is to convince potential customers that individuals important to them want and expect them to join and actively participate in the social network, perhaps by demonstrating that such important referents are already disclosing personal information. This may increase the social pressure on current and potential customers to disclose personal information as well.

6.3.3 Organizations must consider the ethics of manipulating customers to disclose

This dissertation shows that individuals often make decisions about whether to disclose personal information without full cognitive effort, sometimes intuitively. Furthermore, it shows that organizations can take advantage of this mindset by using anchors to influence customers' decisions. For example, by providing a large text field, organizations can increase the amount of desirable input provided by individuals, such as personal information, and by providing a small text field, organizations can reduce the length of undesired input, such as complaints. However, the ethics of such customer manipulation with regard to privacy management, such as in order to increase revenues through targeted advertising, are questionable and must be considered carefully.

6.3.4 Technology could protect privacy, especially on social networks

This dissertation demonstrates that individuals can only manage their own privacy to a limited degree and are dependent on authorized and unauthorized co-owners of their personal information, including friends, acquaintances, organizations and the government, to protect their privacy. One way that technology can help to protect privacy on social networks is by automatically requiring co-owners to receive the permission of original owners to disclose the original owner's personal information. Another form of protection would be to automatically inform co-owners that the information they intend to disclose does not belong to them and require them to actively acknowledge that they have the original owner's permission to disclose it. Organizations could help protect the privacy of their customers by implementing such technologies.

6.3.5 The state should address different levels of privacy concerns

By definition, privacy is only lost if private information is actually disclosed, but disclosure is not necessarily and automatically a threat to privacy. For example, if the original owner still has control over her personal information after it is disclosed, then privacy is still maintained. When, however, the original owner loses control over her personal information after it is disclosed, her privacy is threatened. This thesis finds that the then arising level of privacy concerns depends on the relationship between the original owner and the unauthorized co-owner.

The state should help to ensure that the personal information of individuals is not unlawfully disclosed to others. By enacting laws, the state can counteract such disclosure of information. At the same time, the state should also be aware of how individuals react when their information is disclosed.

The results of this dissertation show that individuals are concerned differently depending on who is the one who gains unauthorized access to personal information. The highest level of concern is caused by unauthorized individuals who are somewhat familiar with the individual in question. Less concern arises when there is a strong or no relationship between the two individuals. So, if the state also legislates based on how individuals react, then special emphasis should be placed on ensuring that no unauthorized access to information is possible where both individuals are somewhat familiar with each other.

6.3.6 The state should help prevent unaware disclosure

Email tracking is a common way to collect information in the digital age without consent or awareness. Given the general lack of awareness of email tracking as a very real threat to privacy, the state can increase its citizens' ability to control their personal information by passing laws prohibiting unknown information disclosure such as unauthorized email tracking. The GDPR has already made a first step towards it, however, since roughly all newsletters track their recipients (Brunet 2017), this law seems to be insufficient to address the problem of unaware disclosure.

6.4 LIMITATIONS

As with all research studies, this dissertation has several limitations. First, four of the papers comprising the dissertation (**Paper III**, **Paper IV**, **Paper VII** and **Paper IX**) measure intention rather than actual behavior. Although intention can result in the anticipated behavior, it does not necessarily lead to behavior (Fazio and Roskos-Ewoldsen 2005). This may weaken the explanatory power of the findings from these papers to some degree. This dissertation attempts to overcome this gap by also including papers (**Paper V**, **Paper VIII** and **Paper XI**) that focus on actual behavior. However, the results of the aforementioned papers could be different, when actual behavior instead of the intention would have been the dependent variable.

Second, this dissertation focuses solely on the private usage context, with the exception of **Paper VI**, which integrates the organizational context. However, **Paper VI** is not about privacy issues, but rather demonstrates the importance of mindfulness. Up until around 2000, the organizational usage context was important, but the rise of the use of the Internet in the private domain has shifted the focus of much research to the private usage context (Li 2011b). Given differences between the private and the organizational use domains, such as the purpose of disclosure or the intent of disclosure, further research is needed to test the viability of the results of this dissertation in the organizational use context.

Third, as scholars have recently pointed out, common models used in privacy research assume that individuals invest high effort into their decision-making process with regard to privacy protection, which is not always true (Dinev et al. 2015). **Paper VIII** of this dissertation confirms this issue and takes steps to overcome it. The results of the remaining papers, however, may be influenced by this inaccurate assumption. Future research should account for varying degrees of effort with regard to the possible influence on dependent variables.

Fourth, the body of literature and the entire dissertation is limited to the IS discipline. This especially applies to **Paper I**, yet, also to all other papers. However, also other disciplines deal with privacy such as psychology or marketing in an effort to better understand individual management of privacy in general. This dissertation tries to deal with this limitation by clearly pointing at the IS domain.

Fifth, the majority of the studies comprising this dissertation use a cross-sectional research design (**Paper II**, **Paper III**, **Paper IV**, **Paper VII**, **Paper IX** and **Paper X**). This dissertation tries to overcome this limitation by taking approaches with multiple snapshots (**Paper V**, **Paper VI**, **Paper VIII** and **Paper XI**).

Sixth, **Paper III**, **Paper IV**, **Paper V** and **Paper IX** focus on SNS technology, which has been shown

to be a suitable context for privacy research (Biczók and Chia 2013). However, since data was only collected in one particular SNS usage setting, the results may or may not be generalizable to other SNS or other technologies. In an effort to overcome this limitation, this dissertation also includes studies involving other technologies, such as email tracking (**Paper XI**), technology to conduct mass surveillance (**Paper II**) and studies without a focus on a particular technology (**Paper X**).

Seventh, **Papers II, III, VII, VIII and IX** rely on participants that predominantly come from the US. In contrast, **Papers IV, V, VI, X and XI** rely on participants who come from Germany. Previous research has indicated that cultural differences, especially in the privacy domain, may lead to different results (Krasnova and Veltri 2010). This dissertation tries to overcome this issue by not only focusing on one culture. However, although the results of e.g. **Paper VI** show that results from Germany and the U.S. are comparable, the results of the particular papers may still be different when participants from a different culture would have been asked.

6.5 FUTURE RESEARCH

The above-mentioned contributions and limitations point to potentially fruitful avenues for future research into privacy management.

First, as discussed above, and especially in **Paper III**, privacy control is influenced by privacy ownership because individuals who no longer think they are the sole owners of their personal information control their privacy differently. Future research in this area should consider the effect of the loss of privacy ownership on privacy turbulence and the degree to which privacy control and privacy turbulence are still necessary if individuals no longer think they are the sole owners of their personal information.

Second, **Paper VIII** shows how disclosure varies depending on the anchoring effect. Future research on individuals who put only low effort into their decisions could include other cognitive biases, how biases influence concepts besides disclosure, or to what degree effects are moderated. Building on **Paper VIII**, which investigates the amount and accuracy of disclosure, future research should identify and test other dimensions, such as the nature of the private information (Biczók and Chia 2013; Wheelless and Grotz 1976) and the valence of the information (Posey et al. 2010; Wheelless 1978; Wheelless and Grotz 1976).

Third, this paper contributes by suggesting that individuals may no longer always think that they are the sole owners of their personal information. A rival theory here is the concept of psychological ownership (Pierce et al. 2001). This concept describes that individuals can have feelings of ownership, e.g. regarding their personal information (Anderson and Agarwal 2010), having a feeling that it is “theirs”. Such psychological ownership leads to protective behavior in case their ownership is threatened (Anderson and Agarwal 2010). This might stand in contrast to the implications of this study. Therefore, one possibility for future research is to particularly concentrate on the concept of psychological ownership especially in the domain of mass surveillance.

Fourth, building on **Paper X**, which provides insight into the role of the co-owner in privacy concerns, future research should investigate other questions: For example, how original owners are influenced by co-owners in controlling their privacy. Or how privacy ownership needs to be considered differently, depending on the co-owner.

Fifth, future research should define and distinguish between voluntary and mandatory disclosure and the impact on privacy ownership. For example, little is known about privacy control and the role of privacy turbulence in mandatory disclosure settings.

Sixth, this dissertation considers IT as a main vehicle of increased threats to privacy in the digital age (Solove 2004). Future research should also focus on IT's potential role in protecting privacy. For example, **Paper X** finds that privacy concerns vary according to co-owners and that absent ties between the original owner and the co-owner lead to less privacy concerns than weak ties between them. Technology facilitating disclosure to absent ties (e.g. online shopping) rather than to weak ties (brick-and-mortar retail) may therefore help reduce privacy concerns. Further investigation into this research stream is needed.

Seventh, as discussed in this dissertation, the assumption that individuals need privacy control to manage privacy effectively is challenged by the control paradox as a rival theory (Brandimarte et al. 2013). According to this theory, individuals are more likely to disclose information the more control they have over it because it makes them feel more safe and secure. Future research should investigate how much control individuals need to protect e.g. against email tracking and at what point they stop protecting against it. A deeper understanding of how the level of resignation influences the control paradox is also needed.

7 CONCLUSION

This dissertation poses and answers the overall research question of how individuals manage their privacy. The eleven papers comprising this dissertation, structured according to the CPM, find that individuals often no longer consider themselves the sole owners of their personal information, which affects how they control their privacy. The papers identify individual differences, the benefits and privacy risks of disclosure, the level of subjective norm, the level of resignation, the sensitivity of the information to be disclosed and how much effort individuals put into their decision making as interwoven and interdependent concepts influencing privacy control. Furthermore, fear influences the likelihood that individuals will protect their privacy and restore collective boundaries. When privacy is threatened or lost, individuals assess the co-owner and their relationship to the unauthorized co-owner, which influences their level of concern about their privacy.

As quoted at the outset of this dissertation: "*If this is the age of information, then privacy is the issue of our times*" (Acquisti et al. 2015, p. 509). There is no doubt that we live in the age of information, the digital age, and that privacy is the issue of our times. This dissertation is an effort to help both scholars and practitioners understand the nuances of how we grapple with this issue and manage our privacy as individuals.

8 APPENDIX

8.1 UPDATE OF THE LITERATURE REVIEW OF PAPER I

The literature review of **Paper I** has been published in 2018. The literature that has been reviewed in this paper is from the early year 2017 and before. For the introductory paper of this dissertation, the literature review has thus been updated to also cover more recent findings. To gather literature, the same procedure as described in **Paper I** has been applied. With this technique, 127 additional articles were identified in the first run. After the selection procedure, 40 articles remained. All in all, the literature review thus then deals with 182 articles (40 articles of the updated selection and 142 articles which have already been analyzed in **Paper I**).

Generally, the key results of the literature review do not change. *First*, the majority of studies is still focusing on SNS, however, some of them have also focused on location based or healthcare contexts (see Figure 16). *Second*, the intention to disclose is still the most behavioral-researched variable, followed by usage of technology. In **Paper I**, actual disclosure behavior has been the second-most researched behavioral variable. However, usage of technology and actual disclosure behavior go head to head as it has already been before. Privacy concerns and WTP/WTS are still the most two psychological-related dependent variables (see Figure 17). *Third*, the privacy calculus remains to be the most often applied theoretical lens in privacy research (see Figure 18). *Fourth*, surveys are still the most applied research method with experiments following. However, experiments have made up ground (see Figure 19).

When only considering the 40 articles from the years 2017 – 2020, the results do not differ much. For example, also in this range of years, SNS is the most used research context or intention to disclose is the most used dependent variable. However, what should be noted is that five out of the 28 studies focusing on actual disclosure behavior have been conducted in the years 2017 – 2020, indicating an increase of studies on this dependent variable. Furthermore, 15 out of the 72 studies conducting experiments have been conducted in the same range of years, again, indicating an increase in this type of methodology.

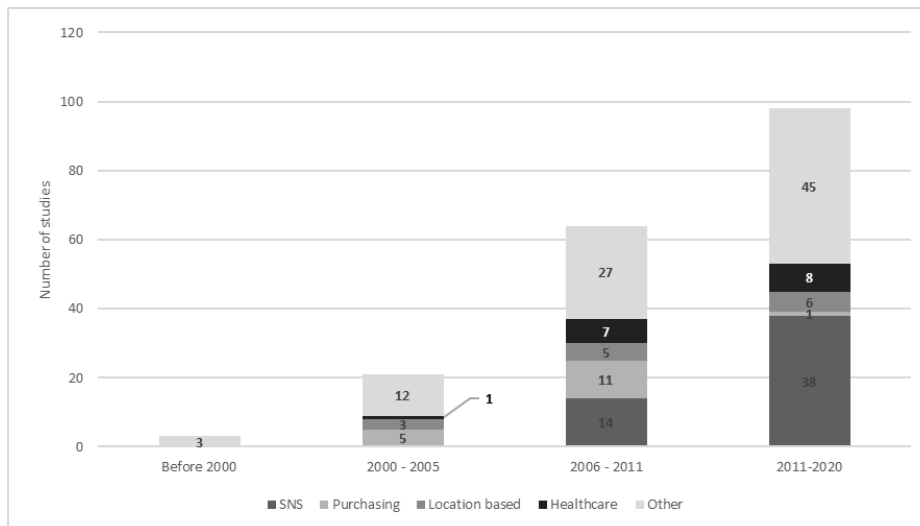


Figure 16. Research setting

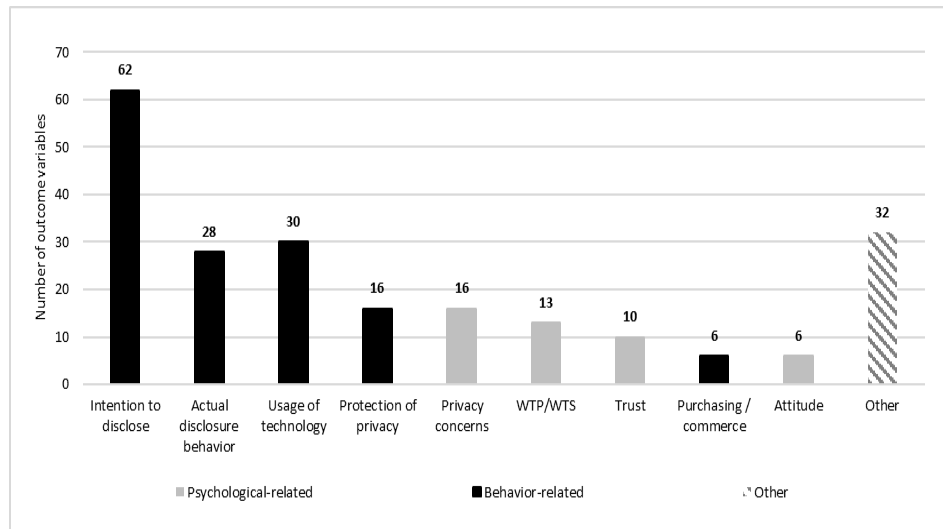


Figure 17. Dependent variables applied by prior research

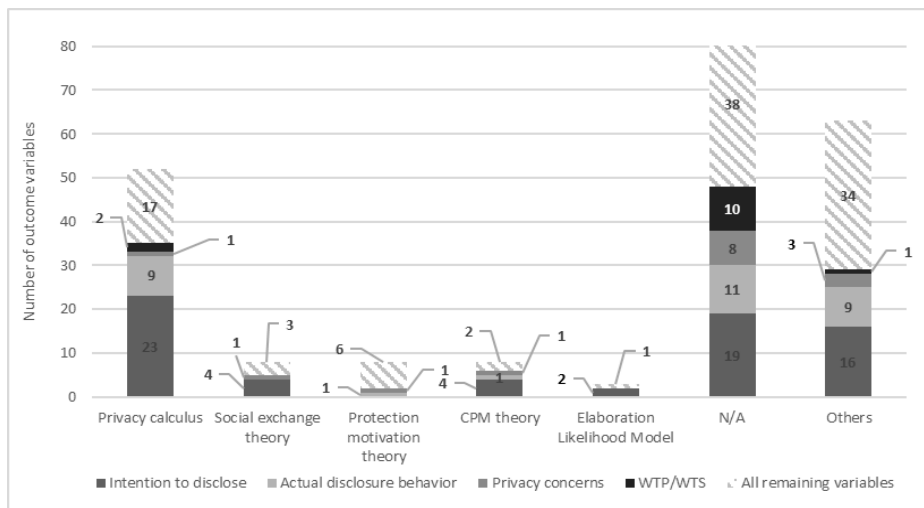


Figure 18. Applied theories in relation to dependent variables

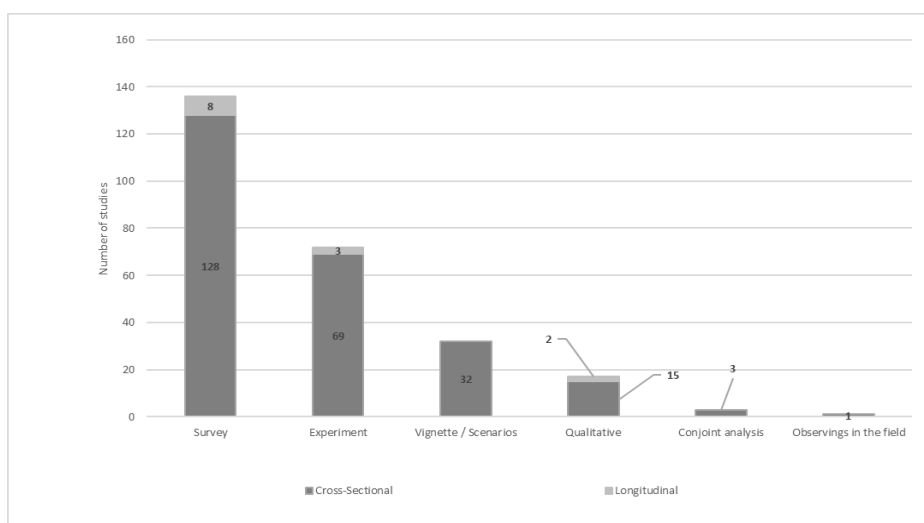


Figure 19. Methodology and research design

8.2 METHODOLOGY AND DATA ANALYSIS OF THIS DISSERTATION

In this section, an overview of the methodology and data analysis of the eleven papers is given. The corresponding instance that has been implemented in the particular paper is filled grey.

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression	t-Test for independent samples	Interview coding	

Table 17. Methodology and data analysis of Paper I

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression		t-Test for independent samples	Interview coding

Table 18. Methodology and data analysis of Paper II

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression	t-Test for independent samples	Interview coding	

Table 19. Methodology and data analysis of Paper III

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression	t-Test for independent samples	Interview coding	

Table 20. Methodology and data analysis of Paper IV

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews		Past literature		Logfiles
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression		t-Test for independent samples	Interview coding

Table 21. Methodology and data analysis of Paper V

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews		Past literature		Logfiles
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression		t-Test for independent samples	Interview coding

Table 22. Methodology and data analysis of Paper VI

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression	t-Test for independent samples	Interview coding	

Table 23. Methodology and data analysis of Paper VII

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews		Past literature		Logfiles
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression		t-Test for independent samples	Interview coding

Table 24. Methodology and data analysis of Paper VIII

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression	t-Test for independent samples	Interview coding	

Table 25. Methodology and data analysis of Paper IX

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews		Past literature		Logfiles
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression		t-Test for independent samples	Interview coding

Table 26. Methodology and data analysis of Paper X

	Parameter	Instances					
Methodology	Research approach	Quantitative			Qualitative		
	Research method	Literature review	Survey	Online survey experiment	Online field experiment	Case study	
	Data collection technique	Questionnaires	Interviews	Past literature		Logfiles	
	Duration	Cross-sectional			Multiple snapshots		
Data analysis	Data analysis	Structural equation modeling	Instrument development	Logistic regression		t-Test for independent samples	Interview coding

Table 27. Methodology and data analysis of Paper XI

9 REFERENCES

- Abramson, L. Y., Seligman, M. E., and Teasdale, J. D. 1978. "Learned helplessness in humans: Critique and reformulation," *Journal of Abnormal Psychology* (87:1), pp. 49–74.
- Acquisti, A. 2004. "Privacy in electronic commerce and the economics of immediate gratification," in *Proceedings of the 5th ACM conference on Electronic commerce*, J. Feigenbaum and M. Seltzer (eds.), New York, NY, USA: ACM, pp. 21–29.
- Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), pp. 509–514.
- Acquisti, A., and Fong, C. 2019. "An Experiment in Hiring Discrimination via Online Social Networks," *Management Science*, pp. 1–20.
- Acquisti, A., and Grossklags, J. 2003. "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior," in *2nd Annual Workshop on "Economics and Information Security"*, UC Berkeley.
- Acquisti, A., and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security & Privacy* (3:1), pp. 26–33.
- Acquisti, A., John, L. K., and Loewenstein, G. 2013. "What Is Privacy Worth?" *The Journal of Legal Studies* (42:2), pp. 249–274.
- Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., and Schaub, F. 2017. "Nudges for Privacy and Security," *ACM Computing Surveys* (50:3), pp. 1–41.
- Adeyemi, T. O. 2009. "Inferential Statistics for Social and Behavioural Research," *Research Journal of Mathematics and Statistics* (1:2), pp. 47–54.
- Agarwal, R., and Prasad, J. 1998. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology," *Information Systems Research* (9:2), pp. 204–215.
- Aguirre-Urreta, M. I., and Hu, J. 2019. "Detecting Common Method Bias," *ACM Sigmis Database* (50:2), pp. 45–70.
- AIS 2011. *Senior Scholars' Basket of Journals*. <https://aisnet.org/page/SeniorScholarBasket>. Accessed 31 January 2020.
- Ajzen, I. 2006. *Constructing a theory of planned behavior questionnaire*. <http://people.umass.edu/~ajzen/pdf/tpb.measurement.pdf>. Accessed 30 January 2017.
- Ajzen, I., and Fishbein, M. 1980. *Understanding attitudes and predicting social behavior*, Englewood Cliffs, NJ: Prentice-Hall.
- Alashoor, T., Fox, G., and Smith, H. 2017. "The Priming Effect of Prominent IS Privacy Concerns Scales on Disclosure Outcomes: An Empirical Examination," in *Pre-ICIS Workshop on Information Security and Privacy*, M. Curry and S. Goel (eds.), Seoul, South Korea.
- Alashoor, T., Keil, M., Liu, L., and Smith, J. 2015. "How Values Shape Concerns about Privacy for Self and Others," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- Alashoor, T., Lambert, L. S., and Farivar, S. 2016. "A Review of Measures of Disclosure Outcomes in the IS Privacy Literature," in *Proceedings of the Twenty-second Americas Conference on Information Systems*, B. Shin, R. Nickerson and R. Sharda (eds.), San Diego, USA, pp. 1–5.
- Alavi, M., and Carlson, P. 1992. "A Review of MIS Research and Disciplinary Development," *Journal of Management Information Systems* (8:4), pp. 45–62.
- Altman, I. 1975. *The environment and social behavior: Privacy, personal space, territory, crowding*, Monterey, Calif.: Brooks/Cole Publ.
- Anderson, C. L., and Agarwal, R. 2009. "Genetic Information Altruists: How Far and To Whom Does Their Generosity Extend?" in *Proceedings of the 30th International Conference on Information Systems*, J. Nunamaker and W. L. Currie (eds.), Phoenix, USA.
- Anderson, C. L., and Agarwal, R. 2010. "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Quarterly* (34:3), 613–A15.
- Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469–490.
- Anderson, M. 2018. *A Majority of Teens Have Experienced Some Form of Cyberbullying*.

- <https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/>. Accessed 21 February 2020.
- Archer, J. L. 1980. "Self-disclosure," in *The Self in Social Psychology*, D. M. Wegner and R. R. Vallacher (eds.), New York, Oxford: Oxford University Press, pp. 183–204.
- Ariely, D. 2010. *Predictably irrational: The hidden forces that shape our decisions*, New York: Harper Perennial.
- Armstrong, M. 2019. *How Many Websites Are There?* <https://www.statista.com/chart/19058/how-many-websites-are-there/>. Accessed 17 December 2019.
- Aurigemma, S., and Mattson, T. 2019. "Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research," *Journal of the Association for Information Systems* (20:12), pp. 1700–1742.
- Awad, N. F., and Krishnan, M. S. 2006. "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly* (30:1), pp. 13–28.
- Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: Technological antecedents and implications," *MIS Quarterly* (35:4), pp. 831–858.
- Bagozzi, R. P., and Yi, Y. 2012. "Specification, evaluation, and interpretation of structural equation models," *Journal of the Academy of Marketing Science* (40:1), pp. 8–34.
- Bala, H., and Venkatesh, V. 2016. "Adaptation to Information Technology: A Holistic Nomological Network from Implementation to Job Outcomes," *Management Science* (62:1), pp. 156–179.
- Bansal, G., Zahedi, F. "M.", and Gefen, D. 2010. "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems* (49:2), pp. 138–150.
- Barabas, J., and Jerit, J. 2010. "Are Survey Experiments Externally Valid?" *American Political Science Review* (104:2), pp. 226–242.
- Baruh, L., Secinti, E., and Cemalcilar, Z. 2017. "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review," *Journal of Communication* (67:1), pp. 26–53.
- Belanger, F., and Hiller, J. S. 2006. "A framework for e-government: Privacy implications," *Business Process Management Journal* (12:1), pp. 48–60.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.
- Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems* (11:3–4), pp. 245–270.
- Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., and Seeam, A. 2016. "Pervasive eHealth services a security and privacy risk awareness survey," in *International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, C. Onwubiko and T. Owens (eds.), London, United Kingdom, pp. 1–4.
- Bem, D. J. 1967. "Self-perception: An alternative interpretation of cognitive dissonance phenomena," *Psychological Review* (74:3), pp. 183–200.
- Bender, B., Fabian, B., Lessman, S., and Haupt, J. 2016. "E-Mail Tracking: Status Quo and Novel Countermeasures," in *Proceedings of the 37th International Conference on Information Systems*, B. Fitzgerald and J. Mooney (eds.), Dublin, Ireland.
- Bentler, P. M. 1990. "Comparative fit indexes in structural models," *Psychological Bulletin* (107:2), pp. 238–246.
- Berendt, B., Günther, O., and Spiekermann, S. 2005. "Privacy in e-commerce," *Communications of the ACM* (48:4), pp. 101–106.
- Bewick, V., Cheek, L., and Ball, J. 2005. "Statistics review 14: Logistic regression," *Critical Care* (9:1), p. 112.
- Biczók, G., and Chia, P. H. 2013. "Interdependent Privacy: Let Me Share Your Data," in *Financial cryptography and data security*, A.-R. Sadeghi (ed.), Berlin: Springer, pp. 338–353.
- Bodenhausen, G. V., Mussweiler, T., Gabriel, S., and Moreno, K. N. 2001. "Affective influences on stereotyping and intergroup relations," in *Handbook of affect and social cognition*, Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers, pp. 319–343.
- Bollen, K. A. 1989. *Structural equations with latent variables*, New York: Wiley.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users

- Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors,” *MIS Quarterly* (39:4), pp. 837–864.
- Brace, I. 2014. *Questionnaire design: How to plan, structure and write survey material for effective market research*, London, Philadelphia: Kogan Page.
- Brakemeier, H., Widjaja, T., and Peter Buxmann 2016. “Calculating with different goals in mind - The moderating role of the regulatory focus in the privacy calculus,” in *Proceedings of the 24th European Conference on Information Systems*, Istanbul, Turkey.
- Brandimarte, L., Acquisti, A., and Loewenstein, G. 2013. “Misplaced Confidences,” *Social Psychological and Personality Science* (4:3), pp. 340–347.
- Brecht, F., Fabian, B., Kunz, S., and Müller, S. 2019. “Are you willing to wait longer for Internet,” in *Proceedings of the 19th European Conference on Information Systems*, Helsinki, Finland.
- Broota, K. D. 1989. *Experimental design in behavioural research*, New York: Wiley.
- Brown, K. W., and Ryan, R. M. 2003. “The benefits of being present: Mindfulness and its role in psychological well-being,” *Journal of Personality and Social Psychology* (84:4), pp. 822–848.
- Brown, K. W., Weinstein, N., and Creswell, J. D. 2012. “Trait mindfulness modulates neuroendocrine and affective responses to social evaluative threat,” *Psychoneuroendocrinology* (37:12), pp. 2037–2041.
- Brunet, N. 2017. *OMC Releases State of Email Tracking Report*.
<http://www.prweb.com/releases/2017/06/prweb14427071.htm>. Accessed 6 September 2017.
- Buckel, T., and Thiesse, F. 2013. “Predicting The Disclosure of Personal Information on Social Networks: An Empirical Investigation,” in *11th International Conference on Wirtschaftsinformatik*, R. Alt and B. Franczyk (eds.), Leipzig, Germany.
- Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. “Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook,” in *Proceedings of the 31st International Conference on Information Systems*, M. Lacity, S. March and F. Niederman (eds.), St. Louis, USA.
- Campbell, J. E., and Carlson, M. 2002. “Panopticon.com: Online Surveillance and the Commodification of Privacy,” *Journal of Broadcasting & Electronic Media* (46:4), pp. 586–606.
- Campbell, J. L., Quincy, C., Osserman, J., and Pedersen, O. K. 2013. “Coding In-depth Semistructured Interviews,” *Sociological Methods & Research* (42:3), pp. 294–320.
- Carnegie, T. A. M., and Abell, J. 2009. “Information, Architecture, and Hybridity: The Changing Discourse of the Public Library,” *Technical Communication Quarterly* (18:3), pp. 242–258.
- Cavusoglu, H., Phan, T. Q., Cavusoglu, H., and Airoidi, E. M. 2016. “Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook,” *Information Systems Research* (27:4), pp. 848–879.
- Chellappa, R., and Sin, R. 2005. “Personalization versus Privacy: An Empirical Examination of the Online Consumer’s Dilemma,” *Information Technology and Management* (6:2-3), pp. 181–202.
- Chen, W., and Hirschheim, R. 2004. “A paradigmatic and methodological examination of information systems research from 1991 to 2001,” *Information Systems Journal* (14:3), pp. 197–235.
- Chen, Y., and Zahedi, F. M. 2016. “Individuals internet security perceptions and behaviors: Polycontextual contrasts between the united states and china,” *MIS Quarterly* (40:1), 205-A12.
- Child, J. T., and Petronio, S. 2011. “Unpacking the Paradoxes of Privacy in CMC Relationships: The Challenges of Blogging and Relational Communication on the Internet,” in *Computer-Mediated Communication in Personal Relationships*, K. B. Wright and L. M. Webb (eds.): Peter Lang US.
- Chin, W. W. 1998. “The partial least squares approach to structural equation modeling,” in *Modern methods for Business Research*, Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295–336.
- Chin, W. W., Thatcher, J. B., and Wright, R. T. 2012. “Assessing common method bias: Problems with the ULMC technique,” *MIS Quarterly* (36:3), pp. 1003–1019.
- Choi, B., Wu, Y., Yu, J., and Land, L. 2018. “Love at First Sight: The Interplay Between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management,” *Journal of the Association for Information Systems* (19:3), pp. 124–151.
- Choi, B. C.F., Jiang, Z., Ramesh, B., and Dong, Y. 2015. “Privacy Tradeoff and Social Application Usage,” in *48th Hawaii International Conference on System Sciences (HICSS)*, HI, USA, pp. 304–313.
- Cialdini, R. B. 2010. *Influence: Science and practice*, Boston, Mass.: Pearson.

- Cichy, P., Salge, T.-O., and Kohli, R. 2014. "Extending the Privacy Calculus: The Role of Psychological Ownership," in *Proceedings of the 35th International Conference on Information Systems*, E. Karahanna, A. Srinivasan and B. Tan (eds.), Auckland, New Zealand.
- Clarke, R. 1999. "Internet privacy concerns confirm the case for intervention," *Communications of the Association for Information Systems* (42:2), pp. 60–67.
- Cohen, J. 1988. *Statistical power analysis for the behavioral sciences*, Hillsdale, N.J.: L. Erlbaum Associates.
- Cohen-Almagor, R. 2013. "Internet History," in *Moral, ethical, and social dilemmas in the age of technology: Theories and practice*, R. Luppigini (ed.), Hershey, Pa.: IGI Global (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA), pp. 19–39.
- Coppola, R., and Morisio, M. 2016. "Connected Car," *ACM Computing Surveys* (49:3), pp. 1–36.
- Corbin, J. M., and Strauss, A. 1990. "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative Sociology* (13:1), pp. 3–21.
- Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation: Organization Science," *Organization Science* (10:1), pp. 104–115.
- Dane, E. 2011. "Paying Attention to Mindfulness and Its Effects on Task Performance in the Workplace," *Journal of Management* (37:4), pp. 997–1018.
- Davies, S. G. 1997. "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: The New Landscape*, P. E. Agre and M. Rotenberg (eds.), Cambridge, MA, USA: MIT Press, pp. 143–165.
- Derlega, V. J. 1993. *Self-disclosure*, Newbury Park: Sage Publ.
- Dimond, J. P., Fiesler, C., and Bruckman, A. S. 2011. "Domestic violence and information communication technologies," *Interacting with Computers* (23:5), pp. 413–421.
- Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy calculus model in e-commerce – a study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389–402.
- Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61–80.
- Dinev, T., Hart, P., and Mullen, M. R. 2008. "Internet privacy concerns and beliefs about government surveillance – An empirical investigation," *The Journal of Strategic Information Systems* (17:3), pp. 214–233.
- Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* (26:4), pp. 636–655.
- Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems* (22:3), pp. 295–316.
- Drost, E. A. 2011. "Validity and Reliability in Social Science Research," *Education Research and Perspectives* (38:1).
- Elhiber, M. H. A., and Abraham, A. 2013. "Access Patterns in Web Log Data: A Review," *Journal of Network and Innovative Computing* (1), pp. 348–355.
- Englehardt, S., Han, J., and Narayanan, A. 2018. "I never signed up for this!: Privacy implications of email tracking," *Proceedings on Privacy Enhancing Technologies* (2018:1).
- Epel, E., Daubenmier, J., Moskowitz, J. T., Folkman, S., and Blackburn, E. 2009. "Can meditation slow rate of cellular aging? Cognitive stress, mindfulness, and telomeres," *Annals of the New York Academy of Sciences* (1172:1), pp. 34–53.
- Ermakova, T., Fabian, B., Bender, B., and Klimek, K. 2018. "Web Tracking – A Literature Review on the State of Research," in *Hawaii International Conference on System Sciences 2018 (HICSS-51)*, T. Bui (ed.), Hilton Waikoloa Village, Hawaii.
- Ernst, C.-P. H., Pfeiffer, J., and Rothlauf, F. 2015. "Privacy Protecting Behavior in Social Network Sites," in *21st Americas Conference on Information Systems*, Puerto Rico, USA.
- Eysenck, H. J., and Eysenck, M. W. 1985. *Personality and individual differences: A natural science approach*, New York: Plenum Press.
- Fabian, B., Bender, B., and Weimann, L. 2015. "E-Mail Tracking in Online Marketing - Methods, Detection, and Usage," in *Proceedings of the 12th International Conference on*

- Wirtschaftsinformatik*, O. Thomas and F. Teuteberg (eds.), Osnabrück, Germany, pp. 1100–1114.
- Farrell, L., DiTunnariello, N., and Pearson, J. 2014. “The Relationship between Spirituality and Family Privacy,” *Journal of Communication, Speech, and Theatre Association of North Dakota* (26), pp. 14–26.
- Fazio, R. H., and Roskos-Ewoldsen, D. R. 2005. “Acting as We Feel: When and How Attitudes Guide Behavior,” in *Persuasion: Psychological insights and perspectives*, 2nd ed, T. C. B. M. C. Green (ed.), Thousand Oaks, CA, US: SAGE Publications, Inc, pp. 41–62.
- Feifel, H., and Strack, S. 1989. “Coping with conflict situations: Middle-aged and elderly men,” *Psychology and Aging* (4:1), pp. 26–33.
- Finlayson, R., and Cheriton, D. 1987. “Log files: an extended file service exploiting write-once storage,” *ACM SIGOPS Operating Systems Review* (21:5), pp. 139–148.
- Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research*, Reading, Mass: Addison-Wesley Pub. Co.
- Fishbein, M., and Ajzen, I. 2010. *Predicting and changing behavior: The reasoned action approach*, New York: Psychology Press [u.a.].
- Fiske, D. W. 1982. “Convergent-discriminant validation in measurements and research strategies,” *New Directions for Methodology of Social & Behavioral Science* (12), pp. 77–92.
- Flanagan, J. C. 1954. “The critical incident technique,” *Psychological Bulletin* (51:4), pp. 327–358.
- Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. “A meta-analysis of research on protection motivation theory,” *Journal of applied social psychology* (30:2), pp. 407–429.
- Fornell, C., and Larcker, D. F. 1981. “Evaluating structural equation models with unobservable variables and measurement error,” *Journal of Marketing Research* (18:1), pp. 39–50.
- Forte, A., Larco, V., and Bruckman, A. 2009. “Decentralization in Wikipedia governance,” *Journal of Management Information Systems* (26:1), pp. 49–72.
- Frederick, S. 2005. “Cognitive Reflection and Decision Making,” *Journal of Economic Perspectives* (19:4), pp. 25–42.
- Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., and Dell, N. 2017. “Digital Technologies and Intimate Partner Violence,” *Proceedings of the ACM on Human-Computer Interaction* (1), pp. 1–22.
- Furnham, A., and Boo, H. C. 2011. “A literature review of the anchoring effect,” *The Journal of Socio-Economics* (40:1), pp. 35–42.
- Gaines, B. J., Kuklinski, J. H., and Quirk, P. J. 2007. “The Logic of the Survey Experiment Reexamined,” *Political Analysis* (15:1), pp. 1–20.
- Garland, E. L., Gaylord, S. A., and Fredrickson, B. L. 2011. “Positive Reappraisal Mediates the Stress-Reductive Effects of Mindfulness: An Upward Spiral Process,” *Mindfulness* (2:1), pp. 59–67.
- Garrison, D. R., Cleveland-Innes, M., Koole, M., and Kappelman, J. 2006. “Revisiting methodological issues in transcript analysis: Negotiated coding and reliability,” *The Internet and Higher Education* (9:1), pp. 1–8.
- Gidra, M. 2013. *Edward Snowden and the NSA files – timeline*.
<http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>. Accessed 9 February 2016.
- Granovetter, M. S. 1973. “The Strength of Weak Ties,” *American journal of sociology* (78:6), pp. 1360–1380.
- Grant, K. B. 2017. *Identity theft, fraud cost consumers more than \$16 billion*.
<https://www.cnn.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html>. Accessed 13 November 2019.
- Guo, K. H., and Yu, X. 2020. “The anonymous online self: Toward an understanding of the tension between discipline and online anonymity,” *Information Systems Journal* (30:1), pp. 48–69.
- Hair, J. F. 2010. *Multivariate data analysis: A global perspective*, Upper Saddle River: Prentice Hall.
- Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. 2014. *Multivariate data analysis*, Harlow, Essex: Pearson.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: Sage.
- Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. “When to use and how to report the

- results of PLS-SEM,” *European Business Review* (31:1), pp. 2–24.
- Hampton, K., Goulet, L. S., Marlow, C., and Rainie, L. 2012. *Why most Facebook users get more than they give*. <http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give/>. Accessed 25 October 2016.
- Harrison, G. W., and List, J. A. 2004. “Field Experiments,” *Journal of Economic Literature* (42:4), pp. 1009–1055.
- Harrison, R., and Wells, M. 2000. *A Meta-analysis of Multidisciplinary Research*, pp. 1–15.
- Haynes, S. N., Richard, D. C. S., and Kubany, E. S. 1995. “Content validity in psychological assessment: A functional approach to concepts and methods,” *Psychological Assessment* (7:3), pp. 238–247.
- Heirman, W., Walrave, M., and Ponnet, K. 2013. “Predicting adolescents' disclosure of personal information in exchange for commercial incentives: an application of an extended theory of planned behavior,” *Cyberpsychology, behavior and social networking* (16:2), pp. 81–87.
- Henseler, J., Ringle, C. M., and Sarstedt, M. 2014. “A new criterion for assessing discriminant validity in variance-based structural equation modeling,” *Journal of the Academy of Marketing Science* (43:1), pp. 1–21.
- Hilbert, M., and López, P. 2011. “The World’s Technological Capacity to Store, Communicate, and Compute Information,” *Science* (332:6025), pp. 60–65.
- Hoffmann, C. P., Lutz, C., and Ranzini, G. 2016. “Privacy cynicism: A new approach to the privacy paradox,” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* (10:4).
- Hong, W., and Thong, J. 2013. “Internet privacy concerns: An integrated conceptualization and four empirical studies,” *MIS Quarterly* (37:1), pp. 275–298.
- Howard, P. N., Ganesh, B., and Liotsiou, D. 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf>. Accessed 15 November 2019.
- Hu, L.-T., and Bentler, P. M. 1999. “Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives,” *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1–55.
- Hui, K.-L., Teo, H.-H., and Lee, S.-Y. T. 2007. “The value of privacy assurance: An exploratory field experiment,” *MIS Quarterly* (31:1), pp. 19–33.
- Identity Theft Resource Center 2016. *Identity Theft: The Aftermath 2016™*. https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf. Accessed 13 November 2019.
- Jetzek, T., Avital, M., and Bjørn-Andersen, N. 2013. “Generating value from open government data,” in *Proceedings of the 34th International Conference on Information Systems*, R. Baskerville and M. Chau (eds.), Milan, Italy, Milan, Italy.
- Joinson, A., Reips, U.-D., Buchanan, T., and Schofield, C. B. P. 2010. “Privacy, Trust, and Self-Disclosure Online,” *Human-Computer Interaction* (25:1), pp. 1–24.
- Jost, J. T., Banaji, M. R., and Nosek, B. A. 2004. “A Decade of System Justification Theory: Accumulated Evidence of Conscious and Unconscious Bolstering of the Status Quo,” *Political Psychology* (25:6), pp. 881–919.
- Jost, J. T., and Hunyady, O. 2005. “Antecedents and Consequences of System-Justifying Ideologies,” *Current Directions in Psychological Science* (14:5), pp. 260–265.
- Junglas, I. A., Johnson, N. A., and Spitzmüller, C. 2008. “An empirical study in the context of location-based services,” *European Journal of Information Systems* (17:4), pp. 387–402.
- Kahneman, D., and Frederick, S. 2002. “Representativeness revisited: Attribute substitution in intuitive judgment,” in *Heuristics and biases: The psychology of intuitive judgment*, New York, NY, US: Cambridge University Press, pp. 49–81.
- Kahneman, D., Slovic, P., and Tversky, A. 1982. *Judgment under uncertainty: Heuristics and biases*, Cambridge: Cambridge Univ. Press.
- Karahanna, E., Benbasat, I., Bapna, R., and Rai, A. 2018. “Editor's Comments: Opportunities and Challenges for Different Types of Online Experiments Motivation for and Objectives of the Editorial,” *MIS Quarterly* (4:42), pp. iii–x.
- Karwatzki, S., Trenz, M., Tuunainen, V. K., and Veit, D. 2017. “Adverse consequences of access to individuals’ information: An analysis of perceptions and the scope of organisational influence,” *European Journal of Information Systems* (26:6), pp. 688–715.

- Karwatzki, S., Trenz, M., and Veit, D. 2018. "Yes, Firms Have my Data But What Does it Matter? Measuring Privacy Risks," in *Proceedings of the 26th European Conference on Information Systems*, P. Bednar, U. Frank and K. Kautz (eds.), Portsmouth, UK.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus," *Information Systems Journal* (25:6), pp. 607–635.
- Keith, M., Thompson, S., Hale, J., and Greer, C. 2012. "Examining the Rationality of Location Data Disclosure through Mobile Devices," in *Proceedings of the 33rd International Conference on Information Systems*, M.-H. Huang, G. Piccoli and V. Sambamurthy (eds.), Orlando, FL.
- Keith, M. J., Babb, J., Lowry, P. B., Furner, C., and Abdullat, A. 2015. "The Role of Mobile-Computing Self-Efficacy in Consumer Information Disclosure," *Information Systems Journal* (25:6), pp. 637–667.
- Keith, M. J., Babb, J. S., JR., Furner, C. P., and Abdullat, A. 2010. "Privacy assurance and network effects in the adoption of location based services: An iPhone experiment," in *Proceedings of the 31st International Conference on Information Systems*, M. Lacity, S. March and F. Niederman (eds.), St. Louis, USA.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior," *International Journal of Human-Computer Studies* (71:12), pp. 1163–1173.
- Kenny, D. A. 2015. *Moderator Variables*. <http://www.davidakenny.net/cm/moderation.htm>. Accessed 27 October 2015.
- Kokolakis, S. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* (64), pp. 122–134.
- Kolfschoten, G. L., Niederman, F., Briggs, R. O., and Vreede, G.-J. de 2012. "Facilitation roles and responsibilities for sustained collaboration support in organizations," *Journal of Management Information Systems* (28:4), pp. 129–162.
- Kordzadeh, N., and Warren, J. 2017. "Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment," *Journal of the Association for Information Systems* (18:1), pp. 45–81.
- Krasnova, H., and Veltri, N. F. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," in *43rd Hawaii International Conference on System Sciences (2010)*, R. Sprague and S. Laney (eds.), Koloa, Kauai, Hawaii, pp. 1–10.
- Krasnova, H., and Veltri, N. F. 2011. "Behind the Curtains of Privacy Calculus on Social Networking Sites: The Study of Germany and the USA," in *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, A. Bernstein and G. Schwabe (eds.), Zurich, Switzerland.
- Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering* (4:3), pp. 127–135.
- Kwong, M. 2015. *Smart devices think you're 'too lazy' to opt out of privacy defaults*. <http://www.cbc.ca/news/technology/smart-devices-think-you-re-too-lazy-to-opt-out-of-privacy-defaults-1.2957114>. Accessed 10 August 2015.
- Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), pp. 159–174.
- Lane, K., and Levy, S. J. 2019. "Marketing in the Digital Age: A Moveable Feast of Information," in *Marketing in a digital world*, A. Rindfleisch and A. J. Malter (eds.), Bingley: Emerald Publishing, pp. 13–33.
- Lankton, N., and Tripp, J. 2013. "A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro Model," in *Proceedings of the Nineteenth Americas Conference on Information Systems*, J. Shim, Y. Hwang and S. Petter (eds.), Chicago, Illinois, pp. 1–12.
- Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of social issues* (33:3), pp. 22–42.
- Li, H., Sarathy, R., and Xu, H. 2011a. "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems* (51:3), pp. 434–445.
- Li, T., and Unger, T. 2012. "Willing to pay for quality personalization?: Trade-off between quality and

- privacy,” *European Journal of Information Systems* (21:6), pp. 621–642.
- Li, X.-B., and Sarkar, S. 2010. “Data Clustering and Micro-Perturbation for Privacy-Preserving Data Sharing and Analysis,” in *Proceedings of the 31st International Conference on Information Systems*, M. Lacity, S. March and F. Niederman (eds.), St. Louis, USA.
- Li, Y. 2011b. “Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework,” *Communications of the Association for Information Systems* (28).
- Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. “Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management,” *MIS Quarterly* (31:1), pp. 59–87.
- Lin, S., and Armstrong, D. 2019. “Beyond Information: The Role of Territory in Privacy Management Behavior on Social Networking Sites,” *Journal of the Association for Information Systems* (20:4).
- Lowry, P. B., D’Arcy, J., Hammer, B., and Moody, G. D. 2016. ““Cargo Cult” science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels,” *Journal of Strategic Information Systems* (25:3), pp. 232–240.
- Lukka, V., and Paul, J. T.J. 2014. “Attitudes toward Facebook advertising,” *Journal of Management and Marketing Research* (14:4), pp. 1–26.
- Lwin, M., Wirtz, J., and Williams, J. D. 2007. “Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective,” *Journal of the Academy of Marketing Science* (35:4), pp. 572–585.
- Madden, M. 2014. *Public Perceptions of Privacy and Security in the Post-Snowden Era*.
<https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>. Accessed 29 October 2019.
- Maier, C., Laumer, S., and Eckhardt, A. 2015. “Information technology as daily stressor: pinning down the causes of burnout,” *Journal of Business Economics* (85:4), pp. 349–387.
- Maier, C., Wirth, J., Laumer, S., and Weitzel, T. 2017. “Personality and Technostress: Theorizing the Influence of IT Mindfulness,” in *Thirty Eighth International Conference on Information Systems*, Y. J. Kim, R. Agarwal and J. K. Lee (eds.), South Korea.
- Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. “Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model: Information Systems Research,” *Information Systems Research* (15:4), pp. 336–355.
- Margulis, S. T. 1977. “Conceptions of Privacy: Current Status and Next Steps,” *Journal of Social Issues* (33:3), pp. 5–21.
- Marr, B. 2018. *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*. <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/>. Accessed 28 March 2019.
- Matthews, T., O’Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., Manthorne, C., Churchill, E. F., and Consolvo, S. 2017. “Stories from Survivors,” in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, G. Mark, S. Fussell, C. Lampe, m.c. schraefel, J. P. Hourcade, C. Appert and D. Wigdor (eds.), Denver, Colorado, USA, New York, New York, USA, pp. 2189–2201.
- McAskil, E. 2015. *After Charlie Hebdo attack, do spy agencies need more powers?*
<https://www.theguardian.com/uk-news/2015/jan/09/do-spy-agencies-need-more-surveillance-powers>. Accessed 1 June 2017.
- McConnell, A. R., and Rydell, R. J. 2014. “The systems of evaluation model: A Dual-systems approach to attitudes,” in *Dual-process theories of the social mind*, New York, NY, US: The Guilford Press, pp. 204–218.
- McGrath, J. E., Martin, J., and Kulka, R. A. 1982. *Judgment calls in research: By Joseph E. McGrath, Joanne Martin, and Richard A. Kulka*, Beverly Hills: Sage Publications.
- Merchant, B. 2017. *How email open tracking quietly took over the web*.
<https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/>. Accessed 22 January 2018.
- Milne, G. R. 1997. “Consumer Participation in Mailing Lists: A Field Experiment,” *Journal of Public Policy & Marketing* (16:2), pp. 298–309.
- Milne, G. R. 2000a. “Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue,” *Journal of Public Policy & Marketing* (19:1), pp. 1–6.

- Milne, G. R., and Gordon, M. E. 1993. "Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework," *Journal of Public Policy & Marketing* (12:2), pp. 206–215.
- Milne, S., Sheeran, P., and Orbell, S. 2000b. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of applied social psychology* (30:1), pp. 106–143.
- Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., and Brantingham, P. J. 2015. "Randomized Controlled Field Trials of Predictive Policing," *Journal of the American Statistical Association* (110:512), pp. 1399–1411.
- Moon, Y. 2000. "Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers," *Journal of consumer research* (26:4), pp. 323–339.
- Moore, G. C., and Benbasat, I. 1991. "Development of an instrument to measure the perceptions of adopting an information technology innovation," *Information Systems Research* (2:3), pp. 192–222.
- Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., and Wang, S. 2011. "Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information," *Journal of Service Research* (15:1), pp. 76–98.
- Mousavizadeh, M., and Kim, D. J. 2015. "A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- Mussweiler, T., and Strack, F. 1999. "Hypothesis-Consistent Testing and Semantic Priming in the Anchoring Paradigm: A Selective Accessibility Model," *Journal of Experimental Social Psychology* (35:2), pp. 136–164.
- Nagelkerke, N. J. D. 1991. "A Note on a General Definition of the Coefficient of Determination," *Biometrika* (78:3), pp. 691–692.
- Nahm, A. Y., Rao, S. S., Solis-Galvan, L. E., and Ragu-Nathan, T. S. 2002. "The Q-sort method: assessing reliability and construct validity of questionnaire items at a pre-testing stage," *Journal of Modern Applied Statistical Methods* (1:1), p. 15.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.
- Nunnally, J. 1978. *Psychometric theory*: New York: McGraw-Hill.
- Okoli, C., and Schabram, K. 2010. "A Guide to Conducting a Systematic Literature Review," *Working Papers on Information Systems* (10:26), pp. 1–46.
- Onwuegbuzie, A. J., and Frels, R. 2016. *7 steps to a comprehensive literature review: A multimodal & cultural approach*, Los Angeles, London, New Delhi, Singapore, Washinton DC: Sage.
- Orlikowski, W. J., and Baroudi, J. J. 1991. "Studying Information Technology in Organizations: Research Approaches and Assumptions," *Information Systems Research* (2:1), pp. 1–28.
- Paré, G., Trudel, M.-C., Jaana, M., and Kitsiou, S. 2015. "Synthesizing information systems knowledge A typology of literature reviews," *Information & Management* (52:2), pp. 183–199.
- Paunonen, S. V., and Ashton, M. C. 2001. "Big Five factors and facets and the prediction of behavior," *Journal of Personality and Social Psychology* (81:3), pp. 524–539.
- Pavlou, P. A. 2011. "State of the information privacy literature: Where are we now and where should we go?" *MIS Quarterly* (35:4), pp. 977–988.
- Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: a Principal-Agent Perspective," *MIS Quarterly* (31:1), pp. 105–136.
- Peng, C.-Y. J., Lee, K. L., and Ingersoll, G. M. 2002. "An Introduction to Logistic Regression Analysis and Reporting," *The Journal of Educational Research* (96:1), pp. 3–14.
- Penney, J. 2016. "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal* (31:1), pp. 117–182.
- Perl, M. W. 2003. "It's Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft," *The Journal of Criminal Law and Criminology* (1973-) (94:1), p. 169.
- Petronio, S. 2010. "Communication privacy management theory: What do we know about family privacy regulation?" *Journal of Family Theory & Review* (2:3), pp. 175–196.
- Petronio, S. 2013. "Brief Status Report on Communication Privacy Management Theory," *Journal of Family Communication* (13:1), pp. 6–14.

- Petronio, S. 2015. "Communication Privacy Management Theory," in *The International Encyclopedia of Interpersonal Communication*, C. R. Berger, M. E. Roloff, S. R. Wilson, J. P. Dillard, J. Caughlin and D. Solomon (eds.), Hoboken, NJ, USA: John Wiley & Sons, Inc, pp. 1–9.
- Petronio, S. S., and Altman, I. 2002. *Boundaries of privacy: Dialectics of disclosure*, Albany, NY: State University of New York Press.
- Petty, R. E., and Wegener, D. T. 1998. "Attitude change: Multiple roles for persuasion variables," in *The handbook of social psychology*, Vols. 1-2, 4th ed, New York, NY, US: McGraw-Hill, pp. 323–390.
- PeWResearchCenter 2013. *Few See Adequate Limits on NSA Surveillance Program*.
<http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/>.
 Accessed 4 May 2017.
- Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing* (19:1), pp. 27–41.
- Pierce, J. L., Kostova, T., and Dirks, K. T. 2001. "Toward a Theory of Psychological Ownership in Organizations," *Academy of Management Review* (26:2), pp. 298–310.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), p. 879.
- Politou, E., Alepis, E., and Patsakis, C. 2018. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *Journal of Cybersecurity* (4:1), p. 1.
- Poremba, S. M. 2012. *How Friends Spoil Your Social-Media Privacy*.
http://www.nbcnews.com/id/47711709/ns/technology_and_science-security/t/how-friends-spoil-your-social-media-privacy/#.WdTU28hJa70. Accessed 9 October 2017.
- Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities," *European Journal of Information Systems* (19:2), pp. 181–195.
- Posey, C., Raja, U., Crossler, R. E., and Burns, A. J. 2017. "Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA," *Eur J Inf Syst* (26:6), pp. 585–604.
- Preacher, K. J., and Hayes, A. F. 2008. "Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models," *Behavior research methods* (40:3), pp. 879–891.
- Privacy International 2017. *Mass Surveillance*. <https://www.privacyinternational.org/node/52>.
 Accessed 21 April 2017.
- Pu, Y., and Grossklags, J. 2015. "Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- PWC Virginia. *How Burglars Use Social Media*.
<https://www.pwcgov.org/government/dept/police/Pages/How-Burglars-Use-Social-Media.aspx>.
 Accessed 12 November 2019.
- Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., and Qiang Tu 2008. "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," *Information Systems Research* (19:4), pp. 417–433.
- Rasch 2014. *Quantitative Methoden 1*, Berlin, Heidelberg: Springer.
- Recker, J. 2013. *Scientific research in information systems: A beginner's guide*, Berlin, Heidelberg: Springer.
- Reddick, C. G., Chatfield, A. T., and Jaramillo, P. A. 2015. "Public opinion on National Security Agency surveillance programs: A multi-method approach," *Government Information Quarterly* (32:2), pp. 129–141.
- Rigdon, E. E. 2012. "Rethinking Partial Least Squares Path Modeling: In Praise of Simple Methods," *Long Range Planning* (45:5-6), pp. 341–358.
- Rogers, R. W., and Prentice-Dunn, S. 1997. "Protection motivation theory," in *Handbook of health behavior research 1: Personal and social determinants*, New York, NY, US: Plenum Press, pp. 113–132.
- Sagiroglu, S., and Sinanc, D. 2013. "Big data: A review," in *International Conference on Collaboration Technologies and Systems*, G. C. Fox and S. M. Waleed (eds.), San Diego, CA,

- USA, pp. 42–47.
- Sanchez-Rola, I., Ugarte-Pedrero, X., Santos, I., and Bringas, P. G. 2017. “The web is watching you: A comprehensive review of web-tracking techniques and countermeasures,” *Logic Journal of IGPL* (25:1), pp. 18–29.
- Sarathy, R., and Li, H. 2007. “Understanding Online Information Disclosure As a Privacy Calculus Adjusted by Exchange Fairness,” in *Twenty Eighth International Conference on Information Systems*, B. Gallupe and A. Pinsonneault (eds.), Montreal, Quebec, Canada.
- Sarker, S., Xiao Xiao, and Beaulieu, T. 2013. “Qualitative Studies in Information Systems: A Critical Review and Some Guiding Principles,” *MIS Quarterly* (37:4), pp. 3–18.
- Schreiner, M., and Hess, T. 2015. “Examining the role of privacy in virtual migration: the case of WhatsApp and Threema,” in *Proceedings of the 23rd European Conference on Information Systems*, J. Becker, J. vom Brocke and M. de Marco (eds.), Münster, Germany.
- Schryen, G. 2015. “Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research,” *Communications of the Association for Information Systems* (37:12), pp. 286–325.
- Schwaig, K. S., Kane, G. C., and Storey, V. C. 2006. “Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures?” *Information & Management* (43:7), pp. 805–820.
- Schwarz, A., Rizzuto, T., Carraher-Wolverton, C., Roldan, J. L., and Barrera-Barrera, R. 2017. “Examining the Impact and Detection of the “Urban Legend” of Common Method Bias,” *ACM Sigmis Database* (48:1), pp. 93–119.
- Shapiro, S. L., Brown, K. W., Thoresen, C., and Plante, T. G. 2011. “The moderation of Mindfulness-based stress reduction effects by trait mindfulness: results from a randomized controlled trial,” *Journal of clinical psychology* (67:3), pp. 267–277.
- Sheng, H., Nah, F. F.-H., and Siau, K. 2008. “An Experimental Study on Ubiquitous commerce Adoption: Impact of Personalization and Privacy Concerns,” *Journal of the Association for Information Systems* (9:6), pp. 344–376.
- Shin, K. G., Ju, X., Chen, Z., and Hu, X. 2012. “Privacy protection for users of location-based services,” *IEEE Wireless Communications* (19:1), pp. 30–39.
- Siner, E. 2014. *The Internet Flexes Political Muscle With Anti-NSA Protest*.
<https://www.npr.org/sections/alltechconsidered/2014/02/10/274901562/the-internet-flexes-political-muscle-with-anti-nsa-protest?t=1531821946312>. Accessed 17 July 2018.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. “Information Privacy: Measuring Individuals’ Concerns About Organizational Practices,” *MIS Quarterly* (20:2), pp. 167–196.
- Smith, J. H., Dinev, T., and Xu, H. 2011. “Information privacy research: An interdisciplinary review,” *MIS Quarterly* (35:4), pp. 980–1015.
- Smith, M. J., Carayon, P., Sanders, K. J., Lim, S.-Y., and LeGrande, D. 1992. “Employee stress and health complaints in jobs with and without electronic performance monitoring,” *Applied Ergonomics* (23:1), pp. 17–27.
- Solove, D. J. 2004. *The digital person: Technology and privacy in the information age*, New York: New York University Press.
- Solove, D. J. 2006. “A Taxonomy of Privacy,” *University of Pennsylvania Law Review* (154:3), pp. 477–564.
- Solove, D. J. 2007. “I’ve got nothing to hide and other misunderstandings of privacy,” *San Diego L. Rev.* (44).
- Solove, D. J. 2011. “Why privacy matters even if you have ‘nothing to hide’,” *Chronicle of Higher Education* (15).
- Son, J.-Y., and Kim, S. S. 2008. “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model,” *MIS Quarterly* (32:3), pp. 503–529.
- Spencer, L. 2014. *Laziness at the expense of privacy and freedom: John McAfee*.
<http://www.zdnet.com/article/laziness-at-the-expense-of-privacy-and-freedom-john-mcafee/>. Accessed 10 August 2015.
- Spiekermann, S., Grossklags, J., and Berendt, B. 2001. “E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior,” in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, M. Wellman and Y. Shoham (eds.), Tampa, FL, USA, pp. 38–47.
- Stanton, J. M., and Stam, K. R. 2002. “Information technology, privacy, and power within

- organizations: A view from boundary theory and social exchange perspectives,” *Surveillance & Society* (1:2), pp. 152–190.
- statista.com 2015a. *Felt ability to correct, change or delete personal information shared online in the European Union (EU-28) as of March 2015, by level of control**. <https://www.statista.com/statistics/533842/level-of-control-over-personal-data-provided-online-in-the-european-union/>. Accessed 3 April 2019.
- statista.com 2015b. *Impacts of accidental confidential information disclosure worldwide 2015*. <https://www.statista.com/statistics/463363/impacts-accidental-confidential-information-disclosure-worldwide/>. Accessed 29 October 2019.
- statista.com 2015c. *Leading actions taken by consumers due to online privacy concerns in Great Britain (GB) in January 2015 and December 2015*. <https://www.statista.com/statistics/507115/leading-actions-taken-due-to-online-privacy-concerns-in-great-britain-gb/>. Accessed 3 April 2019.
- statista.com 2018a. *Facebook usage changers over privacy concerns by adults in the United States as of April 2018*. <https://www.statista.com/statistics/972877/behavioral-changes-consumers-facebook-privacy-concerns-usa/>. Accessed 3 April 2019.
- statista.com 2018b. *Least common actions undertaken to protect data on the internet in Australia as of August 2018*. <https://www.statista.com/statistics/958030/australia-least-common-actions-taken-to-protect-data/>. Accessed 3 April 2019.
- statista.com 2018c. *Share of internet users in the United States who have been victim of online identity theft as of October 2018*. <https://www.statista.com/study/17352/online-privacy-statista-dossier/>. Accessed 29 October 2019.
- statista.com 2019a. *Global digital population as of October 2019*. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>. Accessed 17 December 2019.
- statista.com 2019b. *Media usage in an internet minute as of March 2019*. <https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/>. Accessed 17 December 2019.
- statista.com 2019c. *Share of internet users who are concerned about risks to their online privacy vs. their willingness to accept certain risks to their online privacy to make their life more convenient as of October 2018, by country*. <https://www.statista.com/statistics/1023952/global-opinion-concern-internet-privacy-risk-convenience/>. Accessed 29 October 2019.
- statista.com 2019d. *Smart speaker with intelligent personal assistant ownership rate among U.S. broadband households from 2017 to 2019*. <https://www.statista.com/statistics/791575/us-smart-speaker-household-ownership/>. Accessed 29 January 2020.
- Steelman, Z. R., Hammer, B. I., and Limayem, M. 2014. “Data Collection in the Digital Age: Innovative Alternatives to Student Samples,” *MIS Quarterly* (38:2), pp. 355–378.
- Stevens, J. 2017. *5 Online Privacy Mistakes that Could Cost You Your Job*. <https://www.glassdoor.com/blog/online-privacy-mistakes/>.
- Strauß, S. 2017. “A game of hide and seek? Unscrambling the trade-off between privacy and security: Discourses of privacy and security,” in *Surveillance, Privacy and Security*, M. Friedewald, J. P. Burgess, J. Čas, R. Bellanova and W. Peissl (eds.), Abingdon, Oxon, New York, NY : Routledge, 2017. |: Routledge.
- Sun, Y., Wang, N., Shen, X.-L., and 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), pp. 278–292.
- Sutanto, J., Palme, E., Chuan-Hoo Tan, and Chee Wei Phang 2013. “Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users,” *MIS Quarterly* (37:4), p. 1141.
- Tam, E.-C., Hui, K.-L., and Tan, B. 2002. “What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses,” in *Proceedings of the 23rd International Conference on Information Systems*, Barcelona, Spain.
- Thatcher, J., Wright, R., Sun, H., Zagenczyk, T., and Klein, R. 2018. “Mindfulness in Information Technology Use: Conceptual and Operational Definitions,” *MIS Quarterly* (42:3).
- Triandis, H. C. 1980. “Values, attitudes, and interpersonal behavior,” *Nebraska Symposium on Motivation* (27), pp. 195–259.

- Tversky, A., and Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases," *Science* (185:4157), pp. 1124–1131.
- van der Toorn, J., Feinberg, M., Jost, J. T., Kay, A. C., Tyler, T. R., Willer, R., and Wilmuth, C. 2015. "A Sense of Powerlessness Fosters System Justification: Implications for the Legitimation of Authority, Hierarchy, and Government," *Political Psychology* (36:1), pp. 93–110.
- van Eerde, W., and Thierry, H. 1996. "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* (81:5), pp. 575–586.
- Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User acceptance of information technology: toward a unified view," *MIS Quarterly* (27:3), pp. 425–478.
- vhb-jourqual 2016. *Teiltrating Wirtschaftsinformatik*. <http://vhbonline.org/en/service/jourqual/vhb-jourqual-3/teiltrating-wi/>. Accessed 2 January 2017.
- Vroom, V. H. 1964. *Work and motivation*, New York: Wiley.
- Wacks, R. 1989. *Personal Information: Privacy and the Law*, Oxford: Clarendon Press.
- Warren, S. D., and Brandeis, L. D. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), pp. 193–220.
- Watkins, E. R., Baeyens, C. B., and Read, R. 2009. "Concreteness training reduces dysphoria: Proof-of-principle for repeated cognitive bias modification in depression," *Journal of Abnormal Psychology* (118:1), pp. 55–64.
- Webster, J., and Watson, R. T. 2002. "Analyzing the past to prepare for the future: Writing a literature review," *Management Information Systems Quarterly* (26:2), pp. xiii–xxiii.
- Weiber, R., and Mülhhaus, D. 2014. *Strukturgleichungsmodellierung*, Berlin, Heidelberg: Springer Berlin Heidelberg.
- Weible, R. J. 1993. *Privacy and data: an empirical study of the influence of types of data and situational context upon privacy perceptions*. Doctoral Dissertation.
- Weijters, B., and Baumgartner, H. 2012. "Misresponse to Reversed and Negated Items in Surveys: A Review," *Journal of Marketing Research* (49:5), pp. 737–747.
- Weinstein, N., Brown, K. W., and Ryan, R. M. 2009. "A multi-method examination of the effects of mindfulness on stress attribution, coping, and emotional well-being," *Journal of research in personality* (43:3), pp. 374–385.
- Weitzel, T., Eckhardt, A., Laumer, S., Maier, C., von Stetten, A., Weinert, C., and Wirth, J. 2015a. "Bewerbungspraxis 2015 - Eine empirische Studie mit 7.000 Stellensuchenden und Karriereinteressierten im Internet," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Eckhardt, A., Laumer, S., Maier, C., von Stetten, A., Weinert, C., and Wirth, J. 2015b. "Recruiting Trends 2015 - Eine empirische Untersuchung mit den Top-1.000-Unternehmen aus Deutschland sowie den Top-300-Unternehmen aus den Branchen Finanzdienstleistung, Health Care und IT," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Eckhardt, A., Laumer, S., Maier, C., von Stetten, A., Weinert, C., and Wirth, J. 2015c. "Recruiting Trends im Mittelstand - Eine empirische Untersuchung mit 1.000 Unternehmen aus dem deutschen Mittelstand," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016a. "Active Sourcing und Social Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016b. "Best Practices und Big Failures - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016c. "Bewerbung der Zukunft - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016d. "Employer Branding und Personalmarketing - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016e. "Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016," , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016f. "Techniksprung in der Rekrutierung - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der

- Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017a. “Active Sourcing und Social Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017b. “Bewerbung der Zukunft - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017c. “Employer Branding und Personalmarketing - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017d. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017e. “Women in IT - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018a. “Digitalisierung der Personalgewinnung, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018b. “Employer Branding, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018c. “Mobile Recruiting, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018d. “Social Recruiting und Active Sourcing, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019a. “Digitalisierung und Zukunft der Arbeit - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019b. “Employer Branding - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019c. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019d. “Social Recruiting und Active Sourcing - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020a. “Digitalisierung und Zukunft der Arbeit - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020b. “Employer Branding - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020c. “Generation Z - die Arbeitnehmer von morgen - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020d. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020e. “Social Recruiting und Active Sourcing - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Westin, A. F. 1967. *Privacy and freedom*, New York: Atheneum.

- Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431–453.
- Wheeless, L. R. 1978. "A Follow-Up Study of the Relationships Among Trust, Disclosure, and Interpersonal Solidarity," *Human Communication Research* (4:2), pp. 143–157.
- Wheeless, L. R., and Grotz, J. 1976. "Conceptualization and Measurement of Reported Self-Disclosure," *Human Communication Research* (2:4), pp. 338–346.
- Wirth, J. 2018. "Dependent Variables in the Privacy-Related Field: A Descriptive Literature Review," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, T. Bui (ed.), Waikoloa Village, Hawaii, pp. 3658–3667.
- Wirth, J., and Maier, C. 2017. "The Influence of Resignation on the Privacy Calculus: A Research Approach," in *Pre-ICIS Workshop on Information Security and Privacy*, M. Curry and S. Goel (eds.), Seoul, South Korea.
- Wirth, J., Maier, C., and Laumer, S. 2015. "Influence of laziness on data disclosure: an empirical investigation," in *Twentieth DIGIT Workshop*, H. Sun, C. Hsu and R. T. Wright (eds.), Fort Worth, TX, USA.
- Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2017. "Understanding Privacy Threat Appraisal and Coping Appraisal through Mindfulness," in *Thirty Eighth International Conference on Information Systems*, Y. J. Kim, R. Agarwal and J. K. Lee (eds.), South Korea, pp. 1–11.
- Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2019. "Perceived information sensitivity and interdependent privacy protection: a quantitative study," *electronic markets* (29:3), pp. 359–378.
- Witte, K. 1992. "Putting the fear back into fear appeals: The extended parallel process model," *Communication Monographs* (59:4), pp. 329–349.
- Worsley, J. D., Wheatcroft, J. M., Short, E., and Corcoran, R. 2017. "Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses," *SAGE Open* (7:2), 215824401771029.
- Xu, H., Dinev, T., Smith, J., and Hart, P. 2011a. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798–824.
- Xu, H., Hao, S., Sari, A., and Wang, H. 2018. "Privacy Risk Assessment on Email Tracking," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Honolulu, HI.
- Xu, H., Luo, X., Carroll, J. M., and Rosson, M. B. 2011b. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems* (51:1), pp. 42–52.
- Xu, H., Teo, H.-H., Tan, Bernard C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135–173.
- Xu, Y., Tan, B., and Hui, K.-L. 2003. "Consumer Trust and Online Information Privacy," in *Twenty-Fourth International Conference on Information Systems*, J. Valacich and L. Jessup (eds.), Seattle, Washington.
- Yin, R. K. 2014. *Case study research: Design and methods*: SAGE Publications, Inc.
- Zheng, Z., Pavlou, P. A., and Gu, B. 2014. "Latent Growth Modeling for Information Systems: Theoretical Extensions and Practical Applications," *Information Systems Research* (25:3), pp. 547–568.



1.

Chapter I Literature Review on Privacy

Paper I

DEPENDENT VARIABLES IN THE PRIVACY-RELATED FIELD

A DESCRIPTIVE LITERATURE REVIEW

Jakob Wirth
University of Bamberg

Proceedings of the 51st Hawaii International Conference on System Sciences (2018), T. Bui (ed.),
Waikoloa Village, Hawaii
<http://hdl.handle.net/10125/50351>



Chapter II

Privacy Ownership

Paper II

JUSTIFICATION OF MASS SURVEILLANCE **A QUANTITATIVE STUDY**

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Proceedings of the 14th International Conference on Wirtschaftsinformatik (2019), T. Ludwig and V. Pipek (eds.), Siegen, Germany
<https://aisel.aisnet.org/wi2019/track11/papers/6/>

Paper III

THE INFLUENCE OF RESIGNATION ON THE PRIVACY CALCULUS IN THE CONTEXT OF SOCIAL NETWORKING SITES AN EMPIRICAL ANALYSIS

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Proceedings of the 26th European Conference on Information Systems (2018), P. Bednar, U. Frank and K. Kautz (eds.), Portsmouth, UK

https://aisel.aisnet.org/ecis2018_rp/161/

A decorative graphic consisting of three overlapping squares. The top-left square is light gray, the bottom-right square is a medium gray, and the central square is black with the white number '3.' inside.

3.

Chapter III Privacy Control

Paper IV

SUBJECTIVE NORM AND THE PRIVACY CALCULUS

EXPLAINING SELF-DISCLOSURE ON SOCIAL NETWORKING SITES

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Proceedings of the 27th European Conference on Information Systems (2019), P. Johannesson, P. Ågerfalk and R. Helms (eds.), Stockholm & Uppsala, Sweden
https://aisel.aisnet.org/ecis2019_rp/131/

Paper V

**LAZINESS AS AN EXPLANATION
FOR THE PRIVACY PARADOX
AN EMPIRICAL INVESTIGATION WITH MULTIPLE
SNAPSHOTS**

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Tim Weitzel

University of Bamberg

A prior version has been presented and discussed at the 20th DIGIT Workshop (2015), Fort Worth, TX, USA

LAZINESS AS AN EXPLANATION FOR THE PRIVACY PARADOX

AN EMPIRICAL INVESTIGATION WITH MULTIPLE SNAPSHOTS

Abstract

Purpose: “Smart devices think you're 'too lazy' to opt out of privacy defaults” was the headline of a recent news report indicating that individuals might be too lazy to stop disclosing their private information and therefore to protect their information privacy. In current privacy research, privacy concerns and self-disclosure are central constructs regarding protecting privacy. One might assume that being concerned about protecting privacy would lead individuals to disclose less personal information. However, past research has shown that despite high privacy concerns, individuals continue to disclose personal information, which is commonly referred to as the privacy paradox. This study introduces laziness as a personality trait in the privacy context, asking to what degree individual laziness influences privacy issues.

Design/methodology/approach: After conceptualizing, defining and operationalizing laziness, we analyzed information collected in an empirical study with multiple snapshots and evaluated the results through structural equation modeling.

Findings: The findings show that the privacy paradox holds true, yet, is influenced by the level of laziness. In particular, the privacy paradox applies to very lazy individuals but not to less lazy individuals.

Research limitations/implications: With these results one can better explain the privacy paradox and self-disclosure behavior.

Practical implications: One might implement regulatory measures that make it as easy as possible to protect privacy, for example by making default privacy threats illegal.

Originality/value: Based on a literature review, a clear research gap has been identified which is filled by this research study.

Keywords: laziness, privacy paradox, social networking sites, multiple snapshots, privacy concerns, personality

1 INTRODUCTION

Individuals are often concerned about their privacy but still disclose a huge amount of information, which is called the privacy paradox (Norberg et al. 2007). Research so far explains this by the privacy calculus, cognitive biases and irrational behavior (Acquisti and Grossklags 2003, 2005c; Dinev and Hart 2006; Grossklags and Acquisti 2007). However, there is still room for new theoretical perspectives (Kokolakis 2017), as among others, individual differences, such as personality traits, predetermine whether beliefs result in user behavior (Sheeran 2002). This means the way how privacy concerns shape individuals' disclosure behavior, is aligned with ones' personality traits such that personality traits might explain the privacy paradox. However, there has been little research into the role of personality traits in this context (Smith et al. 2011) and scholars have called for more research into personality traits in the privacy context (Bélanger and Crossler 2011).

Anecdotal evidence indicates that individuals are predisposed to be too lazy to take care about their privacy (Kwong 2015; Spencer 2014). For example, it is stated that individuals share private information by default with the manufacturer of televisions because they are too lazy to change these settings. Laziness as a personality trait (Abramson et al. 1978; Watkins et al. 2009) might therefore influence the way how individuals translate their privacy concerns into actual disclosure behavior and would therefore serve as an additional explanation for the privacy paradox. Therefore, this study introduces laziness as a personality trait in the privacy context. We pose the research question:

How does laziness as a personality trait influence the privacy paradox?

Answering the research question contributes to theory by providing an additional explanation for the privacy paradox as requested by previous research (Kokolakis 2017). To answer this research question, we conducted a quantitative study with multiple snapshots by drawing on the model of personality theory (McAdams 1996). The model of personality theory states that the way how concerns of individuals are transferred into behavior is influenced by personality traits. In particular, we research on in how far laziness as a personality trait influences the way privacy concerns influence disclosure behavior. Laziness is indicated to be an important factor in privacy-related research (Spencer 2014) and is considered to be a personality trait (Abramson et al. 1978; Watkins et al. 2009). We therefore consider the model of personality theory to be an adequate theory to research on the question in how far laziness as a personality trait influences the way how privacy concerns are transferred into disclosure behavior.

The rest of the paper is structured as follows: in section two we provide some theoretical background about privacy and the privacy paradox and conceptualize and define laziness. In section three we construct our research model. In section four we present our methodology and operationalize laziness as a new construct. Section five presents our results and section six discusses the theoretical and practical implications of our findings. Besides an additional explanation for the privacy paradox, theoretical implications include a conceptualization and operationalization of laziness.

2 PRIVACY AND THE PRIVACY PARADOX

Although privacy is a confusing concept (Berry 2004), the plethora of definitions of privacy in modern IS research vary only slightly (Bélanger and Crossler 2011). The construct concerns controlling information (Bélanger et al. 2002), information collection, unauthorized secondary use, improper access, and errors (Smith et al. 1996) or about time, matter, and space dimensions (Skinner et al. 2006). In this study, we rely on the following definition: the interest of an individual in controlling the handling of information about themselves (Bélanger and Crossler 2011).

The plethora of privacy research in general also reveals a paradox which is well known in privacy research and is called the privacy paradox (see Figure 1). The privacy paradox is that even though individuals are gravely concerned about their privacy (privacy concerns), they often behave in ways that threaten it, i.e. they disclose a great deal of personal information (self-disclosure). A review of the privacy paradox (Kokolakis 2017) identified several articles proving the privacy paradox (Acquisti and Grossklags 2005b; Lee et al. 2013). However, several articles also provide evidence proving the contrary i.e. that privacy concerns significantly influenced self-disclosure behavior (Son and Kim 2008; Wakefield 2013). According to Kokolakis (2017), the reasons why current research yields contradictory results are related to the choice of methodologies, information interpretation, and the research context. Proponents of the privacy paradox offer three basic explanations: 1) the privacy calculus (Dinev and Hart 2006) where individuals weigh their benefits of revealing their information with the particular downsides of doing so. If benefits outweigh the downsides, then individuals disclose information although being concerned about their privacy. 2) cognitive biases and heuristics (Grossklags and Acquisti 2007). Research has shown that individuals do not always act fully rational, as supposed by the

privacy calculus, but their decisions are based on cognitive biases and heuristics. For example, individuals tend to be overconfident when making privacy-related decisions (Jensen et al. 2005), are heavily optimistic when it comes to their privacy (Baek 2014) or value short-term benefits more than long-term risks; 3) irrational behavior (Acquisti and Grossklags 2003, 2005b) which states that individuals do not have the cognitive skills to calculate all relevant factors with respect to self-disclosure.

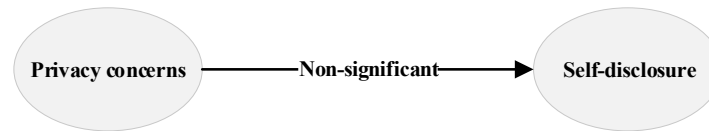


Figure 1. The privacy paradox

Although there are several explanations for the privacy paradox and reasons for the phenomenon of its contradictory results, there is still a call for further investigation into that phenomenon to shed more light on its complexity (Kokolakis 2017). One possibility is to include individual differences, such as personality traits (Agarwal and Prasad 1999), in the context of privacy (Smith et al. 2011). In particular, to better understand the privacy paradox, there is a call to include personality traits as moderators of the relationship of privacy concerns on self-disclosure (Bélanger and Crossler 2011). The rationale for this is that personality traits can lead to different behavior (McAdams 1996) and can therefore be the reason why there are different results referring to the privacy paradox. To find out to what extent prior research in the privacy context has used personality traits in general and laziness in particular and also to find out to what extent personality traits have been used as moderators, we performed a literature review. Our review (see Table 10 in the appendix) was conducted using the search term “privacy” in the Senior Scholars’ basket of eight journals. We used *privacy* as our keyword because it is the overall subject of our review. Laziness is considered to be a personality trait (Abramson et al. 1978; Watkins et al. 2009), however, we categorize the identified literature more broadly by individual differences, which include personality traits (Agarwal and Prasad 1999), to gain a more holistic view. The review was therefore researching on the question to what extent individual differences have been investigated in prior research, independent of their level of significance.

The review confirms a lack of research on the moderating effect of individual differences. In addition, laziness as a personality trait has not been used by prior research. To fill this gap, this study examines whether laziness as a personality trait moderates privacy behavior. To better explain personality traits and the interaction with behavior we use the theory of understanding personality which is described in the following section.

3 THEORY FOR UNDERSTANDING PERSONALITY AS THE THEORETICAL LENS

To integrate laziness into the privacy context, we rely on McAdams’ model of personality theory (McAdams 1996), which has been used in other research settings (Eckhardt et al. 2016). As can be seen in Figure 2, the theory can be divided into three hierarchical levels. Personality traits are at the bottom and can be split up into three different kinds of traits (Thatcher and Perrewé 2002). The middle level includes personal concerns determined by personality traits. The top level includes the actual behavior of an individual, which is affected by the two other levels. The explanation for these assignments and the interplay between these aspects is elucidated in the following in more detail.

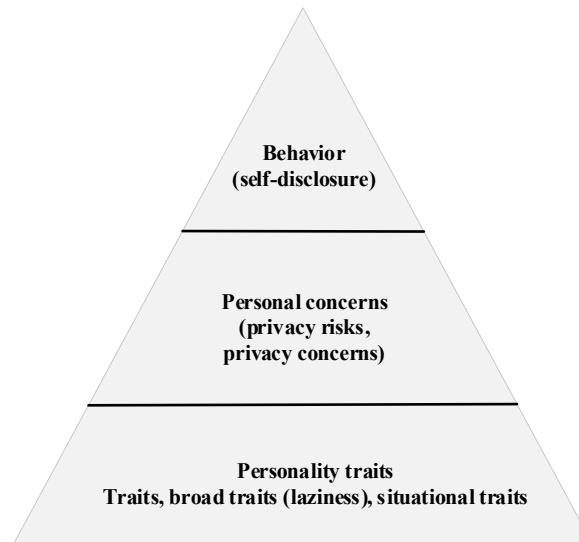


Figure 2. Theoretical perspective on laziness, privacy risk, privacy concerns, and self-disclosure according to McAdams' model of personality theory (McAdams 1996)

3.1 LAZINESS AS A PERSONALITY TRAIT

According to McAdams' model, every person has personality traits. As illustrated in Figure 2 these personality traits can be seen as the basis of a person which affect the concerns of a person (on the mid-level) and her/his behavior (on the top-level). Hence, the way how concerns are transferred into behavior are dependent on personality traits.

Personality traits are defined as an “*individual's dispositions or tendencies that lead to certain attitudinal and behavioral patterns across situations*” (Junglas et al. 2008, p. 391). To integrate laziness into the concept of personality traits, one needs to consider that traits can be divided into 1) the big five personality traits such as conscientiousness or neuroticism (Costa and McCrae 1992), 2) broad traits which are permanent and predispose a person to behave in a consistent manner to stimuli across diverse situations (Thatcher and Perrewé 2002), and 3) situational traits which are identical to broad traits, but differ as the situation is narrowly defined (Thatcher and Perrewé 2002).

According to personality traits research, laziness is treated as a stable, internal and global factor (Abramson et al. 1978) which is invariant across situations (Watkins et al. 2009) and has also been seen as a subpart of the trait of conscientiousness (Ashton et al. 2004; McCrae and Costa 1987). In addition to our literature review, we also identified several descriptions of laziness (see Table 1) that suggest that laziness is more commonly viewed as a broad trait because it is not situation-specific, but rather independent of the situation. This study thus also treats laziness as a broad trait. However, despite the descriptions of laziness identified in our review, the term still lacks conceptual clarity. We thus conceptualize laziness and clearly define how we treat laziness in our research paper.

The Oxford Dictionaries (2016) define laziness as “*the quality of being unwilling to work or use energy*”. Laziness from this point of view is thus seen as a broad trait in which individuals do not want to put any effort into anything. Lazy people thus do not want to use energy independent of the context, the kind of work or the expected reward. This also fits the definition of laziness by Garrison et al. (1917) simply as “*that you don't want to work*”.

Further descriptions treat laziness as the opposite of hardworking (McCrae and Costa 1987; Schneider et al. 1994) or just as “*sitting and doing nothing*” (Jackson et al. 2010, p. 510). Those definitions are similar in the view that also in those definitions, lazy people do not work. However, it is

different as they do not treat lazy individuals as individuals who do not *want* to work but as individuals who simply do not work, regardless of whether they want to or not and regardless of whether there are external circumstances which could constrain an individual's behavior with regard to work.

Additional definitions given by Puhl and Brownell (2001) and Abramson et al. (1978) define people as lazy if they exhibit a lack of effort. This is somewhat different from not wanting to work because individuals might demonstrate a lack of effort but still want to work. For example, lack of effort might stem from not obtaining rewards or other factors which influence the possible amount of effort one can put into work. It is also different to the above definition "*not working*", as individuals who lack of effort might still work but still demonstrate a lack of effort when they work.

Putting all those descriptions together it is obvious that laziness is not clearly defined and ill-conceptualized in current research. However, consistent with all given descriptions, laziness is a broad trait which is independent of the situation (Kassin 2003) and which drives individuals to work as little as possible. Working as little as possible can also have the consequence that one might not reach the goals one would like to reach. We therefore define laziness as *a broad trait in which individuals summon as little energy as possible to work even if that means not reaching a goal*".

Citation	Definition/Description
Oxford Dictionaries 2016	"The quality of being unwilling to work or use energy"
Garrison et al. 1917	"Laziness is that you don't want to work"
McCrae and Costa 1987; Schneider et al. 1994	The opposite of hardworking
Jackson et al. 2010, p. 510	"Sitting and doing nothing"
Puhl and Brownell 2001, p. 801	"Flaws in personal effort"
Abramson et al. 1978, p. 57	"It can be to lack of [sic] effort"

Table 1. Definitions of laziness

To better delineate laziness from other constructs in current research, we divided our definition of laziness into two key categories (highlighted in bold): *a broad trait in which individuals summon as little **energy** as possible to work even if that means not **reaching a goal***. Based on these two categories we performed a literature review and identified seven similar constructs of laziness (see Table 2) (Bélanger and Crossler 2011; Williams et al. 2009):

Energy: Three constructs – effort expectancy, ease of use, and idleness – fit the category we call energy. Effort expectancy refers to the "*degree of ease associated with the use of the system*" (Venkatesh et al. 2003, p. 450) and is thus similar to laziness in that it reflects the energy one puts into performing a task. Although individuals with high effort expectancy think that it will not be easy to use a system, this does not mean that they are not willing to put energy into using that system. Thus, individuals with high effort expectancy may still be willing to work a lot despite the expected high effort, whereas individuals who demonstrate a high degree of laziness try to work as little as possible, no matter how high the effort is.

Ease of use is a similar construct to laziness as it is defined as the "*degree to which a person believes that using a particular system would be free of effort*" (Davis 1989 p. 320). Thus, it is also about the amount of energy one puts into using an IS. But only because using a system is free of effort does not mean that an individual will put any energy into it. And only because using a system requires a lot of effort does not mean that an individual will *not* put any energy into it. Hence, ease of use might be relevant for lazy individuals because depending on the ease of use individuals have to put a certain amount of effort into using that system. However, no matter how easy the system is to use lazy individuals will always try to put as little energy as possible into using that system even if it means that they will not use it at all.

A third construct related to energy is idleness, which Garrison et al. (1917) explicitly differentiated

from laziness: “*Laziness is that you don't want to work; idleness is you can't, for a while*”. In other words, individuals with high idleness are not able to put energy into doing work for a certain amount of time, whereas lazy individuals permanently try to put as little energy as possible into doing any work.

Reaching goals: Three common constructs – inertia, extrinsic, and intrinsic motivation – fit the category we call reaching goals. Inertia refers to how attached a user is to the status quo even if there are better alternatives (Polites and Karahanna 2012). Inertia is related to laziness in that it implies having goals but not reaching them as easily due to an unwillingness to switch to an alternative. However, laziness differs from inertia with respect to behavior. Individuals who exhibit a high degree of laziness try to put as little energy as possible into everything, no matter what, whereas individuals with high inertia do not put any energy into switching to a new state but they can still put a lot of energy into their current status quo.

Extrinsic and intrinsic motivation are additional constructs, which indicate how willing an individual is to reach a goal. Individuals who are extrinsically motivated do things to receive external rewards such as compensation, praise or prestige, whereas individuals who are internally motivated do things based on an internal psychological force, such as enjoyment, duty, meaningfulness or progress (Deci and Ryan 2000; Ryan and Deci 2000). Motivated individuals thus have a particular goal, e.g. having fun or making progress when internally motivated or reaping rewards when externally motivated and willingly want to reach that goal by putting energy into doing their work. In contrast, although lazy individuals may have goals, they do not put energy into achieving them.

Citation	Definition	Different from laziness because	Category
Laziness	Laziness is a broad trait in which individuals summon as little energy as possible to work even if that means not reaching a goal.	-	-
Effort expectancy	“The degree of ease associated with the use of the system” (Venkatesh et al. 2003, p. 450).	Individuals with high effort expectancy can still invest a lot of energy into performing the task, whereas lazy individuals will put as little energy as possible into that task.	Energy
Ease of use	“The degree to which a person believes that using a particular system would be free of effort” (Davis 1989, p. 320).	No matter how easy to use a system is, lazy individuals will always try to put as little energy as possible into using that system.	Energy
Idleness	“Laziness is that you don't want to work; idleness is you can't, for a while” (Garrison et al. 1917).	Individuals with high idleness are not able to work for a while, whereas lazy individuals permanently try to put as little energy as possible into doing any work.	Energy
Inertia	“User attachment to and persistence in using an incumbent system (i.e., the status quo), even if there are better alternatives or incentives to change” (Polites and Karahanna 2012, p. 24).	Individuals with high inertia do not put energy into changing their status quo, whereas lazy people do not put energy into anything.	Reaching goals
Extrinsic motivation	“Extrinsic motivation is a construct that pertains whenever an activity is done in order to attain some separable outcome” (Ryan and Deci 2000, p. 60).	Motivated individuals have a goal which they want to reach by putting energy into their work, whereas lazy individuals do not put energy into their work regardless of whether or not they have a goal.	Reaching goals
Intrinsic motivation	“Intrinsic motivation is defined as the doing of an activity for its inherent satisfactions rather than for some separable consequence” (Ryan and Deci 2000, p. 56).	Motivated individuals have a goal which they want to reach by putting energy into their work, whereas lazy individuals do not put energy into their work regardless of whether or not they have a goal.	Reaching goals

Table 2. Constructs related to laziness

In conclusion, we have shown that although laziness is similar to other common constructs with regard to the amount of energy one puts into doing work and to reaching goals, it differs from each construct significantly. Now we return to McAdams’ model of personality and explain personal concerns which is on the middle level (see Figure 2) and thus also dependent on personality traits.

3.2 PRIVACY CONCERNS AND PRIVACY RISK AS PERSONAL CONCERNS

The second part of McAdams' theory for understanding personality refers to what he calls "*personal concerns*" (McAdams 1996, p. 301) in which personality descriptions invoke personal strivings, life tasks or coping strategies. This study considers privacy concerns and privacy risks as examples of personal concerns in keeping with McAdams' model.

Privacy concerns are a central construct in current privacy research (Smith et al. 2011) that measure how worried individuals are about losing control over their personal information. We define privacy concerns as an individual's perception that the privacy of personal information disclosed online is threatened (Son and Kim 2008). This is slightly different from privacy risk, which can be defined as "*the expectation of losses associated with the disclosure of personal information*" (Xu et al. 2011, p. 804) and is often used to research on privacy-issues in the domain of IS (Choi et al. 2018; Zhan and Zhou 2018). Hence, whereas privacy concerns are about how the information is used and who has access to the information (Dinev and Hart 2006), privacy risk is about the possible opportunistic behavior of others.

3.3 SELF-DISCLOSURE AS A BEHAVIOR

The third part of McAdams' theory for understanding personality expressing "*the form of stories of the self*" (McAdams 1996, p. 301) reflecting the development of an individual over time. In line with previous studies (e.g., Eckhardt et al. 2016) we conceptualize this development with behavior of individuals that is developed through both other levels, i.e. personality traits and personal concerns. The behavior we measure is information self-disclosure, the variable frequently used in privacy contexts (Krasnova et al. 2010). Self-disclosure of information is defined as "*the breadth and depth of personal information that one individual willingly provides to another*" (Jourard 1971; Wakefield 2013, p. 159).

In the following section, we introduce our research model, name our constructs and present our hypotheses on how they will be related to each other. In the subsequent section, we operationalize laziness as a new construct in privacy research.

4 RESEARCH MODEL

Our research model is presented in Figure 3 and includes hypotheses using the constructs discussed in the previous section.

Building on the privacy paradox (Kokolakis 2017) we integrate privacy concerns and self-disclosure as illustrated in Figure 1. We also include laziness as a personality trait into our research model which could determine why users disclose information even when they have privacy concerns. We also include privacy risk as it is one of the most salient beliefs in privacy related research (Malhotra et al. 2004) and as it is highly related to privacy concerns on a semantic base (Dinev and Hart 2006). To account for the most common demographic variables we also use the control variables age and gender as is common practice in privacy research (see Table 10 in the appendix). To avoid confusion between intention and behavior of disclosure (Smith et al. 2011) we focus on the actual self-disclosure behavior of the individuals.

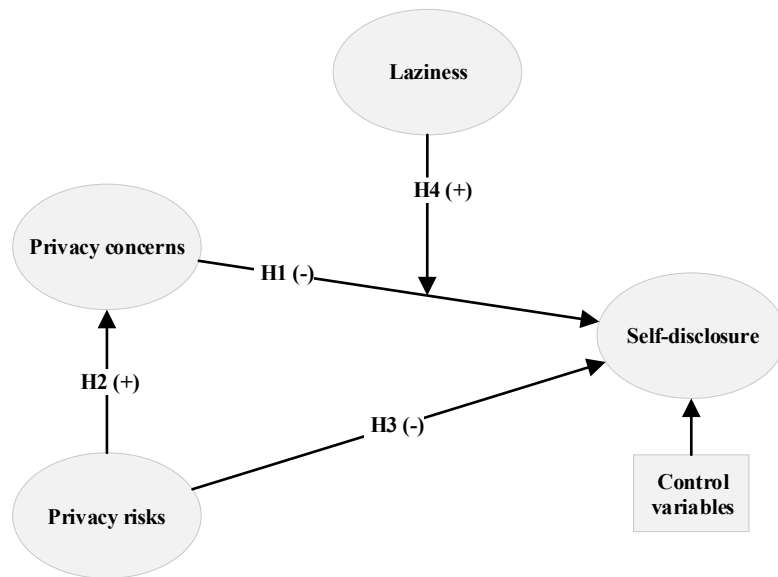


Figure 3. Research model

Privacy concerns reflect the level of worry that individuals feel when disclosing their information because of a threat to their privacy (Son and Kim 2008). As discussed above, it would be logical to assume that the more worried people are about the potential threat to their privacy, the less personal information they will disclose. However, the privacy paradox is that privacy concerns only sometimes lead to lower disclosure of personal information and is often non-significant (Kokolakis 2017), due to different reasons such as a general intention – behavior gap (Norberg et al. 2007; Smith et al. 2011). As we research on actual behavior we hypothesize that:

H1: Privacy concerns do not significantly influence self-disclosure.

Based on the privacy calculus model (Dinev and Hart 2006), individuals' privacy concerns are positively influenced by privacy risk. The higher the privacy risk of self-disclosure, the higher the concerns that the privacy will be threatened. This is because privacy risk is about possible opportunistic behavior of others, i.e. if an individual thinks that there is a risk that an unauthorized individual will access personal information and use it inappropriately, she will have higher concerns about her privacy. In line with the privacy calculus, we therefore hypothesize that:

H2: The higher the privacy risk an individual perceives, the higher the privacy concerns.

In addition, privacy risk should negatively influence self-disclosure directly. When individuals think that self-disclosure is risky then they will lower their self-disclosure. This is consistent with the expectancy theory (van Eerde and Thierry 1996; Vroom 1964), which says "*that individuals are motivated to minimize negative outcomes*" (Dinev and Hart 2006, p. 65). In our case, the privacy risk is the level of expected negative outcomes by disclosing information. Hence in line with the privacy calculus and other researchers (Keith et al. 2015; Xu et al. 2009) we hypothesize that:

H3: The higher the privacy risk an individual perceives, the less information the individual will disclose.

To integrate laziness into our research model, we treat it as a broad personality trait which is an individual difference. There are many precedents for including personality traits in IS research, e.g. as a moderator of beliefs on intention to use (Agarwal and Prasad 1998; Devaraj et al. 2008) or as direct antecedents of behavior (McElroy et al. 2007). In the privacy context, Bélanger and Crossler (2011) have called to integrate personality traits by investigating the degree to which personality traits moderate

the influence of privacy concerns on self-disclosure. Our research question also aims at investigating in how far laziness has an influence on individuals' actions to protect their information privacy in response to information privacy concerns. We therefore also ask for a more moderating effect of laziness. Since our literature review (see Table 10 in the appendix) reveals little prior research on this issue, we are responding to Bélanger and Crossler's call by investigating the moderating influence of laziness on the relationship between privacy concerns and self-disclosure.

Specifically, we hypothesize that being lazy (i.e. putting as little energy as possible into anything) may moderate the act of translating privacy concerns into actual behavior, i.e. taking steps to disclose less personal information, since this act requires putting energy into something, searching for secure alternatives, or thinking about what personal information to disclose. For instance, users of a social networking site (SNS) who exhibit a high degree of laziness might continue disclosing personal information despite great privacy concerns because it takes too much energy to translate their privacy concerns into actual behavior. Hence, if an individual who is highly concerned about her privacy is lazy, then we posit that those privacy concerns will not influence her self-disclosure behavior because she is too lazy to protect her privacy.

On the contrary, if individuals who exhibit a low degree of laziness and willingly put energy into work are highly concerned about their privacy, they will be willing to put energy into protecting their privacy. We posit that such individuals will translate their privacy concerns into actual behavior and disclose less personal information. For example, SNS users who exhibit a low degree of laziness and who are highly concerned about their privacy might take steps to disclose less personal information on the SNS to protect their privacy. Hence, we hypothesize that:

H4: Laziness will moderate the influence of privacy concerns on self-disclosure such that privacy concerns will have a stronger negative effect on self-disclosure for less lazy people and have no significant effect for lazier people.

To validate these hypotheses, we have conducted a quantitative study with multiple snapshots following the methodology presented in the following section.

5 METHODOLOGY

Since the construct of laziness in the context of privacy does not yet exist, we first conceptualized laziness in the theoretical background. Now, we operationalize laziness following the lead of several other researchers (Agarwal and Prasad 1998; Bala and Venkatesh 2016; Ragu-Nathan et al. 2008).

5.1 STEP 1: ITEM DEVELOPMENT

After doing an extensive search in the highly regarded Senior Scholars' "basket of eight" IS journals (EJIS, ISJ, ISR, JAIS, JIT, JMIS, JSIS, MISQ) as well as ICIS and ECIS as the two top IS conferences and in additional respected journals in the fields of psychology and medicine, we ascertained that the construct "laziness" has not been developed and validated. There is one research article which uses laziness as a construct (Jackson et al. 2010), but the construct was not validated in that article and no clear definition of laziness was provided, so it remains unclear what exactly the construct measured.

Since we rely on our own conceptualization and definition of laziness, we developed our own scale. Our new items are partly based on the items used by Jackson et al. (2010) and on our definition of laziness. In particular, our definition of laziness is that we define laziness as a broad trait in which individuals summon as little energy as possible to work even if that means not reaching a goal. The two main parts of the definition thereby refer to the amount of energy an individual summons to work and

the possibility that one is not reaching a goal. Our developed items therefore include both main parts. We evaluated and revised these items based on discussions with four academic colleagues and settled on five items which everyone agreed on (see Table 3).

Label	Item	Amount of energy	Reaching goals
Laziness-1	I try to work as little as possible even if that has disadvantages for me.	first part	second part
Laziness-2	I consciously try to put as little energy as possible into doing work even if that means that what I am working on will not be done properly.	first part	second part
Laziness-3	Sometimes I do not reach my goals because I did not put enough energy into reaching them.	second part	first part
Laziness-4	I'm sometimes aware that I should put more energy into working.	second part	
Laziness-5	If I worked more, I could reach more goals.		second part
<i>"First part" refers to the first part of the item, whereas "second part" refers to the second part of the item.</i>			

Table 3. Developed items including a categorization by our definition of laziness

All items are measured on a 7-point Likert scale ranging from 1 ("strongly disagree") to 7 ("strongly agree"). The second step in the process was to test the validity and reliability of the newly developed construct.

5.2 STEP 2: RELIABILITY AND CONSTRUCT VALIDITY

To assess the reliability and construct validity of those items, we posted a questionnaire on the online crowdsourcing market (OCM) Amazon Mechanical Turk (Mturk). On this OCM, individuals are paid for participating in studies. We chose Mturk because it has been used successfully in other settings (Boyer O'Leary et al. 2014) as well as in privacy settings (Pu and Grossklags 2015) and has also been successfully validated (Steelman et al. 2014). Following the lead of prior research (Landis and Koch 1977; Nahm et al. 2002), we asked participants to assign the newly developed items and the similar items (see Table 2) to the corresponding constructs. All in all, 28 participants took part in our study.

In particular, we first provided the participants with some information about all constructs (by defining the constructs and giving practical examples) and provided information about how to assign the items. Then we gave them a list of all items which participants then had to assign to the construct they think it fits best to. As only those items which have been assigned correctly by at least 61 percent should be included (Landis and Koch 1977; Nahm et al. 2002) we removed those items which were assigned correctly by less than 61 percent of the time (see Table 4). This resulted in the removal of two items (Laziness-4 and Laziness-5). Three items were assigned correctly by at least 61 percent (Laziness-1, Laziness-2, Laziness-3).

Label	Item	Assigned correctly by (in percentage)
Laziness-1	I try to work as little as possible even if that has disadvantages for me.	74.1
Laziness-2	I consciously try to put as little energy as possible into doing work even if that means that what I am working on will not be done properly.	81.5
Laziness-3	Sometimes I do not reach my goals because I did not put enough energy into reaching them.	85.2
Laziness-4	I'm sometimes aware that I should put more energy into working.	26.0
Laziness-5	If I worked more, I could reach more goals.	11.1
<i>The bottom two items were removed because less than 61 percent of those surveyed assigned it correctly.</i>		

Table 4. Laziness items

5.3 STEP 3: EXPLORATORY AND CONFIRMATORY FACTOR ANALYSIS

To provide statistical evidence that these items belong together we also performed an exploratory and confirmatory factor analysis following the approach taken by other researchers (Ragu-Nathan et al. 2008). In this survey, we asked participants questions about our construct of laziness (see Table 4) and

about ease of use (Davis 1989) as this was the construct which was closest related to laziness in the previous step. 166 participants filled out our survey without missing values. In line with prior research we then split up the dataset into two assigned datasets. The split was random and came out with set 1 consisting of 70 items and set 2 consisting of 96 items. We used the items of set 1 to develop the construct and then used the items of set 2 to validate the results.

Consistent with prior research we first performed an exploratory factor analysis. The results show that our newly developed construct laziness indeed consists of three items as all those items were grouped together and all other remaining items of ease of use were grouped together. Hence, we did not have to remove any items from our newly developed construct.

Set 1	Set 2	Recommended values
CFI: 1.000	CFI: 0.995	CFI: >0.95 (Hu and Bentler 1999)
SRMR: 0.0215	SRMR: 0.0759	SRMR: <0.08 (Hu and Bentler 1999)
RMSEA: 0.000	RMSEA: 0.052	RMSEA: <0.06 (Hu and Bentler 1999)

Table 5. Confirmatory factor analysis

Then after performing an exploratory factor analysis we conducted a confirmatory factor analysis with AMOS 23. We calculated comparative fit indices (CFI), standardized root mean square residual (SRMR), and root mean square error of approximation (RMSEA) as is familiar from other research settings (Steelman et al. 2014). CFI should be at least 0.95, SRMR below 0.08, and RMSEA below 0.06 (Hu and Bentler 1999). As all measures fit the recommended values, we did not have to remove any item (see Table 5).

5.4 STEP 4: CONSTRUCT RELIABILITY

To assure construct reliability one needs to account for means, standard deviation, and reliability. The results of these calculations are depicted in Table 6. We performed the calculations based on the results of both samples in step three. The obtained values are greater than the recommended value of 0.7 (Nunnally 1978).

Label	Item	Mean	SD	Reliability
Laziness-1:	I try to work as little as possible even if that has disadvantages for me.	2.69	1.43	0.788
Laziness-2:	I consciously try to put as little energy as possible into doing work even if that means that what I am working on will not be done properly.	2.96	1.47	
Laziness-3:	Sometimes I do not reach my goals because I did not put enough energy into reaching them.	2.67	1.36	
The range of answers received is between 1 (strongly disagree) through 7 (strongly agree).				

Table 6. Construct reliability with laziness items

5.5 STEP 5: DISCRIMINANT AND CONVERGENT VALIDITY

In the last step, we used the information of both samples, i.e. of all 166 participants who filled out our survey without missing values, to account for discriminant and convergent validity. We again used AMOS 23 to calculate the reliability, composite reliability (CR) and average variance extracted (AVE). The results show that CR values are above 0.7 and AVE is above 0.5. As values of CR are greater than of AVE, we have good convergent validity. In addition, we accounted for maximum shared squared variance (MSV) values and average shared squared variance values (ASV) which are both smaller than AVE (see Table 7). Hence discriminant validity is also good.

	Reliability	CR	AVE	MSV	ASV
Laziness	0.788	0.868	0.688	0.003	0.002
Ease of use	0.954	0.971	0.917	0.220	0.111

Table 7. Discriminant and convergent validity

To summarize, we operationalized laziness as a three-item construct after performing several steps

to make sure that there is semantic and statistical evidence for that construct. Based on this evidence, we used the three-item construct in our research model.

5.6 RESEARCH SETTING: A STUDY WITH MULTIPLE SNAPSHOTS

The technology we used in our research setting is a social networking site (SNS). We chose this technology because through digitization, SNS have become a major part of current research (e.g., Turel 2014) and have major impacts on the daily life of individuals. Furthermore, on SNS individuals generate digital traces among others by sharing a lot of private information, e.g. their real name, pictures or private messages which are highly sensitive. If those messages were breached it would cause serious problems in respect to the privacy of the persons concerned. We chose the SNS Facebook because it has the higher numbers of users worldwide (statista.com 2018).

The research setting itself was done in with multiple snapshots, i.e. we conducted two surveys at two different points of time. We did this because when researching beliefs which influence behavior one should separate the point of time of the research from the point of time of the behavior (Kim and Malhotra 2005). Hence our study consisted of two surveys. We conducted our first survey in August 2015 and inquired into the independent variables influencing behavior, i.e. privacy concerns and privacy risk. In our second survey in January 2016, we inquired into the self-reported measurement of self-disclosure as the behavior and as the dependent variable. Laziness, as a broad trait, is per definition stable over time (Costa and McCrae 1994), so we chose to include the laziness items only in the second survey when the variable was fully conceptualized.

We followed two approaches in finding participants for our study. First, we drew on a list of people who had registered on our university website to take part in forthcoming surveys voluntarily. Second, we drew on a list of previous survey participants who had expressed interest in being invited to participate in future surveys. Together, our pool included 1,265 individuals.

We invited the entire pool to participate in our study by email in August 2015, assigning each person an individual username and password to eliminate the danger of double participation. As an incentive, we also raffled three iPads among study participants. The second survey took place in January 2016. Again all 1,265 participants were invited to take part in our study and received the same instructions as the first time. After removing individuals who did not take part in both surveys, who do not use Facebook and who provided unrealistic information such as being online for more than 24 hours a day or claiming to have an unrealistic number of Facebook friends, we ended up with a total of 188 participants. In particular, 243 participants of the 1,265 participants took part in both surveys, 221 participants do have a Facebook profile and 188 provided realistic information which leads us to a number of 188 participants. The demographics are depicted in Table 8.

	Mean	SD
Age	42.5	11.4
Number of friends on Facebook	211.1	198.3
Average time spent on Facebook in minutes per day	38.4	61.6
Gender	Male	Female
	63.8 percent	36.2 percent

Table 8. Demographic information

We analyzed the information following a partial least square (PLS) approach. The items of the questionnaire can be found in the appendix. Information about the degree to which the results support the hypotheses is provided in the following section, followed by a discussion of implications for theory and practice.

6 INFORMATION ANALYSIS AND RESULTS

By taking a PLS-approach we were able to assess both a measurement model and a structural model (Barclay et al. 1995; Chin 1998). Taking a PLS-approach also enables the impact of common method bias (CMB) to be evaluated (Liang et al. 2007; Podsakoff et al. 2003). As we consider laziness to be rather negative than a positive trait we also would not expect a normal distribution (Turel et al. 2011). Thus, a PLS approach seemed to be appropriate in our study. The rule of 10 says that the minimum of participants is 10 times the number of antecedents directed at a particular construct (Hair et al. 2011). Based on the rule of 10 the minimum number would be 50 participants as there are five antecedents directing at self-disclosure (including control variables and the moderating effect). Thus the 188 participants in our study are enough to validate our research model (Hair et al. 2011). We start the analysis by evaluating the CMB, which can occur when doing research on survey information.

CMB test: Using surveys where individuals can self-report their information can result in CMB, which may influence the information. To account for CMB we therefore conducted a study multiple snapshots where the independent variables are measured separately from the dependent variables which reduces potential CMB (Podsakoff et al. 2003). In addition, we performed two CMB tests. Harman's single factor test, which indicates if a single factor can explain the majority of the variance showed that only 30.17 percent can be explained by a single factor. We also added a CMB factor to our research model as suggested by prior research (Podsakoff et al. 2003; Williams et al. 2003). In particular, we added one additional construct which contains all items of the original model. All other constructs were transformed into single-order constructs, i.e. every indicator of every construct was transformed into a single-item construct which points to the construct it had been an indicator of. In addition, that construct was still assigned to all corresponding items. Then we compared the ratio of the variance extracted (R^2) including the CMB factor with the variance extracted without the CMB factor. The R^2 including the CMB factor is 0.00325 higher than including the R^2 including the CMB factor. As the R^2 without the CMB factor is 0.671 the ratio is 1:206 which indicates that CMB is not a problem (Liang et al. 2007). This indicates that CMB does not distort the results and we can continue with the evaluation of the measurement model.

6.1 MEASUREMENT MODEL

In our measurement model, we only used reflective indicators. To have a high **content validity** we use existing measurement items and adapted them to fit the context of Facebook. In addition, we operationalized laziness as a new construct as described above. Items with references are represented in Table 13 in the appendix, along with the Cronbach alpha values, which all exceed the widely-recommended value of 0.70.

Indicator reliability: To explain more than 50 percent of the variance of the latent variables, the values of the indicators should be greater than 0.707 (Barclay et al. 1995; Carmines and Zeller 1979). Table 13 in the appendix shows that this is true for all indicators used in our model. Also, after employing bootstrapping with 1,000 samples, all indicators proved highly significant.

Construct reliability: To assess the reliability of the constructs, composite reliability (CR) and average variance extracted (AVE) are used. CR should be greater than 0.8 (Nunnally 1978) and AVE greater than 0.5 (Fornell and Larcker 1981). Both are true in our model, as illustrated in Table 9.

Discriminant validity: By using discriminant validity, one can assess the degree to which items differ from each other (Campbell and Fiske 1959). As shown in Table 9, the square root of AVE is greater than the correlation of every construct with each other (Barclay et al. 1995; Gefen and Straub

2005). However, the heterotrait-monotrait (HTMT) ratio is more reliable in finding a lack of discriminant validity than the Fornell-Larcker criterion (Henseler et al. 2014). Hence, we also use it to evaluate discriminant validity. When using the most conservative approach with $HTMT_{0.85}$ our results show that there is discriminant validity. The highest correlation value in our information is 0.648 between privacy concerns and privacy risk which is lower than 0.85.

Construct	Mean	SD	AVE	CR	1	2	3	4	5	6
1 Privacy concerns	4.90	1.65	0.806	0.961	0.898					
2 Privacy risk	5.24	1.41	0.651	0.903	0.594	0.807				
3 Laziness	2.77	1.42	0.688	0.868	0.083	-0.015	0.830			
4 Self-disclosure	3.21	1.69	0.683	0.896	-0.253	-0.429	0.103	0.826		
5 Age	42.5	11.35	<i>Single item construct</i>	<i>Single item construct</i>	0.076	0.029	0.008	0.009	<i>Single item construct</i>	
6 Gender	1.35	0.48	<i>Single item construct</i>	<i>Single item construct</i>	0.158	0.075	-0.170	-0.098	-0.158	<i>Single item construct</i>

Table 9. AVE, CR, Fornell-Larcker criterion, and bivariate correlations

As all tests were successful, we conclude that our measurement model is valid and we can continue with the evaluation of the structural model.

6.2 STRUCTURAL MODEL

When the research model contains a moderator, the results should report the R^2 without the moderator and the R^2 including the moderator to provide information about the influence of the moderator (Carte and Russell 2003). The explained variance of self-disclosure without the moderator is 19.6 percent, and 21.6 percent including the moderating effect (see Figure 4). Furthermore, privacy risk explains 35.3 percent of the variance of privacy concerns, no matter if including or excluding the moderating effect as the moderator does not affect the path between privacy risk and privacy concerns. Another method to assess the strength of a moderator and all other constructs is using the effect size in the form of f^2 values. Using the common f^2 values to determine the effect of a construct one can see that the moderating effect of laziness is strong (see Table 11 in the appendix) whereas the effect of privacy risk on self-disclosure is medium and the direct effect of laziness and privacy concerns is non existing (see Table 12 in the appendix).

After conducting bootstrapping with 1,000 samples, the results reveal that the influence of privacy risk on self-disclosure and privacy concerns is highly significant. Also, the moderating effect of laziness on the relation between privacy concerns and self-disclosure is significant whereas the direct effect of privacy concerns on self-disclosure is insignificant. In addition, age and gender, as control variables are non-significant. The results of the path coefficients are depicted in Figure 4 and show that all hypotheses are supported.

To further investigate the moderating effect of laziness we performed a multi-group analysis depending on the level of laziness. Usually a moderator is used to explain if the effect of one path is stronger/weaker depending on the value of the moderator. Hence, in our example we figured out if the influence of privacy concerns on self-disclosure is different for diverse individuals depending on their level of laziness. In such a model all answers of all participants are used to explain the hypotheses. By performing a multi-group analysis, we try to better explain the influence of laziness by only using those answers of individuals who are in a specific group, depending on their level of laziness. In our example we divided the individuals into two groups (“high lazy”, i.e. individuals who exhibit a high degree of laziness and “low lazy”, i.e. individuals who exhibit a low degree of laziness). Then we calculated partial

derivatives for each of the two groups, as has similarly been done in other settings (Boss et al. 2015). The results are depicted in Table 14 in the appendix. The results show that the influence of privacy concerns on self-disclosure is non-significant when individuals are “high lazy”. However, among “low lazy” individuals, the influence of privacy concerns on self-disclosure becomes negative and significant. These results support our fourth hypothesis.

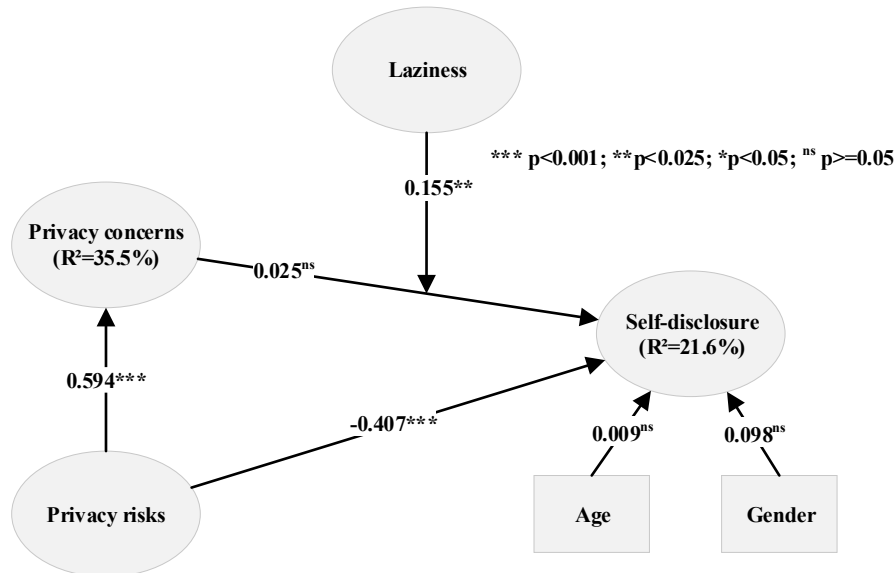


Figure 4. Path model result

A discussion of the results is provided in the following section alongside with limitations and a guidance for future research.

7 DISCUSSION

This research aims to explain how laziness as a personality trait provides an additional explanation for the privacy paradox. Using the lens of the personality theory (McAdams 1996) one can see that personality traits influence the way how concerns are transferred into behavior. We have therefore used this theory to explain how personality traits determine the way how privacy concerns influence self-disclosure. As one should use personality traits which best fit the context the study takes place in (Paunonen and Ashton 2001) and as it is indicated that laziness plays an important role in a privacy context (Spencer 2014) we chose laziness as the personality trait. In particular, we defined and conceptualized laziness as a broad personality trait (Abramson et al. 1978; Watkins et al. 2009) and built a research model (see Figure 3) which is based on the personality theory and which aim is it to explain the privacy paradox based on the level of laziness of individuals.

Our results show that the influence of privacy concerns on self-disclosure is significantly negative for individuals who exhibit a low degree of laziness, and insignificant for individuals who exhibit a high degree of laziness. The implications of these findings for theory and practice will be discussed below.

7.1 THEORETICAL IMPLICATIONS

Advancing the privacy paradox through laziness. Our results confirm the existence of the privacy paradox (Norberg et al. 2007), as our results indicate that there is no significant relationship between privacy concerns and self-disclosure. As other scholars have shown, privacy concerns do not significantly influence self-disclosure behavior (Keith et al. 2013). However, including laziness as a broad trait to moderate the relationship between privacy concerns and self-disclosure sheds new light

on the privacy paradox. Considering the personality trait laziness helps fill the gap on this topic in privacy research (see Table 10 in the appendix) and responds to calls for such research by other scholars (Bélanger and Crossler 2011; Smith et al. 2011). In particular, by examining laziness as a moderator we a) shed new light on the privacy paradox, b) explain the *why* and not only the *how* of the privacy paradox, and c) contribute to the privacy calculus model as an explanation of the privacy paradox.

a) Our findings shed new light on the privacy paradox (Kokolakis 2017; Norberg et al. 2007). As shown in Figure 5, previous research has provided different explanations for the privacy paradox, which are the privacy calculus, cognitive biases and heuristics as well as irrational behavior (Acquisti and Grossklags 2003, 2005a; Dinev and Hart 2006). Our findings contribute to this research stream by proving that individuals might be too lazy to convert their privacy concerns into actual behavior i.e. to stop disclosing information to protect their privacy. Our research indicates that only individuals who exhibit a low degree of laziness actually convert their privacy concerns into actual behavior and disclose less personal information. Therefore, with our research, we prove that laziness of individuals as a personality trait is considered as a fourth explanation for the privacy paradox (see Figure 5). Previous research has also found out that negative factors influence user behavior (Cenfetelli and Schwarz 2011). Hence, with our research, we show that negative factors, such as privacy concerns, are differently translated into user behavior aligned with personality traits.



Figure 5. Explanations for the privacy paradox

b) In addition, by using laziness as a possible explanation for the privacy paradox, we also explain the *why* and not only the *how* of the privacy paradox as called for in previous research (Bélanger and Crossler 2011). We show that the trait of laziness among individuals influences the degree to which they translate their privacy concerns into actual behavior. Individuals who exhibit a high degree of laziness refrain from putting energy into work, including taking actions to protect their privacy, while individuals who exhibit a low degree of laziness put energy into translating their privacy concerns into actual behavior by disclosing less personal information.

c) Furthermore, by including laziness in the privacy context, we contribute to the privacy calculus model which is considered to be an explanation of the privacy paradox (Dinev and Hart 2006). The privacy calculus says that individuals disclose their personal information when benefits outweigh the downsides of doing so. Our results indicate that laziness moderates the influence of privacy concerns as a downside of self-disclosure. That means that the level of laziness of an individual, moderates the effect of privacy concerns as a disadvantage of self-disclosure. Therefore, research on self-disclosure behavior should not focus solely on the benefits or disadvantages of self-disclosure, but rather should also consider the degree of laziness of the individuals.

In sum, we contribute to theory by advancing the privacy paradox through the usage of laziness by 1) revealing that besides the privacy calculus, cognitive biases and irrational behavior, laziness is a fourth explanation for the privacy paradox (see Figure 5), 2) by showing why laziness is an explanation for the privacy paradox and 3) by possibly advancing the privacy calculus as one of the explanations of the privacy paradox through the inclusion of laziness.

Conceptualization, distinction, definition and operationalization of laziness. Based on the

personality theory we integrated laziness into McAdams' model of personality theory (McAdams 1996). We thereby conceptualized, delimited, and defined laziness as a construct. Prior research has used laziness in several research areas (e.g. medicine, psychology or IS), however, laziness has not before been conceptualized and defined as a construct. Therefore, first, we conceptualized laziness by delineating it from other similar constructs such as inertia (Polites and Karahanna 2012) or ease of use (Davis 1989) (see Table 2). Second, we defined laziness as a broad trait in which individuals summon as little energy as possible to work even if that means not reaching a goal. The clear definition, conceptualization and integration into existing theory will help other researchers in several research areas. For example, scholars in the IS adoption area can use these results and research on in how far individuals' laziness can solve questions about why some individuals adopt IS and others do not (Venkatesh et al. 2003) by using laziness as a broad trait and IS adoption as the behavior. Also, in the privacy research area, our results could help in fostering the understanding of other problems. For example, using laziness as a variable when researching on why individuals do not read privacy terms and conditions could help in receiving a new perspective on this issue (Obar 2016). Third, we operationalized laziness as a new construct by developing new items and by accounting for their semantic and statistical cohesiveness such that other scholars can use laziness in their quantitative studies.

Researching on actual behavior. An ongoing problem in current privacy research is that the majority of prior studies have only investigated the intention to disclose information rather than the actual behavior (Norberg et al. 2007). Unfortunately, the actual behavior of disclosing less personal information does not necessarily match the intention of the individuals to do so (Acquisti and Grossklags 2005c; Norberg et al. 2007). Therefore, there have been several calls for more research on actual disclosure behavior (Bélanger and Crossler 2011; Smith et al. 2011). With our study, we contribute to this research stream by providing results about actual self-disclosure behavior, confirming the results of current research by showing that the privacy paradox is true when researching on the actual behavior of individuals. Finally, our study fills the gap of research multiple snapshots in the privacy context (see Table 10 in the appendix), proving the existence of the privacy paradox over time as well.

7.2 PRACTICAL IMPLICATIONS

Our empirical investigation affirms recent suggestions that laziness could influence the self-disclosure behavior of individuals (Kwong 2015; Spencer 2014), and therefore has several practical implications:

- 1) Prior research has shown that privacy is an ongoing problem in today's society (Matt et al. 2019). In addition to the so-called "dark side of IT" (Tarafdar et al. 2013), including addiction (Turel et al. 2011), privacy harm (Heller 2016) and technostress (Tarafdar et al. 2010), practical observation indicates that individuals themselves willingly endanger their privacy by self-disclosing a vast amount of personal information. This study shows that laziness is one of the reasons why individuals disclose personal information and endanger their privacy despite privacy concerns (Acquisti et al. 2015). One practical implication of our research is that if individuals want to protect their privacy they need to overcome their laziness and start putting energy into the task of protecting their privacy. However, as laziness is a stable, broad trait, which cannot be altered (Abramson et al. 1978; Watkins et al. 2009), society needs to think about how to support lazy individuals in protecting their privacy. One way might be to implement regulatory measures that make it as easy as possible to protect privacy, for example by making default privacy threats illegal and requiring default privacy protection mechanisms. This would lower the amount of energy an individual needs to spend on protecting her privacy and protect lazy individuals' privacy as default without requiring them to spend energy to do it themselves.

2) Our results indicate that organizations that want to receive as much private information as possible will have the most success collecting personal information from individuals who exhibit a high degree of laziness, since they are more likely to disclose personal information despite privacy concerns. Although it is questionable from an ethical point of view, such organizations could invest resources in developing methods of identifying lazy individuals, and then actively target those individuals to collect personal information.

3) Knowing that laziness influences self-disclosure behavior might guide technology design (Junglas et al. 2008). For instance, organizations such as Facebook can alter their privacy control settings and design to match their claims that they are concerned about protecting privacy to avoid losing customers among the target audience of individuals who are not lazy and will translate their privacy concerns into actual behavior by lower their self-disclosure amount.

7.3 LIMITATIONS AND FUTURE RESEARCH

This study also has some limitations. Among others, we treat self-disclosure as a single variable without increments, such as other researchers have recently done (James et al. 2015). However, our used construct has already been validated and successfully used by previous research in the context of SNS (Krasnova et al. 2010). Moreover, this study was performed in an individual, private context and did not consider specific contexts in other settings, such as in an organization. This downside does not diminish the results as we only generalize it to the individual private setting. However, doing more research through extending the context, might shed an advanced view on laziness in the context of privacy. Furthermore, we did not include trust in our research model although it is usually used when including risk. However, as we wanted to strive for a parsimonious model and as we do not see the additional value of including trust to answer our research question, we excluded trust. Besides, the moderating effect of laziness increases the explained variance of the dependent variable by 2.0 percent. Although this is a rather small value, the effect size shows that laziness as a moderator has a strong effect on the explained variance. Finally, our setting with multiple snapshots was done over a period of about five months. Other cycles might reveal different results. Still, we have no reason to think that another period of time would cause fundamental different results.

Our study also opens the door for future research in several other areas. 1) Research in other contexts have shown that the opposite of something does not necessarily have to lead to the opposite outcomes (Herzberg 1966; Turel 2014). Thus, future research could investigate whether the opposite of laziness (e.g. the willingness to work hard (McCrae and Costa 1987; Schneider et al. 1994)) provides further insight into the phenomenon of the relationship between privacy concerns and self-disclosure. 2) As mentioned in the theoretical implications, the construct of laziness could be incorporated into existing research models, such as the privacy calculus model, and in developing new models. It can also be used when researching on the irrational behavior of individuals in the context of the privacy paradox. Irrational behavior is attributed to a lack of self-control (Acquisti and Grossklags 2003). According to this explanation, people might react irrationally and disclose their personal information despite their privacy concerns because they have low self-control. As scholars have linked self-control to laziness (Shefrin and Thaler 1977), our results might be used by this research stream by adding laziness alongside self-control to better explain irrational behavior in the privacy context. 3) In accordance with Kokolakis (2017), our results provide further insight into the privacy paradox, providing additional evidence that it may not be a paradox after all. Future research could build on this momentum and try to find a better term for that phenomenon. One suggestion might be privacy quandary, as individuals maybe do want to protect their privacy but they cannot do so due to the stated reasons. 4) We defined laziness as a broad trait, but other scholars have identified other narrower traits that only apply in specific IS situations, e.g. computer anxiety (Thatcher and Perrewé 2002) or personal innovativeness (Agarwal and Prasad 1998).

Future IS research could refine the definition of laziness as an IS-specific trait and alter the items of laziness accordingly.

8 CONCLUSION

In response to calls to investigate and theorize the degree to which personality traits have a moderating effect on the relationship between privacy concerns and self-disclosure behavior, this study investigates the moderating effect of the broad personality trait of laziness and indicates that laziness indeed moderates the relationship between privacy concerns and self-disclosure. Individuals who exhibit a low degree of laziness are more likely to react to privacy concerns by changing their self-disclosure than individuals who exhibit a high degree of laziness, who are more likely not to change their self-disclosure despite privacy concerns. This study casts new light on the privacy paradox, conceptualizes and operationalizes laziness as a new construct in privacy research and thus has practical and scholarly implications.

9 APPENDIX

Individual difference	Affected variable	Control variable	Antecedent	Moderator	Longitudinal	Crosswise	Disclosure intention	Disclosure behavior	N/A	Author(s)
Age	Willingness to provide access to personal health info	X				X	X			Anderson and Agarwal 2011
Age	Disclosure	X				X		X		Keith et al. 2015
Age	Internet use policy compliance intention	X				X			X	Li et al. 2014
Age	Trusting beliefs, risk beliefs, behavioral intention	X				X	X			Malhotra et al. 2004
Age	Context-specific concerns for privacy	X				X			X	Xu et al. 2012
Age	Self-disclosures on social networking websites	X				X		X		Yu et al. 2015
Big five personality traits	Concern for privacy		X			X			X	Junglas et al. 2008
Computer anxiety	privacy concerns (secondary use, errors, unauthorized use, collection)		X			X	X			Stewart and Segars 2002
Gender	Self-disclosures on social networking websites	X				X		X		Yu et al. 2015
Gender	Context-specific concerns for privacy	X				X			X	Xu et al. 2012
Gender	Trusting beliefs, risk beliefs, behavioral intention	X				X	X			Malhotra et al. 2004
Gender	Internet use policy compliance intention	X				X			X	Li et al. 2014
Gender	Willingness to provide access to personal health info	X				X	X			Anderson and Agarwal 2011
Gender	Intention to disclose private information	X				X	X			Bansal et al. 2015
Gender	Disclosure	X				X		X		Keith et al. 2015
Gender	Importance of information transparency	X				X		X		Awad and Krishnan 2006
Education	Trusting beliefs, risk beliefs, behavioral intention	X				X	X			Malhotra et al. 2004
Education	Context-specific concerns for privacy	X				X		X		Xu et al. 2012
Education	Willingness to provide access to personal health info	X				X	X			Anderson and Agarwal 2011
Education	Importance of information transparency	X				X		X		Awad and Krishnan 2006
Ethnicity	Disclosure	X				X		X		Keith et al. 2015
Internet experience	Internet use policy compliance intention	X				X			X	Li et al. 2014
Internet experience	Trusting beliefs, risk beliefs, behavioral intention	X				X	X			Malhotra et al. 2004
Privacy experience	Context-specific concerns for privacy	X				X			X	Xu et al. 2012
Positive experience with website	Intention to disclose private information	X				X	X			Bansal et al. 2015
Previous privacy experience	Disclosure privacy risks	X				X				Xu et al. 2009
Past experience	Perceived quality of personalization <-> Likelihood of using online personalization, privacy (privacy concerns and privacy protection) <-> likelihood of using online personalization		X			X		X		Li and Unger 2012
Invasion of privacy in the past	Trusting beliefs, risk beliefs, behavioral intention	X				X	X			Malhotra et al. 2004
Mobile computing self-efficacy	Perceived risk, perceived benefit, actual disclosure		X			X		X		Keith et al. 2015
Personal disposition to value privacy	Privacy control, privacy risk, privacy concerns					X			X	Xu et al. 2011
Personal innovativeness	Intention to disclose personal information	X				X	X			Xu et al. 2009
Laziness	Relationship of privacy concerns on self-disclosure		X	X	X			X		This study

Literature review in the basket of eight by using the search term "privacy". Only quantitative studies have been considered.

Table 10. Previous research on individual differences in the privacy domain

	Dependent variable
Moderator	Self-disclosure
Laziness	0.028 (strong)
Moderator variable: >0.025 = strong; >0.01 = medium; >0.005 = weak (Kenny 2015)	

Table 11. Effect size of laziness being a moderator

	Dependent variable	
Independent variables	Self-disclosure	privacy concerns
Laziness	0.009 (no effect)	
Privacy concerns	0.001 (no effect)	
Privacy risk	0.162 (medium)	0.546 (strong)
In general: >0.35 = strong; >0.15 = medium; >0.02 = weak (Cohen 1988)		

Table 12. Effect sizes of independent-dependent variables

Construct and Cronbach's alpha	Items	Loadings	Reference(s)
Privacy concerns (0.951)	When faced with this scenario, it bothers me that Facebook is able to track information about me.	0.928	Dinev and Hart 2004; Smith et al. 1996
	When faced with this scenario, I am concerned that Facebook has too much information about me.	0.932	
	When faced with this scenario, it bothers me that Facebook is able to access information about me.	0.936	
	I am concerned that the information I submitted on Facebook could be misused.	0.903	Dinev and Hart 2006; Malhotra et al. 2004
	I am concerned that a person can find private information about me on the Facebook.	0.804	
	I am concerned about threats to my personal privacy when I use Facebook.	0.876	
Privacy risk (0.866)	In general, it would be risky to give personal information to Facebook.	0.852	Xu et al. 2011
	There would be high potential for privacy loss associated with giving personal information to Facebook.	0.857	
	Personal information could be inappropriately used by Facebook.	0.779	
	Overall, I see no real threat to my privacy due to my presence on Facebook. (Reversed)	0.737	Krasnova et al. 2010
	I feel safe publishing my personal information on Facebook. (Reversed)	0.803	
Self-disclosure (0.843)	I have a comprehensive profile on Facebook.	0.825	Krasnova et al. 2010
	I find time to keep my profile up to date.	0.814	
	I keep my friends updated about what is going on in my life through the OSN.	0.882	
	When I have something to say, I like to share it on the OSN.	0.781	
Laziness (0.788)	I try to work as little as possible even if that has disadvantages for me.	0.740	Self-developed (see section five)
	I consciously try to put as little energy as possible into doing work even if that means that what I am working on will not be done properly.	0.852	
	Sometimes I do not reach my goals because I did not put enough energy into reaching them.	0.890	
Note: Scale ranges from 1 (totally disagree) to 7 (totally agree) on a 7-point Likert scale.			

Table 13. Measurement items with loadings

Laziness Level	Partial derivative of privacy concerns with respect to laziness	T-statistic
"High lazy" (>3)	0.204	1.443
"Low lazy" (<2.5)	-0.263	1.773
Mean (2.77)	0.025	0.416
Missing values have been distributed equally across both categories ("high lazy" and "low lazy")		

Table 14. Privacy concerns in respect to laziness

10 REFERENCES

- Abramson, L. Y., Seligman, M. E., and Teasdale, J. D. 1978. "Learned helplessness in humans: Critique and reformulation," *Journal of Abnormal Psychology* (87:1), pp. 49–74.
- Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), pp. 509–514.

- Acquisti, A., and Grossklags, J. 2003. "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior," in *2nd Annual Workshop on "Economics and Information Security"*, UC Berkeley.
- Acquisti, A., and Grossklags, J. 2005a. "Privacy and rationality in individual decision making," *Security & Privacy, IEEE* (3:1), pp. 26–33.
- Acquisti, A., and Grossklags, J. 2005b. "Privacy and rationality in individual decision making," *IEEE Security & Privacy* (3:1), pp. 26–33.
- Acquisti, A., and Grossklags, J. 2005c. "Privacy Attitudes and Privacy Behavior," *Camp, Lewis – Economics of Information Security* (12), pp. 165–178.
- Agarwal, R., and Prasad, J. 1998. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology," *Information Systems Research* (9:2), pp. 204–215.
- Agarwal, R., and Prasad, J. 1999. "Are Individual Differences Germane to the Acceptance of New Information Technologies?" *Decision Sciences* (30:2), pp. 361–391.
- Anderson, C. L., and Agarwal, R. 2011. "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," *Information Systems Research* (22:3), pp. 469–490.
- Ashton, M. C., Lee, K., Perugini, M., Szarota, P., Vries, R. E. de, Di Blas, L., Boies, K., and Raad, B. de 2004. "A Six-Factor Structure of Personality-Descriptive Adjectives: Solutions From Psycholinguistic Studies in Seven Languages," *Journal of Personality and Social Psychology* (86:2), pp. 356–366.
- Awad, N. F., and Krishnan, M. S. 2006. "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profile online for personalization," *MIS Quarterly* (30:1), pp. 13–28.
- Baek, Y. M. 2014. "Solving the privacy paradox: A counter-argument experimental approach," *Computers in Human Behavior* (38), pp. 33–42.
- Bala, H., and Venkatesh, V. 2016. "Adaptation to Information Technology: A Holistic Nomological Network from Implementation to Job Outcomes," *Management Science* (62:1), pp. 156–179.
- Bansal, G., Zahedi, F. M., and Gefen, D. 2015. "The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern," *European Journal of Information Systems* (24:6), pp. 624–644.
- Barclay, D., Higgins, C., and Thompson, R. 1995. "The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration," *Technology studies* (2:2), pp. 285–309.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.
- Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems* (11:3–4), pp. 245–270.
- Berry, D. M. 2004. "Internet research: privacy, ethics and alienation: an open source approach," *Internet Research* (14:4), pp. 323–332.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864.
- Boyer O'Leary, M., Wilson, J. M., and Metiu, A. 2014. "Beyond being there: The symbolic role of communication and identification in perceptions of proximity to geographically dispersed colleagues," *MIS Quarterly* (38:4), pp. 1219–1243.
- Campbell, D. T., and Fiske, D. W. 1959. "Convergent and discriminant validation by the multitrait-multimethod matrix," *Psychological Bulletin* (56:2), pp. 81–105.
- Carmines, E. G., and Zeller, R. A. 1979. *Reliability and validity assessment*, London: Sage Publications.
- Carte, T. A., and Russell, C. J. 2003. "In Pursuit of Moderation: Nine Common Errors and Their Solutions," *MIS Quarterly* (27:3), pp. 479–501.
- Cenfetelli, R. T., and Schwarz, A. 2011. "Identifying and Testing the Inhibitors of Technology Usage Intentions," *Information Systems Research* (22:4), pp. 808–823.
- Chin, W. W. 1998. "The partial least squares approach to structural equation modeling," in *Modern*

- methods for Business Research*, Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295–336.
- Choi, B., Wu, Y., Yu, J., and Land, L. 2018. "Love at First Sight: The Interplay Between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management," *Journal of the Association for Information Systems* (19:3), pp. 124–151.
- Cohen, J. 1988. *Statistical power analysis for the behavioral sciences*, Hillsdale, N.J.: L. Erlbaum Associates.
- Costa, P. T., and McCrae, R. R. 1992. *Revised NEO personality inventory (NEO PI-R) and NEO five-factor inventory (NEO FFI): Professional manual*, Odessa, FL: Psychological Assessment Resources.
- Costa, P. T., and McCrae, R. R. 1994. "Set like plaster? Evidence for the stability of adult personality," in *Can personality change?* T. F. Heatherton and J. L. Weinberger (eds.), Washington: American Psychological Association, pp. 21–40.
- Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319–340.
- Deci, E. L., and Ryan, R. M. 2000. "The "What" and "Why" of Goal Pursuits: Human Needs and the Self-Determination of Behavior," *Psychological Inquiry* (11:4), pp. 227–268.
- Devaraj, S., Easley, R. F., and Crant, J. M. 2008. "Research Note: How Does Personality Matter? Relating the Five-Factor Model to Technology Acceptance and Use," *Information Systems Research* (19:1), pp. 93–105.
- Dinev, T., and Hart, P. 2004. "Internet privacy concerns and their antecedents - measurement validity and a regression model," *Behaviour & Information Technology* (23:6), pp. 413–422.
- Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61–80.
- Eckhardt, A., Laumer, S., Maier, C., and Weitzel, T. 2016. "The effect of personality on IT personnel's job-related attitudes: establishing a dispositional model of turnover intention across IT job types," *Journal of Information Technology* (31), pp. 48–66.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18:1), pp. 39–50.
- Garrison, C. G., Burke, A., and Hollingworth, L. S. 1917. "The psychology of a prodigious child," *Journal of Applied Psychology* (1:2), p. 101.
- Gefen, D., and Straub, D. 2005. "A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example," *Communications of the Association for Information Systems* (16:1), p. 5.
- Grossklags, J., and Acquisti, A. 2007. "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information.," *WEIS* .
- Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a silver bullet," *The Journal of Marketing Theory and Practice* (19:2), pp. 139–152.
- Heller, M. 2016. *U.S. Data Breaches Almost Match Record High*. <http://ww2.cfo.com/data-security/2016/02/u-s-data-breaches-almost-match-record-high/>. Accessed 16 February 2016.
- Henseler, J., Ringle, C. M., and Sarstedt, M. 2014. "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 1–21.
- Herzberg, F. 1966. *Work and the nature of man*, New York: Thomas Y. Crowell.
- Hu, L.-T., and Bentler, P. M. 1999. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1–55.
- Jackson, J. J., Wood, D., Bogg, T., Walton, K. E., Harms, P. D., and Roberts, B. W. 2010. "What do conscientious people do? Development and validation of the Behavioral Indicators of Conscientiousness (BIC)," *Journal of research in personality* (44:4), pp. 501–511.
- James, T. L., Warkentin, M., and Collignon, S. E. 2015. "A Dual Privacy Decision Model for Online Social Networks," *Information & Management* (52:8), pp. 893–908.
- Jensen, C., Potts, C., and Jensen, C. 2005. "Privacy practices of Internet users Self-reports versus observed behavior," *International Journal of Human-Computer Studies* (63:1-2), pp. 203–227.
- Jourard, S. M. 1971. *Self-disclosure: An experimental analysis of the transparent self*, New York: Wiley-Interscience.
- Junglas, I. A., Johnson, N. A., and Spitzmüller, C. 2008. "An empirical study in the context of location-based services," *European Journal of Information Systems* (17:4), pp. 387–402.

- Kassin, S. M. 2003. *Psychology*, Upper Saddle River, NJ: Pearson/Prentice Hall.
- Keith, M. J., Babb, J., Lowry, P. B., Furner, C., and Abdullat, A. 2015. "The Role of Mobile-Computing Self-Efficacy in Consumer Information Disclosure," *Information Systems Journal* (25:6), pp. 637–667.
- Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior," *International Journal of Human-Computer Studies* (71:12), pp. 1163–1173.
- Kenny, D. A. 2015. *Moderator Variables*. <http://www.davidakenny.net/cm/moderation.htm>. Accessed 27 October 2015.
- Kim, S. S., and Malhotra, N. K. 2005. "A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena," *Management Science* (51:5), pp. 741–755.
- Kokolakis, S. 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* (64), pp. 122–134.
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online social networks: Why we disclose," *Journal of Information Technology* (25:2), pp. 109–125.
- Kwong, M. 2015. *Smart devices think you're 'too lazy' to opt out of privacy defaults*. <http://www.cbc.ca/news/technology/smart-devices-think-you-re-too-lazy-to-opt-out-of-privacy-defaults-1.2957114>. Accessed 10 August 2015.
- Landis, J. R., and Koch, G. G. 1977. "The Measurement of Observer Agreement for Categorical Data," *Biometrics* (33:1), pp. 159–174.
- Lee, H., Park, H., and Kim, J. 2013. "Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk," *Social Networks and Ubiquitous Interactions* (71:9), pp. 862–877.
- Li, H., Sarathy, R., Zhang, J., and Luo, X. 2014. "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance," *Information Systems Journal* (24:6), pp. 479–502.
- Li, T., and Unger, T. 2012. "Willing to pay for quality personalization? Trade-off between quality and privacy," *European Journal of Information Systems* (21:6), pp. 621–642.
- Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS Quarterly* (31:1), pp. 59–87.
- Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model: Information Systems Research," *Information Systems Research* (15:4), pp. 336–355.
- Matt, C., Trenz, M., Cheung, C. M. K., and Turel, O. 2019. "The digitization of the individual: conceptual foundations and opportunities for research," *Electronic Markets* (29:3), pp. 315–322.
- McAdams, D. P. 1996. "Personality, Modernity, and the Storied Self: A Contemporary Framework for Studying Persons," *Psychological Inquiry* (7:4), p. 295.
- McCrae, R. R., and Costa, P. T. 1987. "Validation of the five-factor model of personality across instruments and observers," *Journal of Personality and Social Psychology* (52:1), pp. 81–90.
- McElroy, J. C., Hendrickson, A. R., Townsend, A. M., and DeMarie, S. M. 2007. "Dispositional Factors in Internet Use: Personality versus Cognitive Style," *MIS Quarterly* (31:4), pp. 809–820.
- Nahm, A. Y., Rao, S. S., Solis-Galvan, L. E., and Ragu-Nathan, T. S. 2002. "The Q-sort method: assessing reliability and construct validity of questionnaire items at a pre-testing stage," *Journal of Modern Applied Statistical Methods* (1:1), p. 15.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.
- Nunnally, J. 1978. *Psychometric theory*: New York: McGraw-Hill.
- Obar, J. A. 2016. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services," *SSRN Electronic Journal*.
- Oxford Dictionaries 2016. *laziness*. <http://www.oxforddictionaries.com/definition/english/laziness>. Accessed 13 January 2016.
- Paunonen, S. V., and Ashton, M. C. 2001. "Big Five factors and facets and the prediction of behavior," *Journal of Personality and Social Psychology* (81:3), pp. 524–539.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common method biases

- in behavioral research: a critical review of the literature and recommended remedies,” *Journal of Applied Psychology* (88:5), p. 879.
- Polites, G. L., and Karahanna, E. 2012. “Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance,” *MIS Quarterly* (36:1), pp. 21–42.
- Pu, Y., and Grossklags, J. 2015. “Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios,” in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- Puhl, R., and Brownell, K. D. 2001. “Bias, Discrimination, and Obesity,” *Obesity Research* (9:12), pp. 788–805.
- Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., and Qiang Tu 2008. “The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation,” *Information Systems Research* (19:4), pp. 417–433.
- Ryan, R. M., and Deci, E. L. 2000. “Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions,” *Contemporary Educational Psychology* (25:1), pp. 54–67.
- Schneider, L., Reynolds, C. F., Lebowitz, B., and Friedhoff, A. J. 1994. *Diagnosis and treatment of depression in late life: Results of the NIH Consensus Development Conference*, Washington, DC: American Psychiatric Press.
- Sheeran, P. 2002. “Intention—Behavior Relations: A Conceptual and Empirical Review,” *European Review of Social Psychology* (12:1), pp. 1–36.
- Shefrin, H. M., and Thaler, R. 1977. “An Economic Theory of Self-Control,” *National Bureau of Economic Research Working Paper Series* (No. 208).
- Skinner, G., Han, S., and Chang, E. 2006. “An information privacy taxonomy for collaborative environments,” *Information Management & Computer Security* (14:4), pp. 382–394.
- Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. “Information Privacy: Measuring Individuals' Concerns About Organizational Practices,” *MIS Quarterly* (20:2), pp. 167–196.
- Smith, J. H., Dinev, T., and Xu, H. 2011. “Information privacy research: An interdisciplinary review,” *MIS Quarterly* (35:4), pp. 980–1015.
- Son, J.-Y., and Kim, S. S. 2008. “Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model,” *MIS Quarterly* (32:3), pp. 503–529.
- Spencer, L. 2014. *Laziness at the expense of privacy and freedom: John McAfee*. <http://www.zdnet.com/article/laziness-at-the-expense-of-privacy-and-freedom-john-mcafee/>. Accessed 10 August 2015.
- statista.com 2018. *Most famous social network sites worldwide as of January 2018, ranked by number of active users (in millions)*. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>. Accessed 20 March 2018.
- Steelman, Z. R., Hammer, B. I., and Limayem, M. 2014. “Data Collection in the Digital Age: Innovative Alternatives to Student Samples,” *MIS Quarterly* (38:2), pp. 355–378.
- Stewart, K. A., and Segars, A. H. 2002. “An Empirical Examination of the Concern for Information Privacy Instrument,” *Information Systems Research* (13:1), pp. 36–49.
- Tarafdar, M., Gupta, A., and Turel, O. 2013. “The dark side of information technology use,” *Information Systems Journal* (23:3), pp. 269–275.
- Tarafdar, M., Tu, Q., and Ragu-Nathan, T. S. 2010. “Impact of Technostress on End-User Satisfaction and Performance,” *Journal of Management Information Systems* (27:3), pp. 303–334.
- Thatcher, J. B., and Perrewé, P. L. 2002. “An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy,” *MIS Quarterly* (26:4), pp. 381–396.
- Turel, O. 2014. “Quitting the use of a habituated hedonic information system: a theoretical model and empirical examination of Facebook users,” *European Journal of Information Systems* (42:4), pp. 431–446.
- Turel, O., Serenko, A., and Giles, P. 2011. “Integrating technology addiction and use: An empirical investigation of online auction users,” *MIS Quarterly* (35:4), pp. 1043–1062.
- van Eerde, W., and Thierry, H. 1996. “Vroom's expectancy models and work-related criteria: A meta-analysis,” *Journal of Applied Psychology* (81:5), pp. 575–586.
- Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. “User acceptance of information technology: toward a unified view,” *MIS Quarterly* (27:3), pp. 425–478.

- Vroom, V. H. 1964. *Work and motivation*, New York: Wiley.
- Wakefield, R. 2013. "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157–174.
- Watkins, E. R., Baeyens, C. B., and Read, R. 2009. "Concreteness training reduces dysphoria: Proof-of-principle for repeated cognitive bias modification in depression," *Journal of Abnormal Psychology* (118:1), pp. 55–64.
- Williams, L. J., Edwards, J. R., and Vandenberg, R. J. 2003. "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management* (29:6), pp. 903–936.
- Williams, M. D., Dwivedi, Y. K., Lal, B., and Schwarz, A. 2009. "Contemporary trends and issues in IT adoption and diffusion research," *Journal of Information Technology* (24:1), pp. 1–10.
- Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798–824.
- Xu, H., Teo, H.-H., Tan, Bernard C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services: Journal of Management Information Systems," *Journal of Management Information Systems* (26:3), pp. 135–174.
- Xu, H., Teo, H.-H., Tan, Bernard C. Y., and Agarwal, R. 2012. "Research note-effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services," *Information Systems Research* (23:4), pp. 1342–1363.
- Yu, J., Hu, P. J.-H., and Cheng, T.-H. 2015. "Role of Affect in Self-Disclosure on Social Network Websites: A Test of Two Competing Models: A Test of Two Competing Models," *Journal of Management Information Systems* (32:2), pp. 239–277.
- Zhan, G., and Zhou, Z. 2018. "Mobile internet and consumer happiness: the role of risk," *Internet Research* (28:3), pp. 785–803.

Paper VI

TECHNOSTRESS AND THE HIERARCHICAL LEVELS OF PERSONALITY

A TWO-WAVE STUDY WITH MULTIPLE DATA SAMPLES

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Jakob Wirth

University of Bamberg

Tim Weitzel

University of Bamberg

Paper VII

THE EFFECT OF MINDFULNESS ON THREAT APPRAISAL AND COPING APPRAISAL AN EMPIRICAL ANALYSIS

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Tim Weitzel

University of Bamberg

A prior version has been presented and discussed at the the 38th International Conference on Information Systems, Seoul, South Korea: Wirth et al. 2017

THE EFFECT OF MINDFULNESS ON THREAT APPRAISAL AND COPING APPRAISAL

AN EMPIRICAL ANALYSIS

Abstract

Individuals are facing numerous privacy threats. To protect against them, they evaluate the threat (threat appraisal) and the extent they can cope with it (coping appraisal). Both has an influence on their intention to protect. Whereas previous research has rather focused on these relationships, less research has been conducted to find out what determines the level of threat appraisal and coping appraisal. In this study, mindfulness is included as antecedent of threat appraisal and coping appraisal. Based on the protection motivation theory (PMT), a research model is created, where mindfulness is split upon two concepts: mindfulness on threat appraisal and mindfulness on coping appraisal. A survey with 171 participants is carried out, supporting most of the hypotheses which state that both concepts of mindfulness respectively have a positive effect on threat appraisal and on coping appraisal. The results contribute among others to literature by hinting on the importance of mindfulness when considering threat appraisal and coping appraisal.

Keywords: Protection motivation theory, privacy, antecedents, mindfulness

1 INTRODUCTION

Individuals face a range of privacy threats, for instance, email tracking (Bender et al. 2016; Fabian et al. 2015). Email tracking is prevalent since roughly all newsletters and about every fifth conversational email is using email tracking (Brunet 2017; Merchant 2017), potentially causing severe harm to recipients of such emails (Xu et al. 2018).

However, although individuals can often protect their privacy, e.g. in case of email tracking, privacy protection behavior is surprisingly diverse. Not everyone protects their privacy, e.g. against email tracking (Xu et al. 2018). Research in the field of information systems (IS) suggests that the protection intention of individuals generally depends on their appraisal of the privacy threat and their appraisal of how they can cope with it (Rogers and Prentice-Dunn 1997). If the privacy threat is expected to cause severe harm or expenses, the intention to protect against that privacy threat is greater than in cases with only minor anticipated damages (Mousavizadeh and Kim 2015; Rogers and Prentice-Dunn 1997). Thus, finding out what leads to certain appraisals is instrumental in understanding why individuals are often so less motivated to protect their privacy. However, the focus on previous privacy-related research is usually on appraisal outcomes and not on the question what leads to certain appraisals in the first place (Anderson and Agarwal 2010; Boss et al. 2015; Chen and Zahedi 2016).

Research in the field of psychology suggests that mindfulness of individuals is a factor determining threat and coping appraisal (Epel et al. 2009; Garland et al. 2011; Weinstein et al. 2009). Mindfulness is considered to be a personality trait through which individuals can reach an alert and aware state of being (Langer 1989b). Based on the assumptions of previous research, mindfulness might help in explaining different levels of threat appraisal and coping appraisal in the domain of privacy.

Therefore, this research study aims at investigating to what extent mindfulness influences an individual's appraisal about a certain privacy threat (threat appraisal) and how to cope with it (coping appraisal). The goal is to better understand both concepts which depicts a first step to better understand the protection intention of individuals. Our research question is:

What is the influence of mindfulness on an individual's threat appraisal and coping appraisal?

We draw on protection motivation theory (PMT, Rogers and Prentice-Dunn 1997) which depicts the process of threat and coping appraisal. In particular, the PMT has two main processes: The *threat appraisal* through which individuals evaluate to what degree the actual issue (e.g. email tracking) is an actual threat and the *coping appraisal*, through which individuals evaluate to what degree they are able to protect against the threat. We theorize that mindfulness influences both appraisal concepts, i.e. the threat appraisal and the coping appraisal.

The remainder of the paper is organized as follows. In the next section, we present theoretical foundations for the PMT and mindfulness. Then, we depict our research model and present the methodology of the study. Finally, we discuss the results of this study by providing contributions for literature and practice as well as guidance for future research.

2 THEORETICAL BACKGROUND

To provide a theoretical foundation, we next focus the protection motivation theory (PMT) and explain this theory in a privacy setting. Then, we introduce the mindfulness concept and position it in the PMT and the privacy context.

2.1 PROTECTION MOTIVATION THEORY

The PMT has its origins in the healthcare domain. Here, the PMT has been applied to find out what determines an individual to protect its own health (Rogers and Prentice-Dunn 1997). Thereby, two main processes could be identified: The *threat appraisal* through which individuals evaluate to what degree the actual issue (e.g. email tracking) is an actual threat; and the *coping appraisal*, through which individuals evaluate to what degree they are able to protect against the threat. Both of them have then be included in the PMT which has then also be applied in the IS domain. In the following, the threat appraisal and the coping appraisal are presented in more detail. Afterwards, the results of a literature review are presented, describing in how far previous literature has included the PMT in IS research studies.

2.1.1 Threat appraisal

In this process, individuals evaluate how much the potential danger could threaten them and whether the level of fear of this potential danger outweighs the possible maladaptive rewards. A threat is a source of danger which causes loss of control over authentic personal information, resulting in harm to the individual (Floyd et al. 2000). In particular, individuals assess the *perceived threat severity*, meaning how significant the threat could be to them and what possible harm the threat might cause to them. On the other hand, they also evaluate the *perceived threat vulnerability* by considering their own susceptibility to the threat (Rogers and Prentice-Dunn 1997). For example, in case of email tracking, individuals consider in how far email tracking might actually harm them (perceived threat severity). In a second step, they evaluate if they are even prone to email tracking (perceived threat vulnerability). For example, someone who has no email account might consider email tracking to be severe, yet, considers its own vulnerability as low. Based on the evaluation of the severity and vulnerability of the threat, individuals generate a certain level of *fear* against the threat. Fear is thereby defined as "*a relational construct aroused in response to a situation that is judged as dangerous*" (Rogers 1975, p. 96).

Maladaptive rewards present an evaluation of the received benefits of not protecting against the threat (Boss et al. 2015; Rogers and Prentice-Dunn 1997). That means, it is about the advantages that the individual receives when she is not protecting against the threat. For example, protecting against email tracking might have the effect that emails are not displayed correctly anymore. This could be avoided when one is not protecting against email tracking, which represents the maladaptive rewards.

Concept	Definition	Author(s)
Perceived threat severity	Degree of significance of the threat	Rogers and Prentice-Dunn (1997)
Perceived threat vulnerability	Degree of own susceptibility to the threat	Rogers and Prentice-Dunn (1997)
Fear	A relational construct aroused in response to a situation that is judged as dangerous	Rogers (1975, p. 96)
Maladaptive rewards	Degree of possible benefits when not protecting against the threat	Rogers and Prentice-Dunn (1997)

Table 1. Concepts of threat appraisal

An overview of the threat appraisal is given in Table 1. After having evaluated the threat, the individual appraises in how far she can cope with the threat.

2.1.2 Coping appraisal

In this process, individuals evaluate to what degree they are capable of protecting themselves against the threat. Their efficacy must outweigh the possible costs of protecting against the threat (Boss et al. 2015; Rogers and Prentice-Dunn 1997). Individuals thereby assess their *response efficacy*, which is the degree to which the particular response is a sufficient response to mitigate the threat (Maddux and Rogers 1983). For example, individuals consider protection mechanisms against email tracking and evaluate in how far they would help to actually mitigate email tracking. At the same time, individuals also assess their *self-efficacy*, which is their capability to conduct the response (Rogers and Prentice-Dunn 1997). Again, considering the example of email tracking, individuals would then rate in how far they are even capable to conduct the protection mechanisms.

In addition to efficacy, individuals also rate the *response costs*, which are expenditures associated with protecting against the threat (Floyd et al. 2000). For example, the protection behavior can be time-consuming or might gain additional costs. In case of protecting against email tracking, this might require an induction into protection against email tracking and also continuous attention. Both could be avoided if one is not protecting against email tracking.

Concept	Definition	Author(s)
Response efficacy	Degree to which the particular response is a sufficient response	Maddux and Rogers (1983)
Self-efficacy	Degree of how capable an individual is to conduct the response	Rogers and Prentice-Dunn (1997)
Response costs	Expenditures associated with the response	Floyd et al. (2000)

Table 2. Concepts of coping appraisal

An overview of the concepts related to coping appraisal is given in Table 2. Previous research has applied the PMT with threat appraisal and coping appraisal in several settings. However, the focus was often on the outcomes of both appraisals and less on antecedents.

2.2 ANTECEDENTS OF THE PROTECTION MOTIVATION THEORY

Previous research in the domain of IS has often included the PMT into their research studies. The majority of them have done research in the domain of security (e.g., Johnston and Warkentin 2010), however, several of them have also applied the PMT in other research areas such as privacy (e.g., Mousavizadeh and Kim 2015) or avoidance of IS (e.g., Liang and Xue 2009). In this study, a literature review has been conducted, to present the current state of research on studies that have applied the PMT. Thereby, a focus was also on in how far studies focused on outcomes and on antecedents of threat

appraisal and coping appraisal. An overview is given in Table 7 in the appendix.

The results of the literature review reveal that the majority of previous research studies have focused on the outcomes of threat appraisal and coping appraisal (e.g., Han et al. 2011; Herath and Rao 2009; Johnston et al. 2015; Sonnenschein et al. 2016). Although that is certainly important because the outcomes of the threat appraisal and the coping appraisal then determine the actual protection intention and behavior, antecedents are important as well because of the determining character of subsequent protection intention. However, only a minority of previous research has focused on such antecedents: Herath et al. (2014) state that the coping appraisal is also influenced by the usefulness of the technology that will ultimately lead to protect against the threat. Also, the level of privacy concerns of an individual has an effect on the coping appraisal. Mousavizadeh and Kim (2015) focus on the presence of privacy assurance and the presence of privacy personalization. They state that both have an effect on the level of threat appraisal and coping appraisal. Posey et al. (2015) focus on the security education, training, and awareness. According to their study, both will have an effect on the level of coping appraisal and threat appraisal. Finally, Zahedi et al. (2015) include a benefit and cost component into the PMT. They state that the accuracy and the speed of a detector of threats will influence the coping appraisal whereas the costs of a possible error will influence the threat appraisal.

Whereas these research studies have gained valuable insight into the formation of threat appraisal and coping appraisal, more research in this domain is necessary. This is because threat appraisal and coping appraisal are both influenced by personality traits (Rogers and Prentice-Dunn 1997) which is something previous research in the IS domain has not yet accounted for. Generally, personality traits are dispositions that distinguish individuals from each other (McCrae and Costa 2006). Mindfulness is such a personality trait (Baer et al. 2006). Furthermore, mindfulness has already been shown to influence threat appraisal and coping appraisal in the context of stress (Epel et al. 2009; Garland et al. 2011; Weinstein et al. 2009). However, research in the privacy domain, applying the PMT, has rather neglected to include mindfulness into their studies. This constitutes a research gap and offers promising opportunities to better understand why individuals have a certain level of threat appraisal and coping appraisal. Therefore, in the following section, we introduce mindfulness in the context of privacy.

2.3 MINDFULNESS AND PRIVACY

Mindfulness of individuals has gained more and more attraction by recent researchers in the field of IS (Butler and Gray 2006; Cram and Newell 2016; Dernbecher and Beck 2017; Sun et al. 2016; Thatcher et al. 2018). For example, usage (Thatcher et al. 2018) and adoption of technology (Sun et al. 2016), agile development of IS (Cram and Newell 2016), reliability of IS (Butler and Gray 2006), collective minding in organizations (Carlo et al. 2012) or adoption of RFID (Goswami et al. 2008) just to name a few. Please see Table 7 in the appendix for an overview of prior studies, applying mindfulness in the area of IS.

Mindfulness is generally a condition of an individual where she is an alert and aware state of being (Langer 1989a, 1989b). Individuals who are mindful can better react on and adapt to changes in their environment (Fiol et al. 2009), their well-being is increased (Brown and Ryan 2003), they have a higher reliability (Butler and Gray 2006) and a higher resistance to bandwagon effects (Wolf et al. 2012). However, since some for some individuals it is easier to reach such a mindful state than for others (Dane 2011), mindfulness is often considered from the viewpoint of being a trait (Baer et al. 2006). Particularly, in the IS-domain, traits can be measured as either being broad, context-independent predispositions (Allport 1961), as stable, IS-specific traits that are stable across situations (Thatcher and Perrewé 2002) or as dynamic, IS-specific traits that vary across situations (Davis and Yi 2012). Previous research in the IS domain has focused on mindfulness being a dynamic, IS-specific trait

(Thatcher et al. 2018). Since we also include mindfulness in the domain of IS, and as it is recommended to adapt mindfulness to the particular situation, we concur with this view and consider mindfulness to be a dynamic, IS-specific trait.

The mindfulness concept consists of four facets (Langer 1989a, 1989b; Thatcher et al. 2018). *Novelty seeking* is about being open and curious towards the environment (Bodner and Langer 2001; Langer 1989a) or towards novelty in general (Butler and Gray 2006). *Engagement* is about being aware and inclined to attend to changes in the environment and therefore being more aware of local contexts by gathering more details about the context. Whereas novelty seeking is more about being open and curious towards all information of the environment, engagement is more about actually noticing details in the environment (Langer 1989a; Langer 2004). *Novelty production* is about being able to produce new knowledge by learning more about the current situation (Bodner and Langer 2001; Langer 1989a) and to refrain from solely relying on old information and distinctions (Haigh et al. 2011; Langer 1989a). *Flexibility* is about being able to take different perspectives to assess multiple implications (Bodner and Langer 2001; Langer 1989a). An overview of all four facets is provided in Table 3.

Facet	Definition	Author(s)
Novelty seeking	Degree of openness and curiosity	Butler and Gray (2006)
Engagement	Degree of awareness to changes in the environment	Langer (1989a); Langer (2004)
Novelty production	Degree of production of new knowledge	Bodner and Langer (2001); Langer (1989a)
Flexibility	Degree of taking in different perspectives	Bodner and Langer (2001); Langer (1989a)

Table 3. Four facets of mindfulness

To apply mindfulness in a specific context, e.g. privacy, research has urged to not rely on a general concept of mindfulness but rather adapt it to the particular research context. The rationale for this is that a concept adapted to a particular context has a higher explanatory power (Thatcher et al. 2018). Therefore, we adapt mindfulness to the context of privacy in the domain of the PMT of both threat appraisal and coping appraisal by aligning all four facets of mindfulness to both concepts. In a privacy-context, then, individuals can have different levels of mindfulness which either influence threat appraisal or coping appraisal. For example, individuals can be very mindful on email tracking as a threat but lowly mindful on how to protect themselves against email tracking. In other words, individuals might be highly mindful on the threat appraisal but lowly mindful on coping appraisal or vice versa. Therefore, when adapting mindfulness to the context of privacy in the scope of the PMT, one needs to adapt mindfulness to threat appraisal and coping appraisal by adapting all four mentioned facets of mindfulness to both concepts.

Mindfulness on threat appraisal: Individuals with high levels of *novelty seeking* in the context of threat appraisal are more open and curious about possible privacy threats in their environment. They will not process this information automatically (Sun and Fang 2010) but will be more active to gather information about privacy threats (Sun et al. 2016). For example, these individuals are curious about data breaches (Goel and Perlroth 2016), email tracking (Bender et al. 2016) or all other issues which might be considered as a threat to their privacy.

Individuals with high levels of *engagement* in the context of threat appraisal are more likely to attend to changes in the environment regarding ongoing particular privacy threats. For example, these individuals are more aware of ongoing practices about email tracking as a privacy threat, and they are more likely to gather details about the privacy threat and how it has evolved over the years.

Individuals with high levels of *novelty production* in the context of threat appraisal are more able to learn about privacy threats because they rely more on newly gathered information. For example, these individuals are able to learn about email tracking by processing new information, e.g. from the news, rather than relying on old information.

Individuals with high levels of *flexibility* in the context of threat appraisal are more able to assess the implications of privacy threats, also from different perspectives. For example, these individuals are able to ask in how far email tracking as a privacy threat has any implications for themselves but also in how far email tracking has any implications for other individuals or organizations.

Mindfulness on coping appraisal: Individuals with high levels of *novelty seeking* in the context of coping appraisal are more open towards and curious about possible mechanisms to protect themselves against privacy threats. For example, they are curious about what possibilities exist to protect against email tracking (Bender et al. 2016) to protect their privacy.

Individuals with high levels of *engagement* in the context of coping appraisal are more likely to attend to changes which affect their privacy protection. They go into more detail about particular privacy protection mechanisms and, for example, assess different protection mechanisms, that exist to protect against email tracking (Bender et al. 2016).

Individuals with high levels of *novelty production* in the context of coping appraisal rely on new rather than on old information when it comes to their privacy protection. For example, they are able to gain knowledge on different privacy protection mechanisms, and also update their knowledge on these protection mechanisms based on environmental information.

Individuals with high levels of *flexibility* in the context of coping appraisal are more able to assess in how far the usage of different privacy protection mechanisms has implications for themselves and also for others. For example, they can better assess the extent protecting against email tracking might have consequences beyond more privacy protection and in how far others, e.g. friends or organizations, benefit or suffer from protecting against email tracking.

Summary: All in all, adapting mindfulness to the concepts of threat and coping appraisals in the context of privacy results in the concepts of *mindfulness on threat appraisal* and *mindfulness on coping appraisal*. Both have four facets as suggested by previous research (Langer 1989a, 1989b; Thatcher et al. 2018). However, the facets of threat appraisal differ from the facets of coping appraisal as both are adapted to the particular domain of privacy threats and privacy coping.

To find out, in how far both concepts of mindfulness indeed influence the appraisal of a threat and the appraisal how to cope with the threat, a research model, based on the PMT, is created.

3 RESEARCH MODEL

The research model (see Figure 1) is built upon the PMT, which depicts the process of threat appraisal and coping appraisal. Mindfulness on threat appraisal as well as mindfulness on coping appraisal are then included. Sticking with previous research, both mindfulness dimensions are concepts with four facets, expressed by a second-order construct (Thatcher et al. 2018). Therefore, hypotheses will be developed not for every facet individually but rather for the respective second-order construct.

An individuals' threat appraisal consists of perceived threat severity, perceived threat vulnerability, and maladaptive rewards. An individuals' coping appraisal consists of response efficacy, response costs and self-efficacy. To research on the relationship between mindfulness and both, threat appraisal and coping appraisal, we analyze the influence of mindfulness on these six particular entities. Furthermore, perceived threat severity and perceived threat vulnerability have an effect on fear which then influences the outcome variable, which is the intention to protect. However, concepts of threat appraisal as well as of coping appraisal also have an effect on the outcome variable. In this study, the intention to protect is the intention to protect against email tracking. Hypotheses for all relationships are given below.

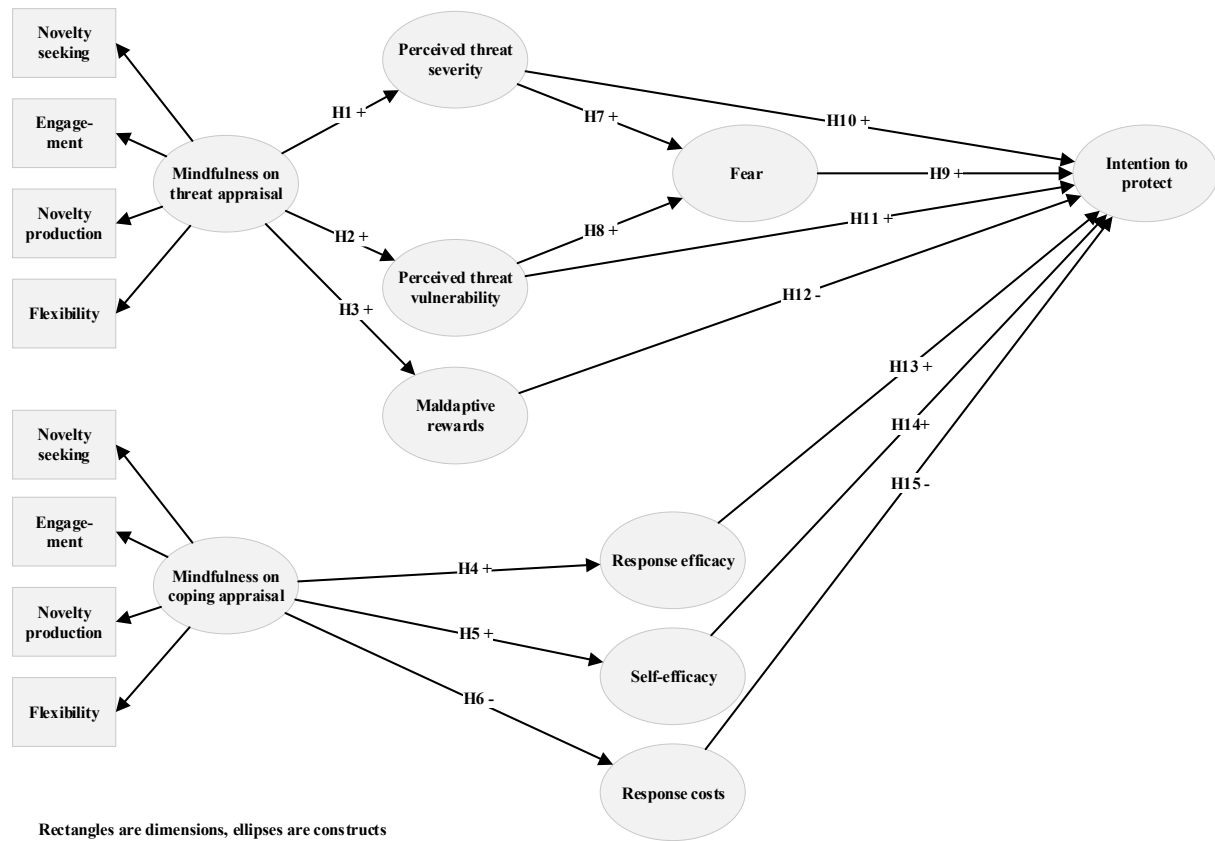


Figure 1. Research model

The research model is depicted in Figure 1. In the following, the hypotheses are developed.

3.1 THE INFLUENCE OF MINDFULNESS ON THREAT APPRAISAL

Previous research in the context of stress states that individuals who are mindful have a lower threat appraisal. This is because individuals who are mindful can re-construe events as more benign or beneficial (Epel et al. 2009; Garland et al. 2011; Weinstein et al. 2009). Contrary to previous research, we argue that individuals who are mindful on threat appraisal have a higher threat appraisal in the context of privacy threats. Justifications are given below for perceived threat severity, perceived threat vulnerability as well as maladaptive rewards.

Individuals assessing threat severity evaluate in how far a threat would be of possible harm for themselves (Rogers and Prentice-Dunn 1997). Privacy threats can cause different harm to individuals, e.g. email tracking may lead to severe outcomes such as burglars trying to burgle into a house (Xu et al. 2018). Individuals who are mindful on threat appraisal are more open towards informing themselves about privacy threats in general (*novelty seeking*) and they can also evaluate the changing nature of privacy threats (*engagement*). These individuals therefore know more about how such privacy threats, such as email tracking, can result in negative outcomes (*novelty production*). Due to their high level of mindfulness, they can also better assess privacy threats by asking in how far privacy threats might result in severe outcomes for themselves or others (*flexibility*). Hence, we hypothesize the following:

H1: The higher the mindfulness on threat appraisal, the higher the perceived threat severity.

Individuals, assessing their own vulnerability to a threat, evaluate in how far they are in danger to lose control over their personal information (Bélanger and Crossler 2011; Rogers and Prentice-Dunn 1997). Previous research has shown that individuals often underestimate their own vulnerability due to privacy threats (Acquisti and Grossklags 2005). Yet, individuals, who are mindful on threat appraisal in

general are less likely to underestimate their own vulnerability because they have a higher understanding of the changing nature of privacy threats (*engagement*). For example, these individuals know that due to the massive amount email tracking, every individual can be a victim including themselves (Abbott 2017; Gidda 2013; Goel and Perlroth 2016). This is because these individuals are more curious about privacy threats (*novelty seeking*), they gain new knowledge on privacy threats (*novelty production*) and they also consider these privacy threats from different perspectives (*flexibility*). Thus, they are more likely to perceive situations where disclosing information online leads to a potential loss of control about the information as a potential privacy threat. We therefore hypothesize:

H2: The higher the mindfulness on threat appraisal, the higher the perceived threat vulnerability.

Individuals assess the maladaptive rewards, by evaluating what benefits they would gain in case they do not protect against the threat (Rogers and Prentice-Dunn 1997). Although the non-protection of privacy can result in adverse outcomes (Karwatzki et al. 2017) it might also have positive effects. For example, not protecting against email tracking, might lead to a better representation of the email (Bender et al. 2016). Individuals, who are more mindful on privacy threats in general should also be more aware of such possible maladaptive rewards. They are more open towards privacy threats (*novelty seeking*) and are aware of the environment of privacy threats (*engagement*). They also know that they can lead to severe outcomes – however, as they have also assessed privacy threats through different perspectives (*flexibility*) and have gained a wide knowledge on them, they also know that not protecting against them will lead to certain benefits (*novelty production*). Therefore, individuals who are more mindful on privacy threats should also be more aware of the potential benefits when not protecting against the threats. Hence, we hypothesize the following:

H3: The higher the mindfulness on threat appraisal, the higher the maladaptive rewards.

After having evaluated the possible privacy threat, individuals then consider in how far they can cope with the threat. Mindfulness might increase their level of coping appraisal.

3.2 THE INFLUENCE OF MINDFULNESS ON COPING APPRAISAL

Previous research on stress suggests that individuals who are more mindful show a higher coping appraisal (Epel et al. 2009; Garland et al. 2011; Weinstein et al. 2009). Accordingly, we argue that mindfulness increases coping appraisal in the context of privacy as well. Coping appraisal consists of response efficacy, response costs and self-efficacy. Justifications for the hypotheses for each of the three concepts are given below.

By evaluating the response efficacy, individuals assess in how far protecting against the threat would actually help to cope with the threat (Rogers and Prentice-Dunn 1997). For example, in case of email tracking, individuals can protect against it by applying several technical measures with some of them being very effective responses (Bender et al. 2016). Individuals who are more mindful on coping appraisal are generally open towards protection mechanisms (*novelty seeking*), they know more about possible privacy protection mechanisms and can better assess them (*novelty production*), such as protection mechanisms against email tracking. These individuals are also more aware of the changing nature of behavioral responses that exist to protect their privacy (*engagement*), how effective these responses are to cope with the privacy threat and what are the consequences of coping for themselves and for others (*flexibility*). Therefore, we hypothesize:

H4: The higher the mindfulness on coping appraisal, the higher the response efficacy.

Self-efficacy to conduct a certain action is a self-evaluation of an individual if she is capable of

performing that action to cope with a threat (Rogers and Prentice-Dunn 1997). For example, an individual who has a high self-efficacy is more confident to be able to apply technical measures to protect against privacy threats such as email tracking. Individuals who are more mindful on coping appraisal are generally curious on protection mechanisms (*novelty seeking*), they have actively scanned the environment for possible privacy protection mechanisms (*engagement*) and gained new knowledge on privacy protection (*novelty production*) from different perspectives (*flexibility*). Therefore, they have a higher self-efficacy since through their created knowledge they are more self-confident to conduct the action such as protection measures against email tracking. We hypothesize:

H5: The higher the mindfulness on coping appraisal, the higher the self-efficacy.

Individuals who assess the response costs ask themselves what possible costs are associated with protecting their privacy (Rogers and Prentice-Dunn 1997). Possible costs refer, for instance, to effort or time (Boss et al. 2015). For example, individuals need some time to think about how to protect against email tracking. However, individuals who are mindful on coping appraisal are generally curious about possible privacy protection mechanisms (*novelty seeking*) and have already gained some knowledge on privacy protection (*novelty production*). They have scanned the environment for possibilities to protect their privacy (*engagement*) and learned more about privacy protection than individuals who are less mindful. They therefore have more knowledge on the particular protection behavior and are also better able to assess the consequences of the behavior for themselves and for others (*flexibility*). When knowing more about a certain action, less time is required to think about and to conduct the action (Kellogg 1987). Individuals who are mindful have gained such knowledge. Hence, these individuals consider time and effort to protect their privacy to be lower due to their mindfulness on coping appraisal. We therefore hypothesize the following:

H6: The higher the mindfulness on coping appraisal, the lower the response costs.

3.3 THE INFLUENCE OF THREAT APPRAISAL AND COPING APPRAISAL ON THE PROTECTION INTENTION

The main factors comprising the PMT refer to the effect of the threat appraisal and coping appraisal on the intention to protect. In the following, the hypotheses regarding these factors are explained.

Regarding the perceived level of threat severity and perceived level of threat vulnerability, individuals assess them which then determines their level of fear. In case a threat is severe, i.e. may cause particular harm and individuals are vulnerable to that threat, i.e. their own susceptibility is high, then fear is the natural response to that judgement (Rogers 1983). For example, in case individuals think that email tracking will cause severe harm and that they are vulnerable to email tracking, their level of fear will also be increased. Therefore, in line with previous research (Boss et al. 2015), we hypothesize:

H7: The higher the perceived threat severity, the higher the fear.

H8: The higher the perceived threat vulnerability, the higher the fear.

Fear itself is an undesirable condition (Rogers 1975). Hence, individuals try to avoid fear to feel better. One way in the domain of the PMT is to conduct the protection behavior. In this case, the threat would be diminished, leading to a reduced level of fear. For example, protecting against email tracking will lead to less severe outcomes, reducing the level of fear. Therefore, individuals who have a high level of fear due to a threat are more likely to protect against that threat to reduce that level of fear. In line with previous research (Boss et al. 2015), we hypothesize:

H9: The higher the fear, the higher the intention to protect.

Perceived threat severity and perceived threat vulnerability also have a direct effect on the protection intention. This is because individuals want to avoid negative outcomes and to maximize positive outcomes (van Eerde and Thierry 1996). If an individual considers a threat to be severe and to be vulnerable to that threat, then not protecting against the threat will lead to more negative than positive outcomes. Therefore, in case threat severity and threat vulnerability are high, then the individual will be more likely to protect against the threat to avoid negative outcomes. For example, in case of email tracking, if individuals think that email tracking is a severe threat and they are vulnerable to it, they will be more likely to protect against it to avoid the severe outcomes. In line with previous research (Boss et al. 2015), we hypothesize:

H10: The higher the perceived threat severity, the higher the intention to protect.

H11: The higher the perceived threat vulnerability, the higher the intention to protect.

The maladaptive rewards present the benefits the individual will receive in case when not protecting against the threat (Rogers and Prentice-Dunn 1997). Individuals aim to maximize their benefits and to minimize possible negative outcomes (van Eerde and Thierry 1996). In case individuals consider possible maladaptive rewards when not protecting against a threat, then they will be more likely to conduct that response to receive the benefits. For example, in case not protecting against email tracking will give the individual benefits, e.g. in terms of a better look-and-feel of emails, then the individual will be less likely to protect against email tracking. In line with previous research (Boss et al. 2015), we hypothesize:

H12: The higher the maladaptive rewards, the lower the intention to protect.

Besides the threat appraisal, individual's consideration of the coping appraisal has an effect on her intention to protect. Response efficacy is one part of coping appraisal and represents the degree to which the individual thinks that conducting the response will actually lead to the anticipated protection (Rogers and Prentice-Dunn 1997). If individuals think that conducting the response will lead to the anticipated protection, they will be more likely to do so because then they will mitigate negative outcomes of the threat and receive more positive outcomes. For example, if individuals find a response to be very efficient to block email tracking they will be more likely to do so because they think that they will then effectively mitigate the threat. In line with previous research, we hypothesize:

H13: The higher the response efficacy, the higher the intention to protect.

Individuals also have a particular level of self-efficacy which reflects their perceived ability to actually be able to conduct a response to protect themselves (Rogers and Prentice-Dunn 1997). In case individuals consider themselves to be capable to conduct the response, they will also be more likely to do so. This is because being able to do so, represents a necessary prerequisite to conduct the response to protect against the threat. For example, if individuals think that they have the necessary capabilities to protect against email tracking they will be more likely to do so. Hence, in line with previous research (Boss et al. 2015), we hypothesize:

H14: The higher the self-efficacy, the higher the intention to protect.

Individuals try to minimize costs and to maximize benefits (van Eerde and Thierry 1996). High response costs means that the costs of protection against email tracking might exceed the benefits out of it (Floyd et al. 2000). Through conducting the protection behavior, individuals would then not be able to maximize their benefits and to minimize their costs. Hence, in case response costs are high, individuals will be less likely to conduct the response to avoid the associated costs (Rogers 1983). For example, in case of email tracking, individuals might have to invest some time and effort to understand

how to protect against email tracking. To avoid these costs, individuals will then be less likely to protect against email tracking. In line with previous research (Boss et al. 2015), we hypothesize:

H15: The higher the response costs, the lower the intention to protect.

To evaluate our hypotheses, an empirical study has been conducted. The methodology is presented in the following section.

4 METHODOLOGY

The aim of this study is to research on the effect of mindfulness on threat appraisal and the effect of mindfulness on coping appraisal. To do so, mindfulness has been adapted to the privacy domain and has been split into two concepts: mindfulness on threat appraisal and mindfulness on coping appraisal. The PMT serves as the basic underlying theory of this research study. The context of the concepts of the PMT is the protection against email tracking (Bender et al. 2016).

4.1 EMAIL TRACKING AS THE CONTEXT OF THE SURVEY

Reasons, why email tracking has been chosen as the context are manifold: First, all individuals who use emails are very likely to be a victim of email tracking. The reason is that roughly all newsletters (Brunet 2017) and about every fifth conversational email includes a tracking element to track the recipients of the email (Merchant 2017). Second, email tracking can be a major threat to individuals' privacy because their personal information such as whether and if so when an email has been opened, the IP-address, the geolocation of the recipient, the used operating system and other information is retrieved (Bender et al. 2016). This can lead to severe adverse outcomes such as burglars finding out when individuals are not at home and then burgling into their house (Xu et al. 2018). Third, there are clear mechanisms to protect against email tracking. The most effective one is to disable the automatic image download in emails. The reason is that senders of emails include a tracking element into an image of the email. As soon as the image is downloaded, the tracking element is activated, and the sender can gather personal information. Blocking the automatic image download is possible for every individual, independent of the email account or software used (Bender et al. 2016). Hence, in sum, email tracking represents an ideal context for the PMT because both, threat appraisal and coping appraisal, may be triggered.

Therefore, in this study, the PMT was contextualized to the domain of email tracking. It is important to consider that only the constructs related to PMT are contextualized to email. Mindfulness has been adapted to the general privacy domain. Hence, the concepts mindfulness on threat appraisal and mindfulness on coping appraisal are adapted to a general privacy domain. All other constructs, that relate to the PMT, are adapted to the email tracking context as it is recommended by previous research (Boss et al. 2015).

The PMT provides items to measure corresponding constructs (Boss et al. 2015) and so does research on mindfulness (Thatcher et al. 2018). Therefore, to assess the research model, a survey with a questionnaire has been set up which is explained in more detail below.

4.2 SETTING UP A SURVEY

The survey includes a web-based questionnaire which consists of items, based on the PMT and mindfulness. In more particular, items for the PMT have been adapted from previous research and have slightly been adapted to the context of email tracking. Mindfulness also relies on items of previous research (Thatcher et al. 2018), yet, has been adapted to depict mindfulness on threat appraisal and mindfulness on coping appraisal. Items for all constructs were measured on a 7-point Likert scale,

ranging from 1 (strongly disagree) to 7 (strongly agree). The items including the corresponding authors for all constructs are displayed in Table 8. Furthermore, the survey includes age and gender as demographics and control variables. To implement the questionnaire, we used the software Limesurvey, which we hosted on our own server.

When applying the PMT, it is recommended to include a fear appeal in the survey (Boss et al. 2015). Such a fear appeal is a message that is shown to the participants to scare them as well as to show them how they can protect against the threat (Witte 1992).

4.3 INCLUSION OF A FEAR APPEAL

A fear appeal may be included twice into a research study: A high fear appeal and a low fear appeal (Boss et al. 2015). Whereas a low fear appeal only superficially describes the threat and available coping mechanisms, the high fear appeal is more specific and has the aim to more frighten the participants but also to provide more valuable insights into how to protect against the threat (Boss et al. 2015; Milne et al. 2000). In this research study the focus is more in the inclusion of mindfulness and less on how the fear appeal might change the way how individuals respond to certain threats. Hence, in this research study, only a high fear appeal is included.

Since this study is in the context of email tracking, the fear appeal also relates to email tracking. Specifically, we warned participants that email tracking is a major threat to their privacy. We gave details on how and what information can be gathered through email tracking. The potential consequences of such a loss of privacy were exposed. Furthermore, information was provided on how many emails (99 percent of newsletters and roughly every fifth conversational email) include tracking elements. With this, we pointed at that probably every participant has already been tracked via email. Finally, we gave information on how the participants can protect against email tracking. This included detailed manuals for major email providers and email applications. The particular high fear appeal is provided in the appendix.

In the following, information is given on how participants have been gathered to take part in the survey.

4.4 GATHERING PARTICIPANTS

To find participants, we draw on two different sources: First, participants in earlier anonymous scientific surveys had been asked after those earlier studies if they were interested in participating in future surveys and, if so, to provide their email address; Second, we asked participants in an annual survey about working conditions, we conduct together with a project partner, whether they wish to be invited by email to participate in any future studies. The individuals who provided their email addresses via these two channels comprise our participant pool. This is a valid methodology that has also been used in several articles in journals of the basket of eight (anonymous references).

Participants from both channels represent a population that varies in terms of age, gender, profession and education. Since email tracking affects all individuals independent of such demographics, we are better able to depict this population with our sample than if we had used a student sample.

In total, our pool included 1,639 potential survey participants. We cleaned this list by removing invalid and duplicate email addresses, leaving 1,615 email addresses. Every email address was assigned an individualized token to anonymize the responses. We then sent an email to the 1,615 individuals in our survey pool inviting them to take part in our survey. Participation was incentivized by the possibility to win technical products. All in all, 175 participants took part in the survey and were exposed to a high fear appeal. An overview of the demographics is given in Table 4.

Age (M: 45.0 SD: 10.99 years)	<25	3.1	Sex	Female	65.8
	25-34	17.5		Male	34.2
	35-44	24.0			
	45-54	34.8			
	>54	20.6			

Table 4. Demographics of the participants

Based on the answers of the 175 participants, the results could be evaluated.

4.5 EVALUATION OF THE RESULTS

To evaluate the results, a partial least squares structural equation modeling approach (PLS-SEM) has been selected. This approach is suitable for investigating privacy-related concepts where answers might skew the normal distribution (Turel et al. 2011). In addition, PLS-SEM is applicable, when the focus is more on exploratory research rather than on theory testing (Hair et al. 2017). Since the inclusion of mindfulness is more of exploratory nature, PLS-SEM seems to be the correct approach here. As the software, we use SmartPLS, version 3 (Hair et al. 2017).

5 RESULTS

In the following, the results of the research model are presented. To do so, common method bias is first considered and the measurement model afterwards. Then, as both show no signs of a CMB or a distorted measurement model, the structural model is assessed and with this the hypotheses of the research model.

5.1 COMMON METHOD BIAS

By checking on common method bias, we can evaluate to what degree our results are distorted (Schwarz et al. 2017). We used the Harman's Single-Factor Test, which shows that 24.1 percent of variance is explained by one factor, which is below the threshold of 50.0 percent. Furthermore, the unmeasured latent method construct explains a delta of R^2 of 0.002325. As the average R^2 without the CMB is 0.663125, we have a ratio of 1:285 (Chin et al. 2012). These tests therefore show no indication of common method bias in our data (Liang et al. 2007).

5.2 MEASUREMENT MODEL

To operationalize mindfulness, a two-stage approach has been followed (Hair et al. 2017): First, one is supposed to create the second-order construct. Then, the corresponding first-order constructs are created. In this case, it is a reflective-reflective second-order construct. Hence, the second-order construct points to every of the first-order constructs. Items for every first-order construct are assigned. Furthermore, all items of all first-order constructs are also assigned to the second-order construct. Then, the loadings of the first-order constructs are evaluated. Most of them are greater than the recommended value of 0.707 (Hair et al. 2017). Two items were dropped because they were clearly below that value. One item has been kept although the value is 0.689 and with this slightly below the value of 0.707. However, we kept this value out of two reasons: First, the authors who constructed the construct mindfulness kept items that were slightly below the value of 0.707 (Thatcher et al. 2018). Second, one may keep values which are only slightly below 0.707 when such values are highly significant, when they are rather newly developed and when the removal would have a strong effect on the content validity (Hair et al. 2017). Since all of this is the case here, the item has been kept.

Afterwards, the latent variable scores are estimated. After having done so, all first-order constructs as well as all items are removed. Instead, the calculated latent variable scores now serve as indicators of the second-order construct (Hair et al. 2017). In this case, mindfulness is represented by four items

(novelty seeking, engagement, novelty production and flexibility). This procedure has been done twice: Once for mindfulness on threat appraisal and once for mindfulness on coping appraisal.

To then evaluate the measurement model, indicator reliability, construct reliability and discriminant validity need to be accounted for. Also, indicator validity is an important issue. The latter has been established by relying on items that have been previously validated by former research. Indicator reliability is that each indicator should at least explain 50 percent of the variance of the latent variable which means that every indicator should be at least 0.707 and highly significant at $p < 0.001$. This is the case for most items as is depicted in Table 8. One exception is that novelty production as an item of mindfulness on coping appraisal, only has a loading of 0.643. However, this item has been kept because of the same reasons as stated above. Furthermore, the items of novelty production of the first-order construct were all far above 0.707, further indicating that the item may be kept.

Construct reliability is composed of average variance extracted (AVE) and the composite reliability (CR). AVE should be above 0.5 which is the case in this study. Furthermore, CR should be above 0.7 which is also the case (Fornell and Larcker 1981). Both values for all constructs are depicted in Table 5. Discriminant validity, a measure of whether constructs differ from each other, is true if the square root of the AVE is greater than the correlation of the constructs with each other (Fornell and Larcker 1981; Hulland 1999). This is also the case in our study (see Table 5). As all requirements have been fulfilled, we can state that our measurement model is valid.

	Mean	SD	AVE	CR	1	2	3	4	5	6	7	8	9	10	11	12
1 Mindfulness on threat appraisal	4.89	1.43	0.678	0.894	0.824											
2 Mindfulness on coping appraisal	5.05	1.39	0.685	0.895	0.796	0.828										
3 Perceived threat vulnerability	4.87	1.39	0.839	0.940	0.286	0.180	0.916									
4 Perceived threat severity	5.56	1.47	0.777	0.913	0.433	0.514	0.221	0.882								
5 Fear	3.53	1.57	0.797	0.922	0.260	0.203	0.359	0.352	0.893							
6 Maladaptive rewards	2.97	1.52	0.686	0.868	0.056	-0.029	0.307	-0.040	0.244	0.828						
7 Response efficacy	5.09	1.55	0.830	0.936	0.190	0.311	0.079	0.272	0.142	-0.017	0.911					
8 Self-efficacy	4.96	2.02	0.944	0.980	0.238	0.355	0.196	0.340	0.138	0.102	0.279	0.971				
9 Response costs	2.61	1.97	0.868	0.952	0.003	-0.036	0.106	-0.081	0.309	-0.068	-0.159	-0.068	0.932			
10 Protection Motivation	5.11	2.88	0.921	0.972	0.150	0.182	0.122	0.416	0.279	0.299	0.348	0.299	-0.102	0.960		
11 Gender	1.34	0.47	n/a	n/a	-0.086	-0.100	-0.006	-0.009	-0.039	-0.137	-0.065	0.138	0.045	0.149	n/a	
12 Age	44.74	11.17	n/a	n/a	0.087	0.026	-0.007	0.015	-0.019	-0.063	-0.048	-0.063	-0.037	-0.034	-0.089	n/a

Table 5. Mean, SD, AVE, CR, bivariate correlations and square root of AVE (bold)

In the following, the structural model may now be evaluated.

5.3 STRUCTURAL MODEL

The overview in Table 6 shows that the majority of the hypotheses are supported. In more particular, mindfulness on threat appraisal influences threat severity and threat vulnerability, yet, not maladaptive rewards. Mindfulness on coping appraisal influences response efficacy and self-efficacy, yet, not response costs. For the traditional relationships of the PMT, the effect of threat vulnerability and response costs on the intention to protect were rejected. All other hypotheses were supported.

Hypotheses	Supported	Rejected
H1: The higher the mindfulness on threat appraisal, the higher the perceived threat severity.	x	
H2: The higher the mindfulness on threat appraisal, the higher the perceived threat vulnerability.	x	
H3: The higher the mindfulness on threat appraisal, the higher the maladaptive rewards.		x
H4: The higher the mindfulness on coping appraisal, the higher the response efficacy.	x	
H5: The higher the mindfulness on coping appraisal, the higher the self-efficacy.	x	
H6: The higher the mindfulness on coping appraisal, the lower the response costs.		x
H7: The higher the perceived threat severity, the higher the fear.	x	
H8: The higher the perceived threat vulnerability, the higher the fear.	x	
H9: The higher the fear, the higher the intention to protect.	x	
H10: The higher the perceived threat severity, the higher the intention to protect.	x	
H11: The higher the perceived threat vulnerability, the higher the intention to protect.		x
H12: The higher the maladaptive rewards, the lower the intention to protect.	x	
H13: The higher the response efficacy, the higher the intention to protect.	x	
H14: The higher the self-efficacy, the higher the intention to protect.	x	
H15: The higher the response costs, the lower the intention to protect.		x

Table 6. Overview of supported and rejected hypotheses

The R^2 of the intention to protect is 37.9 percent and the R^2 of fear is 20.7 percent. The R^2 of the threat appraisal and coping appraisal concepts differ, depending on if the corresponding mindfulness concept has a significant or an insignificant effect on it. Whereas the R^2 of threat severity ($R^2=18.8$ percent) and threat vulnerability ($R^2=8.2$ percent) is considerable, the R^2 of maladaptive rewards is non-existent ($R^2=0.3$ percent). Similarly, for the concepts of the coping appraisal: The R^2 for response efficacy ($R^2=9.7$ percent) and self-efficacy ($R^2=12.6$ percent) are again considerable, the R^2 for response costs is non-existent ($R^2=0.1$ percent). An overview of the structural model is given in Figure 2.

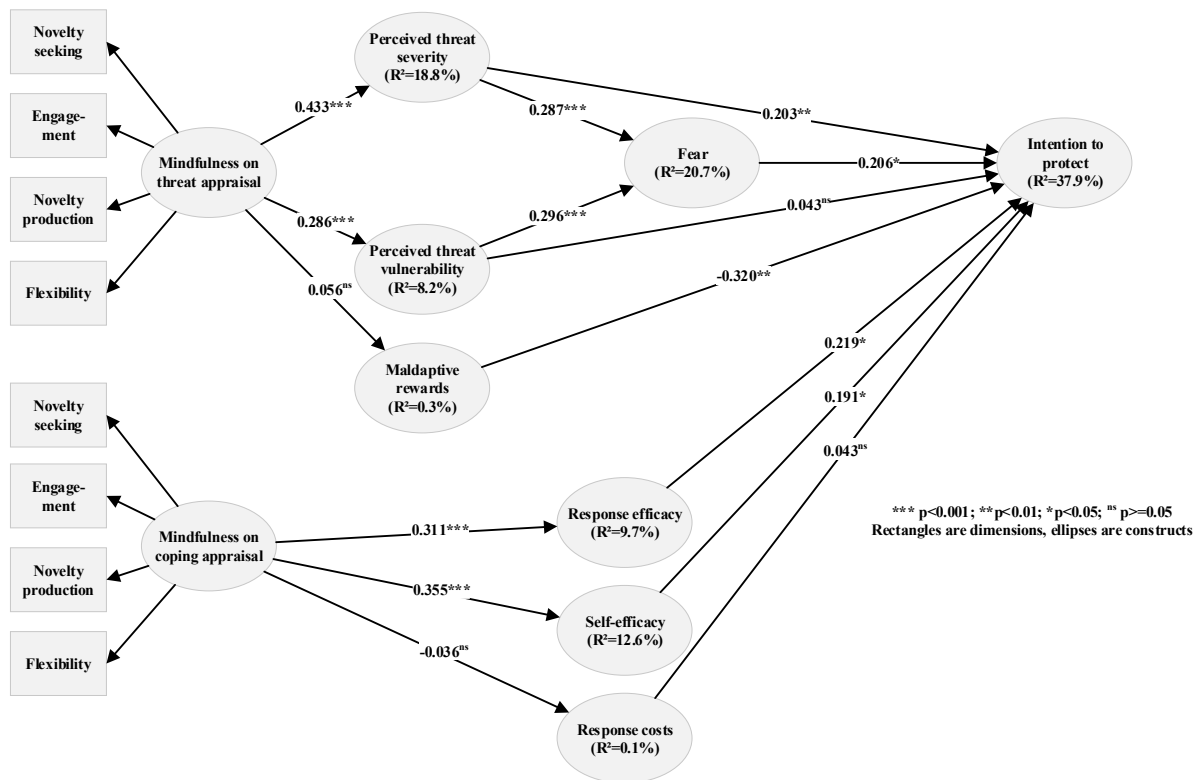


Figure 2. Structural model

These results have contributions for literature and practice which are discussed below.

6 DISCUSSION

In this research study, the aim is to research on the effect of mindfulness on threat appraisal and on coping appraisal. The research question thus is “*What is the influence of mindfulness on an individual’s*

threat appraisal and coping appraisal?” To answer this research question, mindfulness has been split into two different concepts: mindfulness on threat appraisal and mindfulness on coping appraisal. The results then support most of the hypotheses. Hence, the answer to the research question is that mindfulness on threat appraisal indeed increases the appraisal of threats. Furthermore, mindfulness on coping appraisal indeed has a positive effect on how to cope with the threat. The implications of these results for literature and practice are discussed in the following, completed by a discussion of the non-supported hypotheses regarding the effect of both mindfulness concepts.

6.1 IMPLICATIONS FOR LITERATURE AND PRACTICE

Threat appraisal can be explained by mindfulness: Previous research applying the PMT has rather focused on the outcomes of threat appraisal (e.g., Han et al. 2011; Herath and Rao 2009; Johnston et al. 2015; Sonnenschein et al. 2016). Some scholars have also focused on the antecedents (e.g., Mousavizadeh and Kim 2015), however mindfulness in this regard has not been implemented. This research fills this research gap by showing that mindfulness is a concept that increases threat appraisal. With this, one can now partly explain why individuals differently appraise the same threat. Individuals who are more mindful are more likely to perceive the same threat as severe and to be more vulnerable to that threat in comparison to individuals who are less mindful. This means for scholars that if they include a threat appraisal into their research study, they should also account for the level of mindfulness. Especially individuals who are highly mindful on threat appraisal will be more likely to consider a threat to be severe and will be more likely to consider themselves to be vulnerable to that threat. Hence, depending on the aim of the scholars, they should either focus on highly or less mindful individuals or they should at least control for the level of mindfulness.

Coping appraisal can be explained by mindfulness: Similar as for threat appraisal, previous research has rather neglected to focus on antecedents of coping appraisal. This research study fills this gap by introducing mindfulness on coping appraisal as a concept that influences coping appraisal in the domain of privacy. In particular, response efficacy and self-efficacy are increased when the individual is more mindful on coping appraisal. Hence, this research study contributes to the privacy domain by suggesting mindfulness on coping appraisal to be an important concept determining response efficacy and self-efficacy. In case scholars aim to research on one of these two concepts, the results suggest that mindfulness is something they might want to consider. If individuals are highly mindful, then the PMT might be more applicable because then they are more likely to know how to cope with the threat.

Mindfulness supports the function of the fear appeal: The two mentioned contributions also indicate that mindfulness on threat appraisal and mindfulness on coping appraisal support the aim of a fear appeal. The aim of the fear appeal is among others to trigger the threat appraisal and coping appraisal. With this, the entire PMT is then more likely to function in terms of more supported hypotheses, stronger relationships and a better overall model fit (Boss et al. 2015; Rogers and Prentice-Dunn 1997). More mindful individuals are also more likely to have an increased threat appraisal and an increased coping appraisal. This means that in case, scholars want to even more increase threat appraisal and coping appraisal, they should still include a high fear appeal. However, they also might want to focus on highly mindful individuals because they are even more likely to have a high threat appraisal and a high coping appraisal. This supplements previous research on the PMT (Boss et al. 2015), urging scholars to include a high fear appeal into their studies. With this, we suggest that focusing on highly mindful individuals will contribute to the aim of a high fear appeal.

Mindfulness needs to be adapted to the particular domain: In this research study, mindfulness has been conceptualized as mindfulness on threat appraisal and mindfulness on coping appraisal. The reason was that an individual might be highly mindful on privacy threats but less mindful on how to

cope with the threat. The measurement model of this research study supports this notion, showing that both concepts are different from each other. This also goes in line with previous research which urges researchers to not rely on a general concept of mindfulness, yet, rather adapt it to the particular domain of the focal research study (Thatcher et al. 2018). This is also important for scholars who apply other theories than the PMT in the privacy domain should also consider that mindfulness needs to be adapted to the particular domain they are researching on.

Training mindfulness could help in increasing threat appraisal and coping appraisal: This research study also has practical implications. Individuals often consider privacy threats such as email tracking differently. Also, not all individuals have the same capabilities to cope with such privacy threats (Xu et al. 2018). The PMT shows the particular concepts comprising threat appraisal and coping appraisal. However, why individuals differently appraise the threat and why they have different capabilities to cope with the threat has rather been neglected by previous research. This research suggests that mindfulness is one factor determining a higher threat appraisal and a higher coping appraisal. Practitioners who are interested in increasing threat appraisal and coping appraisal thus may focus on the level of mindfulness of individuals. This level of mindfulness can also be trained, e.g. through mindfulness-based interventions (Dane 2011; Kiken et al. 2015). Mindfulness can also be triggered by other concepts such as curiosity (Brewer et al. 2013). Hence, this research shows that there is a way to bring individuals to have a higher appraisal of privacy threats and to also be able to cope with these privacy threats.

6.2 DISCUSSION OF NON-HYPOTHESIZED RESULTS

There is no effect between mindfulness and maladaptive rewards: The results suggest that mindfulness has no effect on maladaptive rewards – neither a positive nor a negative one. This is contrary to the hypothesis in this research study, suggesting a positive effect. One reason could be that only because individuals are highly mindful on the threats of privacy, they do not know more about the benefits when they do not protect against it. In other words, mindfulness on privacy threats has nothing to do with knowledge on maladaptive rewards. Another reason could be that in case the individual is more mindful on privacy threats, the possible maladaptive rewards diminish. In other words, the more privacy threats the individual is considering through her high level of mindfulness, the less likely she will consider possible maladaptive rewards.

Response costs are not determined by mindfulness: Response costs are one important concept of the coping appraisal process. With response costs, individuals consider how high the expenditure of the associated protection behavior is. It was hypothesized that a high level of mindfulness on coping appraisal will decrease the level of response costs. However, the results show a non-significant relationship. One reason could be that individuals already only see low response costs for protecting their privacy, independent of the level of mindfulness. This is supported by the comparatively low mean value of response costs as depicted in Table 5. In case of low response costs, mindfulness might be less likely to even more decrease that already low level. If that explanation is true than that would mean for scholars that mindfulness only helps in case of a certain threshold. For example, if response costs are already low enough, mindfulness on coping appraisal will not further decrease them.

7 LIMITATIONS AND FUTURE RESEARCH

This study has several limitations but also points to possible fruitful avenues for future research. First, we use the items of Thatcher et al. (2018) to measure mindfulness and adapt them to the particular domain. However, also other items of mindfulness exist, which might lead to different results. Furthermore, others also consider mindfulness to be a state rather than a trait (Kiken et al. 2015). In such a case, again other measurements are considered which might alter the results stated here. Second, this

research only includes a high fear appeal. Another possibility would have been to also include a low fear appeal to evaluate in how far the results then still apply. Since this study focused on mindfulness, it does not limit the results of this study. However, including a low fear appeal would shift the focus to the comparison between a high fear appeal and a low fear appeal. Third, this study has been conducted in the privacy domain and in the context of email tracking in particular. Therefore, the results can only speak for this context. However, we do not see any reason why the results should not also be similar in other contexts. The reason is that on the one hand, we have focused on general levels of mindfulness on privacy threats and how to cope with privacy threats and not on mindfulness in the email tracking context. On the other hand, the general relationships of the PMT have already been supported in other contexts such that also in other contexts, threat appraisal and coping appraisal play important roles (Boss et al. 2015).

Possibilities for future research include the following suggestions: First, based on the aforementioned limitation, scholars might want to include a low fear appeal. One suggestion here could especially be to find out, in how far a fear appeal is even still necessary when individuals are highly mindful (Posey et al. 2015). Second, this research has particularly focused on the antecedents of threat appraisal and coping appraisal. One other research possibility could be to focus on the effect of mindfulness on the actual behavior of protecting against a threat. This might be through a mediating effect or also through a direct effect. Third, the results support the hypotheses, indicating that mindfulness is an important concept when applying the PMT. Scholars could also adapt other theories of the privacy domain, e.g. the privacy calculus (Dinev and Hart 2006), researching on in how far mindfulness has an effect on concepts of such theories. Fourth, the results support the notion that mindfulness on threat appraisal and mindfulness on coping appraisal are different, yet, strongly related with each other. Future research might want to focus on in how far there is one concept of mindfulness that captures both, mindfulness on threat appraisal and mindfulness on coping appraisal.

8 CONCLUSION

The aim of this research study was to find out, why individuals have different levels of threat appraisal and coping appraisal. Previous research has indicated that mindfulness has an effect on threat appraisal and coping appraisal. This led to the inclusion of mindfulness into the PMT to research on its effects. In particular, mindfulness has been split into two concepts: mindfulness on threat appraisal and mindfulness on coping appraisal. The results support that both concepts respectively affect threat appraisal and coping appraisal of the PMT. The contributions for literature are among others that scholars, who apply the PMT, might want to focus on the level of mindfulness of their participants to explain different levels of threat appraisal and coping appraisal.

9 APPENDIX

9.1 LITERATURE REVIEW ON MINDFULNESS AND THE PROTECTION MOTIVATION THEORY

Antecedents of appraisals	Outcomes of appraisals	PMT	Mindfulness	Context	Reference
-	-	-	x	Reliability of IS	Butler and Gray 2006
-	-	-	x	Agile development	Cram and Newell 2016
-	-	-	x	Adoption of RFID	Goswami et al. 2008
-	-	-	x	Organizational IS adoption	Goswami et al. 2009
-	-	-	x	Technostress	Maier et al. 2019
-	-	-	x	Individual IS adoption	Sun 2011
-	-	-	x	Individual IS adoption	Sun and Fang 2010
-	-	-	x	Individual IS adoption	Sun et al. 2016

-	-	-	x	Individual IS usage	Thatcher et al. 2018
-	-	-	x	Individual IS adoption	Zou et al. 2015
-	x	x	-	Security	Han et al. 2011
-	x	x	-	Security	Herath and Rao 2009
x	x	x	-	Security	Herath et al. 2014
-	x	x	-	Security	Johnston and Warkentin 2010
-	x	x	-	Security	Johnston et al. 2015
-	-	-	-	Privacy	Junglas et al. 2008
-	x	x	-	IT avoidance	Liang and Xue 2009
x	x	x	-	Privacy	Mousavizadeh and Kim 2015
x	x	x	-	Security	Posey et al. 2015
-	x	x	-	Security	Sonnenschein et al. 2016
-	x	x	-	Security	Woon et al. 2005
-	x	x	-	Security	Wynn et al. 2013
x	x	x	-	Fake-Websites	Zahedi et al. 2015
x	x		x	Privacy	This research

Literature review in the AIS basket of eight including ICIS; Search was done in title/abstract/keywords using protection motivation theory OR mindfulness

Table 7. Literature review on mindfulness and the protection motivation theory

9.2 MEASUREMENT ITEMS

Construct	Items	Loadings	Dimension and loading (if applicable)	Author(s)
Mindfulness on threat appraisal	I like to investigate possible privacy threats.	0.917	Novelty seeking (0.854)	Thatcher et al. (2018)
	I am very curious possible privacy threats.	0.955		
	I like to figure out possible privacy threats.	0.917		
	I often notice how other people handle privacy threats.	0.689	Engagement (0.828)	
	I attend to the 'big picture' of privacy threats.	0.793		
	I 'get involved' when evaluating privacy threats.	0.852		
	I find it easy to create new information about privacy threats.	0.829	Novelty production (0.774)	
	I am very creative when it comes to privacy threats.	0.882		
	I make many novel contributions to myself when assessing privacy threats.	0.836		
	I am often open to learning new issues about privacy threats.	0.945	Flexibility (0.836)	
	I have an open mind about privacy threats.	0.483 (dropped)		
Mindfulness on coping appraisal	I like to investigate how to protect my privacy.	0.916	Novelty seeking (0.844)	Thatcher et al. (2018)
	I am very curious about how to protect my privacy.	0.945		
	I like to figure out to protect my privacy.	0.934		
	I often notice how other people are protecting their privacy.	0.537 (dropped)	Engagement (0.890)	
	I attend to the 'big picture' of privacy when evaluating how to protect my privacy.	0.823		
	I 'get involved' when thinking about how to protect my privacy.	0.849		
	I find it easy to create new and effective ways of protecting my privacy.	0.892	Novelty production (0.644)	
	I am very creative when it comes to protecting my privacy.	0.915		
	I make many novel contributions to myself when protecting my privacy.	0.900		
	I am often open to learning new ways of protecting my privacy.	0.913	Flexibility (0.906)	
	I have an open mind about new ways of protecting my privacy.	0.845		
Perceived threat severity	If emails I receive were tracked, it would be severe.	0.923	n/a	Johnston and Warkentin 2010
	If emails I receive were tracked, it would be serious.	0.846		
	If emails I receive were tracked, it would be a real problem for me.	0.875		
Perceived threat vulnerability	E-mails I receive are at risk to be tracked.	0.889	n/a	Johnston and Warkentin 2010
	It is likely that emails I receive are tracked.	0.941		
	It is possible that emails I receive are tracked.	0.917		
Fear	My email account has a serious email tracking problem.	0.875	n/a	Osman et al. 1994
	My emails might be seriously getting tracked.	0.908		
	The amount of my emails getting tracked is terrifying.	0.896		
Maladaptive rewards	Not disabling the automatic image download on my email account saves me time.	0.847	n/a	Boss et al. 2015; Myyry et al. 2017
	Not disabling the automatic image download on my email account saves me money.	0.800		
	Not disabling the automatic image download on my email account keeps me from being confused.	0.837		

Response efficacy	Disabling image download on my email account is effective to protect against email tracking.	0.891	n/a	Johnston and Warkentin 2010
	When disabling image download on my email account, my emails are more likely to be protected against email tracking.	0.925		
	Disabling image download on my email account is sensible to protect against email tracking.	0.916		
Self-efficacy	I was able to disable automatic image download on my email account, ...		n/a	Compeau and Higgins 1995
	... if I could call someone for help if I got stuck.	0.959		
	... if someone else helped me get started.	0.977		
	... if someone showed me how to do it first.	0.987		
Response costs	I would be discouraged from disabling automatic image download because it would take too much time.	0.930	n/a	Milne et al. 2002
	Taking the time to disable automatic image download would cause me too many problems.	0.916		
	I would be discouraged from disabling automatic image download because I would feel silly to do so.	0.948		
Intention to protect	My intentions to disable automatic image download on my email account are high.	0.942	n/a	Johnston and Warkentin 2010; Posey et al. 2015
	It is likely that I will disable automatic image download on my email account.	0.977		
	I intend to expend effort to disable automatic image download on my email account.	0.960		

Table 8 Measurement items

9.3 HIGH FEAR APPEAL

The following text was given all participants of the study as a high fear appeal:

Please read the following information carefully. The subsequent statements to be evaluated also refer to this text. Thank you very much.

Through e-mail tracking you pay more when shopping online!

Email tracking is a relatively unknown, but no less dangerous way to undermine the privacy of users. 99 percent of all sent newsletters and even almost 20 percent of all "normal" e-mails are tracked. Tracking means that the sender of an e-mail can find out a lot of data about the recipient of an e-mail. For example, whether and when he opened the e-mail, whether he forwarded the e-mail, where he was at the time the e-mail was opened, and much more. The recipient is not aware of this and does not have to give any consent at all. The tracking therefore runs unnoticed. Such tracking undermines the privacy of the recipient. As shown in the headline, merchants, for example, use e-mail tracking to categorize their customers and thus offer different prices for their products. Employers can use email tracking to monitor their employees at home. Burglars can use email tracking to check if someone is at home and better plan their break-in.

Technically, the sender of the e-mail inserts a tracking element - usually in the form of an invisible image. As soon as the recipient opens the e-mail and downloads the image, he transmits further information to the sender, who can evaluate it. At the moment, there is only one really effective protective measure: deactivate the automatic download of images in e-mails. This ensures that no more images are downloaded in emails and that all tracking elements are blocked.

Often the automatic download of images is already activated. However, users can disable this in the settings of their e-mail account or e-mail program. Instructions for the most common programs and e-mail accounts are linked here.

Browser-Access:

GoogleMail (Google states that they limit the tracking of e-mail. However, it is only fully restricted when downloading of images is deactivated).

GMX

web.de

Access via Smartphone:

Android / Gmail

iOs (Apple iPhone or iPad)

MacOS (Mountain Lion)

Access via software on a computer:

Outlook 2016/2013/2010/2007

Thunderbird

10 REFERENCES

- Abbott, C. 2017. *Cyber-Attacks: A Problem In 2016, Still A Problem in 2017*.
<http://www.natlawreview.com/article/cyber-attacks-problem-2016-still-problem-2017>. Accessed 24 January 2017.
- Acquisti, A., and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security & Privacy* (3:1), pp. 26–33.
- Allport, G. W. 1961. *Pattern and growth in personality*, Oxford, England: Holt, Reinhart & Winston.
- Anderson, C. L., and Agarwal, R. 2010. "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Quarterly* (34:3), 613–A15.
- Baer, R. A., Smith, G. T., Hopkins, J., Krietemeyer, J., and Toney, L. 2006. "Using self-report assessment methods to explore facets of mindfulness," *Assessment* (13:1), pp. 27–45.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.
- Bender, B., Fabian, B., Lessman, S., and Haupt, J. 2016. "E-Mail Tracking: Status Quo and Novel Countermeasures," in *Proceedings of the 37th International Conference on Information Systems*, B. Fitzgerald and J. Mooney (eds.), Dublin, Ireland.
- Bodner, T. E., and Langer, E. J. 2001. "Individual differences in mindfulness: the mindfulness/mindlessness scale," in *Proceedings of the 13th annual American Psychology Society Convention*, n/a (ed.), Toronto, Ontario, Canada.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864.
- Brewer, J. A., Davis, J. H., and Goldstein, J. 2013. "Why is it so hard to pay attention, or is it? Mindfulness, the factors of awakening and reward-based learning," *Mindfulness* (4:1).
- Brown, K. W., and Ryan, R. M. 2003. "The benefits of being present: Mindfulness and its role in psychological well-being," *Journal of Personality and Social Psychology* (84:4), pp. 822–848.
- Brunet, N. 2017. *OMC Releases State of Email Tracking Report*.
<http://www.prweb.com/releases/2017/06/prweb14427071.htm>. Accessed 6 September 2017.
- Butler, B. S., and Gray, P. H. 2006. "Reliability, mindfulness, and information systems," *MIS Quarterly* (30:2), pp. 211–224.
- Carlo, J. L., Lyytinen, K., and Boland, J. R. J. 2012. "DIALECTICS OF COLLECTIVE MINDING: CONTRADICTIONARY APPROPRIATIONS OF INFORMATION TECHNOLOGY IN A HIGH-RISK PROJECT," *MIS Quarterly* (36:4), 1081–A3.
- Chen, Y., and Zahedi, F. M. 2016. "Individuals internet security perceptions and behaviors: Polycontextual contrasts between the united states and china," *MIS Quarterly* (40:1), 205–A12.
- Chin, W. W., Thatcher, J. B., and Wright, R. T. 2012. "Assessing common method bias: Problems

- with the ULMC technique,” *MIS Quarterly* (36:3), pp. 1003–1019.
- Compeau, D. R., and Higgins, C. A. 1995. “Computer self-efficacy: Development of a measure and initial test,” *MIS Quarterly* (19:2), pp. 189–211.
- Cram, W. A., and Newell, S. 2016. “Mindful revolution or mindless trend? Examining agile development as a management fashion,” *European Journal of Information Systems* (25:2), pp. 154–169.
- Dane, E. 2011. “Paying Attention to Mindfulness and Its Effects on Task Performance in the Workplace,” *Journal of Management* (37:4), pp. 997–1018.
- Davis, J. M., and Yi, M. Y. 2012. “User disposition and extent of Web utilization: A trait hierarchy approach,” *HCI research in privacy and security* (70:5), pp. 346–363.
- Dernbecher, S., and Beck, R. 2017. “The concept of mindfulness in information systems research: A multi-dimensional analysis,” *European Journal of Information Systems*, pp. 1–22.
- Dinev, T., and Hart, P. 2006. “An extended privacy calculus model for e-commerce transactions,” *Information Systems Research* (17:1), pp. 61–80.
- Epel, E., Daubenmier, J., Moskowitz, J. T., Folkman, S., and Blackburn, E. 2009. “Can meditation slow rate of cellular aging? Cognitive stress, mindfulness, and telomeres,” *Annals of the New York Academy of Sciences* (1172:1), pp. 34–53.
- Fabian, B., Bender, B., and Weimann, L. 2015. “E-Mail Tracking in Online Marketing - Methods, Detection, and Usage,” in *Proceedings of the 12th International Conference on Wirtschaftsinformatik*, O. Thomas and F. Teuteberg (eds.), Osnabrück, Germany, pp. 1100–1114.
- Fiol, C. M., Pratt, M. G., and O'Connor, E. J. 2009. “Managing Intractable Identity Conflicts,” *Academy of Management Review* (34:1), pp. 32–55.
- Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. “A meta-analysis of research on protection motivation theory,” *Journal of applied social psychology* (30:2), pp. 407–429.
- Fornell, C., and Larcker, D. F. 1981. “Evaluating structural equation models with unobservable variables and measurement error,” *Journal of Marketing Research* (18:1), pp. 39–50.
- Garland, E. L., Gaylord, S. A., and Fredrickson, B. L. 2011. “Positive Reappraisal Mediates the Stress-Reductive Effects of Mindfulness: An Upward Spiral Process,” *Mindfulness* (2:1), pp. 59–67.
- Gidda, M. 2013. *Edward Snowden and the NSA files – timeline*.
<http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline>. Accessed 9 February 2016.
- Goel, V., and Perlroth, N. 2016. *Yahoo Says 1 Billion User Accounts Were Hacked*.
<http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html>. Accessed 15 December 2016.
- Goswami, S., Teo, H., and Chan, H. 2008. “Real Options from RFID Adoption: The Role of Institutions and Managerial Mindfulness,” in *Proceedings of the Twenty Ninth International Conference on Information Systems*, D. Te'eni and F. Rowe (eds.), Paris, France.
- Goswami, S., Teo, H., and Chan, H. 2009. “Decision-Maker Mindfulness in IT Adoption: The Role of Informed Culture and Individual Personality,” in *Proceedings of the 30th International Conference on Information Systems*, H. Chen and S. Slaughter (eds.), Phoenix, USA.
- Haigh, E. A. P., Moore, M. T., Kashdan, T. B., and Fresco, D. M. 2011. “Examination of the factor structure and concurrent validity of the Langer Mindfulness/Mindlessness Scale,” *Assessment* (18:1), pp. 11–26.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne: Sage.
- Han, W., ada, S., Sharman, R., Brennan, J., and Rao, H. R. 2011. “Critical Factors Affecting Compliance to Campus Alerts,” *ICIS 2011 Proceedings*.
- Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. 2014. “Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service,” *Information Systems Journal* (24:1), pp. 61–84.
- Herath, T., and Rao, H. R. 2009. “Protection motivation and deterrence: a framework for security policy compliance in organisations,” *European Journal of Information Systems* (18:2), pp. 106–125.
- Hulland, J. 1999. “Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies,” *Strategic Management Journal* (20:2), pp. 195–204.

- Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* (34:3), 549-A4.
- Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric," *MIS Quarterly* (39:1), 113-A7.
- Junglas, I. A., Johnson, N. A., and Spitzmüller, C. 2008. "An empirical study in the context of location-based services," *European Journal of Information Systems* (17:4), pp. 387–402.
- Karwatzki, S., Trenz, M., Tuunainen, V. K., and Veit, D. 2017. "Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence," *European Journal of Information Systems* (26:6), pp. 688–715.
- Kellogg, R. T. 1987. "Effects of topic knowledge on the allocation of processing time and cognitive effort to writing processes," *Memory & Cognition* (15:3), pp. 256–266.
- Kiken, L. G., Garland, E. L., Bluth, K., Palsson, O. S., and Gaylord, S. A. 2015. "From a state to a trait: Trajectories of state mindfulness in meditation during intervention predict changes in trait mindfulness," *Personality and Individual Differences* (81), pp. 41–46.
- Langer, E. 2004. *Langer Mindfulness Scale User Guide and Technical Manual*, Worthington, OH: IDS Publishing Corporation.
- Langer, E. J. 1989a. *Mindfulness*, Cambridge, MA, USA: Perseus Books.
- Langer, E. J. 1989b. "Minding Matters: The Consequences of Mindlessness–Mindfulness," in *Advances in experimental social psychology*, L. Berkowitz (ed.), San Diego: Academic Press, pp. 137–173.
- Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS Quarterly* (31:1), pp. 59–87.
- Liang, H., and Xue, Y. 2009. "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly* (33:1), pp. 71–90.
- Maddux, J. E., and Rogers, R. W. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology* (19:5), pp. 469–479.
- Maier, C., Laumer, S., Wirth, J., and Weitzel, T. 2019. "Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples," *European Journal of Information Systems* (28:5), pp. 496–522.
- McCrae, R. R., and Costa, P. T. 2006. *Personality in adulthood: A five-factor theory perspective*, New York, NY: Guilford Press.
- Merchant, B. 2017. *How email open tracking quietly took over the web*. <https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/>. Accessed 22 January 2018.
- Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions," *British Journal of Health Psychology* (7:2), pp. 163–184.
- Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of applied social psychology* (30:1), pp. 106–143.
- Mousavizadeh, M., and Kim, D. J. 2015. "A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- Myry, L., Siponen, M., Pahnla, S., Vartiainen, T., and Vance, A. 2017. "What levels of moral reasoning and values explain adherence to information security rules?: An empirical study," *European Journal of Information Systems* (18:2), pp. 126–139.
- Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric properties in a community sample," *Journal of Behavioral Medicine* (17:5), pp. 511–522.
- Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179–214.
- Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The*

- Journal of psychology* (91:1), pp. 93–114.
- Rogers, R. W. 1983. “Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation,” in *Social psychophysiology: A sourcebook*, J. T. Cacioppo (ed.), New York, N.Y.: Guilford, pp. 153–177.
- Rogers, R. W., and Prentice-Dunn, S. 1997. “Protection motivation theory,” in *Handbook of health behavior research 1: Personal and social determinants*, New York, NY, US: Plenum Press, pp. 113–132.
- Schwarz, A., Rizzuto, T., Carraher-Wolverton, C., Roldan, J. L., and Barrera-Barrera, R. 2017. “Examining the Impact and Detection of the “Urban Legend” of Common Method Bias,” *ACM Sigmis Database* (48:1), pp. 93–119.
- Sonnenschein, R., Loske, A., and Peter Buxmann 2016. “Gender Differences in Mobile Users’ IT Security Appraisals and Protective Actions: Findings from a Mixed-Method Study,” in *Proceedings of the 37th International Conference on Information Systems*, B. Fitzgerald and J. Mooney (eds.), Dublin, Ireland.
- Sun, H. 2011. “Making Sound Adoption Decisions: A Longitudinal Study of Mindfulness in Technology Adoption and Continued Use,” *ICIS 2011 Proceedings* .
- Sun, H., and Fang, Y. 2010. “Toward a Model of Mindfulness in Technology Acceptance,” in *Proceedings of the 31st International Conference on Information Systems*, M. Lacity, S. March and F. Niederman (eds.), St. Louis, USA.
- Sun, H., Fang, Y., and Zou, H. 2016. “Choosing a Fit Technology: Understanding Mindfulness in Technology Adoption and Continuance,” *Journal of the Association for Information Systems* (17:6), pp. 377–412.
- Thatcher, J., Wright, R., Sun, H., Zagenczyk, T., and Klein, R. 2018. “Mindfulness in Information Technology Use: Conceptual and Operational Definitions,” *MIS Quarterly* (42:3).
- Thatcher, J. B., and Perrewé, P. L. 2002. “An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy,” *MIS Quarterly* (26:4), pp. 381–396.
- Turel, O., Serenko, A., and Giles, P. 2011. “Integrating technology addiction and use: An empirical investigation of online auction users,” *MIS Quarterly* (35:4), pp. 1043–1062.
- van Eerde, W., and Thierry, H. 1996. “Vroom's expectancy models and work-related criteria: A meta-analysis,” *Journal of Applied Psychology* (81:5), pp. 575–586.
- Weinstein, N., Brown, K. W., and Ryan, R. M. 2009. “A multi-method examination of the effects of mindfulness on stress attribution, coping, and emotional well-being,” *Journal of research in personality* (43:3), pp. 374–385.
- Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2017. “Understanding Privacy Threat Appraisal and Coping Appraisal through Mindfulness,” in *Thirty Eighth International Conference on Information Systems*, Y. J. Kim, R. Agarwal and J. K. Lee (eds.), South Korea, pp. 1–11.
- Witte, K. 1992. “Putting the fear back into fear appeals: The extended parallel process model,” *Communication Monographs* (59:4), pp. 329–349.
- Wolf, M., Beck, R., and Pahlke, I. 2012. “Mindfully resisting the bandwagon: reconceptualising IT innovation assimilation in highly turbulent environments,” *Journal of Information Technology* (27:3), pp. 213–235.
- Woon, I., Tan, G.-W., and Low, R. 2005. “A Protection Motivation Theory Approach to Home Wireless Security,” *ICIS 2005 Proceedings* .
- Wynn, D., Williams, C., Karahanna, E., and Madupalli, R. 2013. “Preventive Adoption of Information Security Behaviors,” *ICIS 2013 Proceedings* .
- Xu, H., Hao, S., Sari, A., and Wang, H. 2018. “Privacy Risk Assessment on Email Tracking,” in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Honolulu, HI,
- Zahedi, F. M., Abbasi, A., and Chen, Y. 2015. “Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance,” *Journal of the Association for Information Systems* (16:6), pp. 448–484.
- Zou, H., Sun, H., and Fang, Y. 2015. “Understanding Post-Adoption Regret from the Perspectives of Herding and Mindfulness,” *ICIS 2015 Proceedings* .

Paper VIII

**ANCHORING INFLUENCES
ACTUAL DISCLOSURE**

**FOUR STUDIES ON THE AMOUNT AND ACCURACY OF
INFORMATION DISCLOSURE**

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Tim Weitzel

University of Bamberg

ANCHORING INFLUENCES ACTUAL DISCLOSURE

FOUR STUDIES ON THE AMOUNT AND ACCURACY OF INFORMATION DISCLOSURE

Abstract

Through the anchoring-effect, which is a cognitive bias, individuals are unable to dismiss often irrelevant information when coming to a decision. In this study, we include the anchoring-effect to find out in how far it influences the amount (i.e. the quantity) and the accuracy (i.e. the correctness) of disclosure of information. Based on four studies with 528 participants, we conclude that the anchoring-effect influences both. These results indicate that the anchoring-effect leads to a behavior which cannot be explained when considering the individual to be fully rational. With this, we contribute to the recent research stream on cognitive biases in the privacy domain. We particularly provide evidence that the anchoring-effect helps in explaining the amount and the accuracy of disclosure. Furthermore, we provide guidance that scholars should generally consider cognitive biases in their studies. We also discuss future research possibilities, e.g. the influence of the anchoring-effect on the privacy calculus.

Keywords: Privacy, Amazon Mechanical Turk, Actual disclosure behavior, Heuristics

1 INTRODUCTION

Individuals can disclose information to gain certain benefits (Dinev and Hart 2006). At the same time, when disclosing information, individuals put themselves at risk of diminished privacy. This can then lead to further negative consequences (Karwatzki et al. 2017). To avoid these, individuals can alter their level of disclosure. In particular, individuals can manage their level of disclosure and thus can manage their privacy by disclosing less information or by disclosing incorrect information. In other words, individuals can alter the *amount* and the *accuracy* of their information they aim to disclose (Posey et al. 2010; Son and Kim 2008).

To find out, what determines individuals' management of their privacy, much research has been conducted in that field (Smith et al. 2011). Thereby, with a few exceptions, the clear majority of this research assumes that the individual is conducting a deliberate and thoughtful thinking process, coming to a rational decision to disclose more or less information that is correct or incorrect (Dinev et al. 2015). However, this leaves out the fact that individuals, who undertake decisions, are also influenced by cognitive biases. These cognitive biases can lead to distorted decisions because they are not fully based on logic and rationality (Ariely 2010; Bodenhausen et al. 2001; Cialdini 2010; Kahneman et al. 1982; Tversky and Kahneman 1974).

Thereby, based on previous research, it is possible that the *amount* of information (Acquisti et al. 2017; Mussweiler and Strack 1999) as well as the *accuracy* of information (Tversky and Kahneman 1974) is influenced by cognitive biases. One such cognitive bias is the anchoring-effect that potentially influences all decisions (Furnham and Boo 2011; Kahneman et al. 1982). It states that individuals are unable to dismiss some type of information when making decisions. This information that cannot be dismissed then biases their actual decision (Tversky and Kahneman 1974). For example, in one study, individuals should spin a wheel of fortune which showed a number between 0 and 100. Afterwards, they should guess the actual percentage of African countries in the United Nations. It was shown that the

higher the number on the wheel of fortune the higher the guessed number. The individuals used the number on the wheel of fortune as an anchor which biased their final guess (Tversky and Kahneman 1974).

More recent research in the privacy-domain has already focused on several cognitive biases, including stereotypical thinking (Gerlach et al. 2019) or loss aversion (Choi et al. 2018), yet, leaving out the anchoring-effect. There is consequently a call for researching on the influence of the anchoring-effect on disclosure of information (Dinev et al. 2015) and also indications that the anchoring-effect might influence disclosure (Acquisti et al. 2017). The call is justified because from a theoretical perspective, we do know that generally individuals are influenced by cognitive biases, yet, do not know, how the anchoring-effect as a predominant cognitive bias influences the amount and accuracy of disclosure.

Therefore, in this research study, we focus on the anchoring-effect and in how far it influences the amount and accuracy of disclosure. With this, we aim to research on in how far individuals are influenced by such a cognitive bias when thinking about the amount and accuracy of the information to be disclosed. As the anchoring-effect possibly influences both, the amount as well as the accuracy of disclosure (Acquisti et al. 2017; Mussweiler and Strack 1999; Tversky and Kahneman 1974), we pose the research question:

What is the influence of the anchoring-effect on the amount and the accuracy of disclosure of personal information?

To answer the research question, we structure the manuscript as follows:

Related Work: In this section, we provide information on disclosure of personal information by explaining in detail the amount and accuracy of disclosure. We then proceed with an overview of already researched cognitive biases in the privacy domain. We thereby explain that these cognitive biases have furthered our understanding of several concepts, yet, none of them have been used to better explain the amount and accuracy of disclosure. We then explain the anchoring-effect and provide reasons why we have chosen that cognitive bias to better explain the amount and accuracy of disclosure. Afterwards, we provide deeper information on the anchoring-effect.

The Anchoring-Effect on Actual Disclosure in the Privacy-Related Domain: Disclosure of information as well as the anchoring-effect can come in different forms. We have therefore conducted four studies to cover different forms of both concepts. In this section, we present the hypotheses, methodologies and results of all four studies. Thereby, we have conducted two studies on the amount of disclosure and two studies on the accuracy of disclosure.

Overall Discussion: Afterwards, we discuss the results of all four studies. This will be done, by providing implications for theory in the privacy-related area as well as by providing implications for practice. We then also give guidance for future research and insights into the limitations of our study.

2 RELATED WORK

In the following, we focus on actual disclosure and cognitive biases in the privacy domain. Afterwards, we continue with research on the anchoring-effect.

2.1 DISCLOSURE OF PERSONAL INFORMATION

Disclosure describes the revelation of personal information to another party (Wakefield 2013). In privacy research, disclosure is one of the main studied outcome variables (Smith et al. 2011). This is

because disclosure is necessary to threat individuals' privacy. Thereby, privacy is defined as the control individuals have over their personal information (Bélanger and Crossler 2011).

To measure disclosure, privacy research can rely on different conceptualizations. The most used one is the intention to disclose (Smith et al. 2011). The intention to disclose is defined as the extent to which an individual is willing to reveal personal information to another party (Gerlach et al. 2015). Although it has been used in many studies, it has also been criticized. This is because the intention often does not result in actual behavior (Norberg et al. 2007). Therefore, there is a call for more nuanced research on actual disclosure. With the exception of a few studies (e.g., Cavusoglu et al. 2016; Hui et al. 2007; Jensen et al. 2005) most studies did not focus on actual disclosure and stop with intention. Actual disclosure refers to the effective revelation of personal information by the individual, usually in the study itself (Alashoor et al. 2016). This conceptualization is the preferred one in privacy research since other measurements are often inadequate and often do not reflect the actual behavior of individuals (Smith et al. 2011). Actual disclosure thereby can be considered from multiple perspectives: two, that are relevant in this context refer to the *amount* and the *accuracy* of disclosure (Posey et al. 2010). Both refer to actual disclosure and both are important to protect one's own privacy (Son and Kim 2008):

Amount of disclosure refers to the duration and frequency of disclosure, i.e. how much an individual is about to disclose. The more an individual is about to disclose, the higher the amount of disclosure. To protect their privacy, individuals can limit the amount of disclosure (Son and Kim 2008).

Accuracy of disclosure: Accuracy is defined by the correctness of the personal information that the individual is disclosing. Often, this concept is also called honesty of disclosure (Wheless 1976). Individuals can also disclose inaccurate information. That means that they do not disclose their real, true information but rather disclose information that is fake. Thereby, the information might be incorrect due to two reasons: Either because the individual is *uncertain* about the correct personal information (Wheless 1976), e.g. when a request for personal information is made, the individual is unsure about. Or because the individual wants to protect her privacy and discloses inaccurate information, although she is *certain* about the correctness of the information. In other words, the individual might be uncertain about the information and then provides inaccurate information or she is certain about the information and still provides inaccurate information. In both cases, the individual can protect her privacy (Son and Kim 2008).

When considering previous research, only a couple of research articles have explicitly focused on the amount and / or accuracy of disclosure. None of them has researched on actual behavior (see Table 1). Hence, there is a research gap on actual behavior, when considering the amount and accuracy of disclosure.

Amount of disclosure	Accuracy of disclosure	Actual behavior	Author(s)
x	x	-	Posey et al. (2010)
x	x	-	Hollenbaugh and Ferris (2015)
x	-	-	Tang and Wang (2012)
x	-	-	Sundar et al. (2013)

Table 1. Previous research on amount of disclosure and accuracy of disclosure in the privacy domain¹⁸

Independent of the conceptualization of disclosure, previous research has already emphasized that disclosure in general might be influenced by cognitive biases (Bazerman and Moore 2013; Dinev et al. 2015; Ployhart and Vandenberg 2010). Also, previous privacy-related research has already included

¹⁸ Literature review was conducted in the electronic AIS library as well as the entire EBSCO host, using a full-text search with the keywords "privacy" AND "accuracy" AND "honesty" AND "disclosure". Conferences, except ICIS and CHI, were excluded.

such cognitive biases into their studies.

2.2 COGNITIVE BIASES

Cognitive biases have been part of many research articles. In this section, we focus on cognitive biases in general and continue with an overview of used cognitive biases in the privacy domain. Afterwards, in the subsequent section, we focus on the anchoring-effect in general as one cognitive bias.

2.2.1 Cognitive biases in general

Cognitive biases result from heuristics. A cognitive bias is a deviation from logic and rationality (Ariely 2010; Bodenhausen et al. 2001; Cialdini 2010; Kahneman et al. 1982; Tversky and Kahneman 1974). Individuals, who rely on a cognitive bias will make decisions that are systematically distorted from rationality (Haselton et al. 2015). A heuristic as the reason for a cognitive bias “*reduce[s] the complex tasks of assessing probabilities and predicting values to simpler judgmental operations*” (Tversky and Kahneman 1974, p. 1124). Often such heuristics are rather useful. However, in certain situations, they can also lead to severe and systematic errors. In privacy research, several cognitive biases have been part of research studies.

2.2.2 Cognitive biases in privacy research

Although the majority of studies is more using a perspective of a fully rational and logical-thinking individual (Dinev et al. 2015) there are some studies that have relied on different cognitive biases. In Table 2, we provide an overview of used cognitive biases in privacy research. These research studies have been conducted in a variety of settings, including several cognitive biases, researching on several affected variables.

Cognitive bias	Affected variables	Setting	Author(s)
Affect: Initial emotion formed by an overall impression.	Privacy protection belief and privacy risk belief	e-commerce	Li et al. (2011)
	Website trust, privacy beliefs and intention to disclose	e-commerce	Wakefield (2013)
Benefit heuristic: Positive privacy-related heuristics.	Amount of disclosure	Websites	Sundar et al. (2013)
Fuzzy boundary heuristic: Negative privacy-related heuristics.	Amount of disclosure	Websites	Sundar et al. (2013)
Loss aversion: Preference of individuals to avoid losses than for acquiring gains.	Privacy risks and benefits	Social networking sites	Choi et al. (2018)
Optimistic bias: Individuals think they are much less vulnerable than others.	Privacy-protective behaviors, i.e. erasing cookies, using anti-spyware programs and avoiding suspicious websites.	Online privacy	Baek et al. (2014)
	Privacy risks	Online privacy	Cho et al. (2010)
Stereotypical Thinking: Individuals' human tendency to have particular characteristics in an overgeneralized manner that come readily to mind when thinking about particular entities of a group	Misjudgment of a provider's user-information-handling activities and privacy risks perceptions	Mobile apps	Gerlach et al. (2019)
Anchoring effect: Unable to dismiss pieces of information.	Amount and accuracy of actual disclosure.	Online privacy	This study

Table 2. Previous research on cognitive biases in the privacy domain¹⁹

Thereby, we see that 1) none of the studies has included the anchoring-effect and 2) none of the studies has researched on the amount and accuracy of actual disclosure. However, the protection of privacy relies on the amount and the accuracy of disclosure and the anchoring-effect might help in explaining what leads individuals to disclose a certain amount of disclosure with a particular accuracy.

¹⁹ The literature review was conducted in the electronic AIS library as well as the entire EBSCO host, using a full-text search with the keywords “cognitive bias” AND privacy. Conferences, except ICIS and CHI were excluded.

Therefore, there exists a research gap on that issue that needs to be addressed.

Considering previous research, one study seems to be researching on the amount of disclosure by including benefits heuristic and fuzzy boundary heuristic as cognitive biases (Sundar et al. 2013). However, this study did not include the accuracy of disclosure, they did not include the anchoring-effect and their study was more a first step towards including cognitive biases into privacy-research without having definite results. They state that “*more experimentation is needed before we can be dispositive of these findings*” (Sundar et al. 2013, p. 815). Other studies also included disclosure, yet, only focused on the intention to disclose (Kehr et al. 2015; Wakefield 2013). And still others have focused only on beliefs in the privacy-related domain (Cho et al. 2010; Choi et al. 2018; Li et al. 2011) or on privacy-protective behaviors (Baek et al. 2014) which is different to disclosure.

Previous research suggests that the anchoring-effect might play a role when researching on disclosure (Acquisti et al. 2017). Consequently, there is also a call from previous research in the privacy domain, to integrate the anchoring-effect to better understand disclosure (Dinev et al. 2015). In this study we will therefore include the anchoring-effect into our research study to better understand the amount and accuracy of disclosure.

In the following, we will therefore explain the anchoring-effect in general and also show in how far previous research already indicates that the anchoring-effect might not only have an effect on disclosure in general but on the amount and accuracy of disclosure in particular.

2.3 THE ANCHORING-EFFECT

The anchoring-effect is one form of a cognitive bias and has been proven to be very robust in everyday decision making processes (Furnham and Boo 2011). It is especially prevalent when individuals are uncertain about their decision (van Exel et al. 2006).

The anchoring-effect is defined as “*the assimilation of a judgment to a previously considered standard*” (Bahník et al. 2017, p. 224). In other words, the anchoring-effect describes that individuals’ judgement is also influenced by the anchor. Thereby, the anchor is a piece of information. For example, judges who sentence the defendant are heavily influenced by the state attorney who suggests a particular sentence. The suggestion by the state attorney is used as an anchor by the judge. The judge then relies on a heuristic by using the anchor to form more simpler judgements. The outcome of the decision is that the higher the suggested sentence the higher the actual sentence by the judge – even for the exact same crime (Enough and Mussweiler 2001). In general, that means that even if the initial conditions are the same – the anchor has the power to influence the final decision of the individual. As stated in the following sections, that even applies when the anchor is completely irrelevant to that decision.

In the following, we outline more information on the anchoring-effect by giving *theoretical explanations*, showing the *origin and content* as well the *presentation and relevancy* of the anchor as a piece of information. We then provide a short *summary on the anchoring-effect* and relate it with privacy.

2.3.1 Theoretical explanations

Two theoretical explanations mainly explain the mechanisms behind the anchoring-effect:

One, *insufficient adjustment*: The anchoring-effect has first been described as a phenomenon in which individuals solve a problem by using the anchor as a starting-point that is then adjusted to come to an actual decision (Tversky and Kahneman 1974). These decisions are then usually insufficient which is why this explanation is called insufficient adjustment. For example, individuals was given a spinning

wheel of fortune, displaying a number between 0 and 100. The individuals did not know that the spinning wheel was faked such that only the number 10 or 65 was displayed. The individuals therefore either received the number 10 or 65. They were then asked if the percentage of African countries in the United Nations is below or above that number. Afterwards, they should estimate the exact percentage of African countries in the United Nations. The results have proven that the median of these individuals who was displayed a 65 on the spinning wheel was 45 – in comparison to these individuals who was displayed a 10, whose median was 25. In other words, those who had a higher number on the spinning wheel also estimated a higher number of African countries. That means, their decision which is the number of African countries, was adjusted by the number on the spinning wheel, which served as the anchor. The individuals therefore used the number as a starting point to then come to a conclusive decision. Another example refers to the more serious domain of price negotiations (Ariely et al. 2003). When two individuals negotiate about a price, both use the first mentioned price – either by the seller or the buyer – as the anchor to then insufficiently adjust the final price.

Two, the *selective accessibility model* (Strack and Mussweiler 1997). More recent research has emphasized that insufficient adjustment is not the only explanation for the anchoring-effect. Rather, the anchor serves as a piece of information activating information in the individual. In particular, the anchor is used to make information more available that is consistent with the anchor (Chapman and Johnson 1999). It is thus the result of an association-based error. In particular, individuals, who are facing a decision to make, rely on information from their memory and their environment. However, they do not use all available information but only a subset of that information. The anchor now serves as a mechanism to define that subset of information. That means that the individual will then rely on a subset of information that is similar to the anchor. This is because individuals usually search for reasons why the presented anchor might be similar with their own information rather than finding reasons why it might be different (Chapman and Johnson 1999). In other words, these individuals conduct a confirmatory hypothesis testing (Chapman and Johnson 1994; Mussweiler and Strack 1999, 2001; Strack and Mussweiler 1997; Wegener et al. 2010). For example, in one study, individuals was given the length of the river Elbe (Mussweiler and Strack 1999). They were then asked to provide a list of thoughts that came through their mind. Those participants, who was given a great number according to the length then tended to present a list of thoughts that is related to such a great length. In comparison, those individuals who was given a low number according to the length then presented a list of thoughts that are related to such a small length. That means, in this study, the two different lengths presented pieces of information that were used as anchors by the individuals. Their decisions were then not adjusted but rather based on the anchor, only a subset of information in their mind was activated.

To better understand the anchoring-effect, one needs on the one hand to understand where it comes from (origin) and what is its' content. On the other hand, the anchor with its' content can be presented in different forms and can be relevant or irrelevant for the decision process.

2.3.2 Origin and content

Origin: The origin is where the anchor is created. It can be created by the environment, e.g. the random number of the spinning wheel, the length of the river Elbe or the sentencing demand by the state attorney. However, the anchor can also be self-generated by the individual. In one example, individuals of two groups should either calculate the value “ $8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$ ” or “ $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8$ ” (Tversky and Kahneman 1974). Both groups had five seconds to calculate the value. The results have shown that the median of the first group was 2,250 whereas the median of the second group was 512 (the correct answer is incidentally 40,320). The reason is that individuals read the equation from left to right such that the first group first calculated 8×7 and so on whereas the other group first calculated 1×2 and so on. Both groups used these numbers – e.g. 56 or 2 – as self-generated anchors. They then estimated the final result based on that anchor. Another example is the freezing point of vodka. Individuals use the freezing

point of water as their self-generated anchor to estimate the freezing point of vodka (Epley and Gilovich 2006).

Content: Independent of the relevancy, the anchor can have different content. Usually, the anchor itself is considered to be a numerical value whereas also the outcome is a numerical value. For example, take again the spinning wheel example: The anchor was a numerical value and so was the outcome. However, the example of the length of the river Elbe has already shown that the outcome does not necessarily have to be a numerical value. Here, a list of thoughts was the outcome. Also, in other studies it was shown that even the anchor itself does not have to be a numerical value (Tomczak and Traczyk 2017). For example, it was shown that when individuals were asked to either draw a long line or a short line, their subsequent answers to the question of the length of the river Mississippi were quite different: Those who have drawn a long line gave answers that were significantly greater than those who have drawn a short line. Drawing a line is obviously different from a numerical input. In another study, a set of qualitative attributes was presented as the anchor (Chapman and Johnson 1999). Again, these attributes were different from a numerical anchor.

Furthermore, extreme values that are beyond the range of sensible answers do not increase the anchoring effect (Mussweiler and Strack 1999, 2001; Wegener et al. 2001). For example, individuals were asked the hottest temperature for a day in Seattle. The provided anchor was 8905° Fahrenheit. Individuals were then asked if their suggested value is above or below that temperature and then estimate the actual value. Results have shown that such an extreme anchor has no anchoring-effect or sometimes even the opposite effect.

2.3.3 Presentation and relevancy of the anchor

Presentation: The presentation, i.e. how the anchor is displayed, can be salient or unobtrusive. In both situations, the anchor works (Bahník et al. 2017). Thereby, even hinting on the anchor and firmly asking individuals to avoid relying on the anchor often does not always have an effect. Hence, not even forewarning individuals about a potential influence of the anchor has to yield to a lower effect of the anchor (Wilson et al. 1996).

Relevancy: The anchor itself can be relevant to the decision process or irrelevant (Furnham and Boo 2011). No matter of the relevancy, the anchor still has the potential to bias the decision. Several studies have shown that even if the anchor itself is completely irrelevant for the decision process, it still biases the decision. For example, the spinning wheel represents an irrelevant piece of information, yet, still biased the final outcome value (Tversky and Kahneman 1974). Despite the fact that the information can be irrelevant to present an anchor, also relevant information can serve as an anchor. For example, it was shown that when giving the individuals a certain height of the Brandenburger Tor and asking them, if they think the actual height is below or above that height, and then estimating the actual height, biased their final decision (Strack and Mussweiler 1997).

2.3.4 Summary of the anchoring-effect and relation to privacy

The anchoring-effect is a cognitive bias that especially takes place, when individuals are uncertain about the outcome of the decision. Explanations refer to either insufficiently adjusting information or by activating a certain subset of information. Independent of the theoretical explanation, the anchor can be self-generated or can come from the environment. The anchor is often a numerical value, but also other pieces of information can serve as anchors. It can be presented salient or unobtrusive and can be a relevant piece of information or an irrelevant piece of information. In sum, the origin, the content, the presentation as well as the relevancy of an anchor can all be different and are not related with each other. For example, taking the example of the wheel of fortune. The origin would be that the number comes from the environment, the content is a numerical value, it is presented in a salient way and it is irrelevant

for the final decision.

Relating the anchoring-effect with privacy, our literature review has shown that previous research has not considered the anchoring-effect in the field of privacy (Dinev et al. 2015). Also, the used examples in this section do not consider privacy due to that research gap. Nevertheless, previous research at least indicates that the anchoring-effect might have an influence on the amount and the accuracy of disclosure.

In particular, taking the example of the wheel of fortune from the introduction (Tversky and Kahneman 1974): It seems like that the accuracy, in this case the estimated percentage of African countries in the U.N., is influenced by the anchor. On the other hand, previous research suggests that the amount, in particular, what we post online might be influenced by an anchor (Acquisti et al. 2017). In addition, previous research has shown that depending on an anchor, individuals have different thoughts in mind and then reproduce these thoughts (Strack and Mussweiler 1997). This suggests that depending on the amount of these thoughts, the amount of disclosure might differ.

In the following, we therefore include the anchoring-effect to research on in how far the anchor has any influence on the amount and the accuracy of disclosure.

3 THE ANCHORING-EFFECT ON ACTUAL DISCLOSURE IN THE PRIVACY-RELATED DOMAIN

In this section, we describe the derivation of hypotheses, the methodology and the results of four studies which all investigate the anchoring-effect on disclosure in privacy research. In the subsequent section, we will discuss these results. In every study, we focus on actual disclosure as the outcome variable. To focus on actual disclosure, we conducted two studies on the amount of disclosure and two studies on the accuracy of disclosure. The reason is that the amount and accuracy are two important concepts of disclosure (Posey et al. 2010; Wheelless 1976) that are also important to understand how individuals manage their privacy (Son and Kim 2008). In the following, we deeper explain the subsections, i.e. the hypothesis, the methodology and the results, of each of the four studies:

Hypothesis: For every of the four studies we have created one hypothesis. With that hypothesis, we conjecture in how far an anchor will either influence the amount (study 1 and study 2) or the accuracy of disclosure (study 3 and study 4). In that section, the derivation of the hypothesis is explained.

Methodology: In this section, we explain, what we did to test the respective hypothesis. In all four studies we conducted quantitative studies and evaluated the results to test our hypotheses.

Results: In this section, we present the results of each of the four studies independently. We thereby show in how far the anchor has an influence on the amount or accuracy of disclosure and we state if the hypothesis has been supported or not.

To firstly conduct these four studies, we rely on participants who we have gathered from Amazon Mechanical Turk (mTurk). mTurk is an online crowdsourcing market (OCM). On such an OCM, individuals earn money for participating in surveys. mTurk has been successfully validated by previous research (Steelman et al. 2014) and it is also considered to be equivalent if not superior to other research methods (Lowry et al. 2016). mTurk has also been successfully used in privacy settings (Bellekens et al. 2016; Pu and Grossklags 2015).

To find out, if the anchoring-effect also affects actual disclosure of information, we have conducted virtually experimental designs. Thereby, in study 1, 2 and 4, participants were randomly assigned to one of two groups. The random assignment was based on a hidden random number in our survey tool. In

both groups, individuals was given a particular task. The task in both groups is similar, yet, different to a degree to research on the anchoring-effect. Generally, the task was to disclose certain information. Here, we asked to actually disclose information and did not ask for the intention to disclose because the intention often does not result in actual behavior (Norberg et al. 2007). Individuals only had to finish one of the two tasks, i.e. disclosing information – depending on their group assignment. The experimental design is therefore a subject-between design. Individuals did not know what group they were assigned to. In fact, they did not even know that they were assigned to any group which makes it a double-blind experimental design. In study 3, individuals were not assigned to different groups, yet, based on their answers they have given, the results were separated into two groups. Details are provided in the methodology section of study 3.

In all four studies, participants were asked to answer questions concerning their demographics (age, gender and country of residence), privacy concerns and their cognitive ability. Privacy concerns are one of the central variables in privacy research – besides disclosure of information (Smith et al. 2011). We therefore included that concept to possibly control for its effect on actual disclosure. In addition, cognitive ability is considered to be one of the main concepts that can potentially influence the anchoring-effect (Furnham and Boo 2011). We used standardized items to measure each of the concepts: privacy concerns on a 7-point Likert scale with 1=strongly disagree and 7=strongly agree (Dinev and Hart 2006) and cognitive ability using the cognitive reflection test (Frederick 2005). The cognitive reflection test consists of three questions which can either be answered correct or incorrect. See Table 11 in the appendix for more details.

To actually answer our research question, we created four different surveys – one for each study. The number of participants in every group ranged from 58 to 72 participants. All in all, we had 528 participants taking part in our surveys. The survey was put online on our own server, using Limesurvey. We then put a link on mTurk to ask workers to conduct the survey. We gave respondents a maximum of seven minutes to conduct the survey and paid each participant \$0.12. We followed the guidelines of previous research to conduct the survey, e.g., by only letting participants take part who have a high ratio of successful completed tasks. To gain a high quality of responses and following recommendations of previous research, we also included a trap question (Lowry et al. 2016). Participants who failed to correctly answer on that question, were removed.

In each of the studies, we conducted t-tests to find out in how far the anchoring-effect takes place. Further details on the hypothesis, the methodology and the results of each study are presented in the following sections. An overall discussion of the results is presented in the subsequent section.

3.1 STUDY 1: AMOUNT OF DISCLOSURE (TEXTBOXES)

To disclose information, individuals are often asked for personal information online by presenting a text input field, called a textbox. For example, online social networks often ask their users to tell something about themselves (e.g., LinkedIn or Facebook). In such cases, individuals can decide on their own how much to disclose. To protect their privacy, they might disclose less information – to gain more benefits such as a better personalization, they might disclose more information (Son and Kim 2008).

However, individuals might also be uncertain on how much they should disclose. Then, they might be especially prone to the anchoring-effect where they possibly do less consider benefits and privacy risks (van Exel et al. 2006). In this study, the aim is to find out in how far the decision on how much to disclose is based on full rationality or if individuals are biased by an anchor.

3.1.1 Hypothesis

Usually an anchor is a numerical value (Tversky and Kahneman 1974), however, it does not have to

be so (Tomczak and Traczyk 2017). In this study, we hypothesize that the size of a textbox is used as an anchor. The anchor is a piece of information that biases subsequent decisions (Bahník et al. 2017). Individuals facing a textbox can often decide on their own, how much to disclose when typing into that textbox. Thereby, they might have the goal to protect their privacy, by not disclosing that much information. However, they also use the size of the textbox as their anchor which leads their thoughts away from protecting their privacy. When they consider the size of a textbox as an anchor, similar thoughts in their mind come up that are related with this size. This is because individuals, using an anchor, rely on the selective accessibility model where the anchor activates a subset of information in ones' mind that is related with this kind of information (Strack and Mussweiler 1997). Therefore, a larger textbox will be more associated with information such as “many words” or “large sentences”. In comparison, a small textbox will be more associated with “few words” or “short sentences”. Thereby, the anchor comes from the environment. Although the size is rather unobtrusive and does not serve as a predominant anchor, previous research has proven that also such unobtrusive anchors bias subsequent decisions (Bahník et al. 2017). This will be strengthened by the fact that the anchor is a relevant anchor – the size of a textbox is not irrelevant in relation to the amount of information to be disclosed. Furthermore, individuals are uncertain on how much they should disclose when an open question is asked, and the answer should be typed in into a textbox. Based on this, individuals will put less effort into the process of how much to disclose but rather use a large textbox as an anchor to disclose more words than when a small textbox is displayed. We hypothesize:

H1: Individuals, confronted with a large textbox, are disclosing more words in comparison to individuals who are confronted with a small textbox.

The methodology to test this hypothesis is presented in the following section.

3.1.2 Methodology

Conduct: To test the hypothesis, we asked individuals to tell us something about their most exciting holidays. In particular, we asked “*Please tell us in detail about your most exciting holidays*”. Answering this question was mandatory to complete the survey.

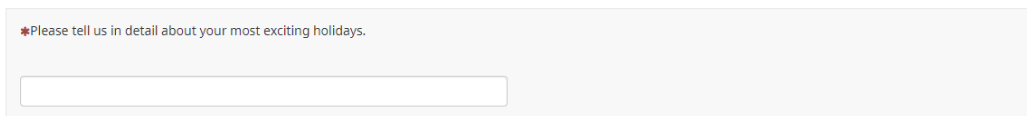


Figure 1. Small textbox

Individuals of group 1 were presented with a small textbox (see Figure 1). This textbox consisted of a one-line-textbox which width was only half as the width of the large textbox. To make sure that individuals were still able to read everything they have disclosed at once, we made the textbox resizable. That means that at the moment, the individuals reached the end of the textbox, the size of the textbox increases by one line such that still all typed in words are readable at once.

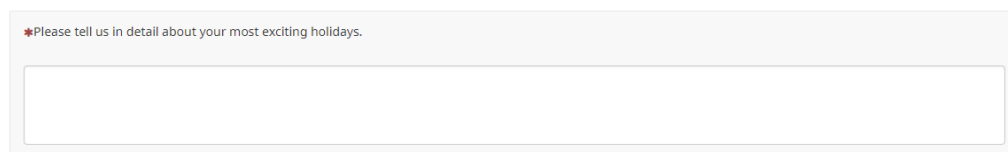


Figure 2. Large textbox

Individuals of group 2 were presented with a large textbox (see Figure 2). This textbox consisted of four lines and the width was as wide as the screen of the participants. Similar as with the small textbox,

this textbox also automatically resizes.

Since the large textbox differs in length as well as in width, the textbox is also bigger even if the survey is undertaken on a smartphone. Thereby, through responsive design, the textbox is shortened such that it fits on the screen of the mobile phone – yet, the large textbox is still larger.

Participants: In group 1, 61 participants took part and in group 2, 60 participants took part. Descriptive data of the participants are depicted in Table 3.

	Group 1 (small textbox)	Group 2 (large textbox)
Age	M:28.17 years Sd: 8.58 years	M:28.73 years Sd:7.18 years
Gender (male = 1; female = 2)	M:1.41 Sd:0.49	M:1.48 Sd:0.49
Cognitive ability (0=no answer correct; 3=all answers correct)	M:0.44 Sd:0.86	M:0.30 Sd:0.76
Privacy concerns (1=strongly disagree;7=strongly agree)	M:4.83 Sd:1.61	M:4.69 Sd:1.57

Table 3. Demographics of the participants of study 1 (M: mean; Sd: standard deviation)

Analysis: We first cleaned the results. We did this by removing those participants who copied and pasted a text from the Internet when they were asked to tell us about their most exciting holidays.

To analyze the results, we counted the number of words for every participant in both groups. Punctuation characters have not been considered to be words such that only full words were used to analyze how much an individual has disclosed.

3.1.3 Results

The results show that our hypothesis is supported. The average number of words in group 1 is 5.78 and in group 2 10.65 words. That means, that individuals disclosed 4,87 more words when the textbox is large in comparison to a small textbox or put another way use 82.96 percent more words. The difference is significant with a p-value < 0.01. The maximum number of words in group 1 is 25 words and in group 2 67 words. The top-eight values of group 2 are all greater than the maximum value of group 1. That means that eight participants of group 2 have disclosed more words than the participant of group 1 who disclosed the maximum number of words in group 1. To also consider the influence of extreme values, we also calculated the median. Again, there is a difference between group 1 and group 2 showing that the median is greater in group 2 than in group 1 (see also Table 4).

	Group 1	Group 2	Difference
Average number of words	5.78	10.65	p-value<0.01
Median	2.5	4	-
Minimum number of words	1	1	-
Maximum number of words	25	67	-

Table 4. Results of study 1 (number of words disclosed)

To gain deeper insights into how the anchoring-effect influences the amount of disclosed information, we conducted a second study.

3.2 STUDY 2: AMOUNT OF DISCLOSURE (CHECKBOXES)

Individuals do not only disclose information by typing in personal information into a textbox. Often, individuals' information is disclosed automatically, e.g. by web browsers, collecting information about the individual (Ermakova et al. 2018). Such information can among others relate to cookies, the IP-address of the individual, her geolocation, the used hardware, the used operating system or the used browser. Such information is then possibly threatening their privacy. When visiting a website, the individual is also often asked to allow the collection of information such as cookies or the geolocation.

The individual is then able to allow that information to be disclosed, e.g. by marking checkboxes what information the owner of the website is allowed to collect.

However, the individual might be uncertain how many checkboxes to mark. In such a case, the anchoring-effect might take place. For example, an owner of a website could state that other individuals usually fill out a specific number of the available checkboxes. This might bias individuals who are using this number as an anchor, to evaluate how many checkboxes to mark. In this study, we will therefore investigate in how far such an anchor will bias an individual's decision to mark checkboxes.

3.2.1 Hypothesis

On websites, individuals are often asked to mark checkboxes to indicate what information they want to disclose about themselves. Examples refer to cookies or the geolocation of an individual (Ermakova et al. 2018). Individuals then have to decide what and especially how many checkboxes they want to mark and thus to indicate how much information they want to disclose. Based on previous research, individuals weigh the benefits and the privacy risks of that disclosure (Dinev and Hart 2006) and based on that rational assessment, they come to a decision how many checkboxes to mark.

However, individuals will also be biased by a possible anchor that might be present (Dinev et al. 2015). For example, there could be a statement on the website, indicating that other individuals usually only mark one checkbox on average. Then, the individual uses that number as a starting point (Tversky and Kahneman 1974) to come to her own decision how many checkboxes to mark. The number is an anchor that is presented by the environment (Bahnik et al. 2017) and also represents a relevant piece of information (Furnham and Boo 2011): If other individuals have only checked one checkbox then it might be sensible to also only check one checkbox. Therefore, the number will bias the subsequent decision process. On the other hand, if the number is greater than one, for example six, then individuals might undergo the same process. With the difference, that they will use six as a starting point when thinking about how many checkboxes to mark. Based on the anchoring-effect (Tversky and Kahneman 1974), individuals will mark more checkboxes when they are presented with a higher anchor, such as six for example. Furthermore, previous research already suggests that such a hypothesized effect exists (Acquisti et al. 2017). We also know from previous research, that individuals discount own information and imitate others (Sun 2013). In this study, we hypothesize that individuals do so by using the information how many checkboxes have been clicked by others as an anchor. We hypothesize:

H2: The greater the number that states how many checkboxes other individuals have marked, the more checkboxes the participant will mark to allow disclosure of information.

To test this hypothesis, we have conducted a survey which is explained in the following section.

3.2.2 Methodology

Conduct: To test the hypothesis, we asked individuals to mark checkboxes. In particular, we asked participants of the survey to mark every checkbox that indicates what information we are allowed to collect. Although we did not really collect that information, the participants of the survey did not know about that. Therefore, they thought they would actually disclose that information by marking the checkboxes. The question contained nine checkboxes with different information that can truly be gathered by website owners: IP-address, browser version, operating system, screen resolution, X- and Y-location of the mouse, names of used plugins of the browser, used hardware, geolocation and the battery status of the device used. That means, individuals could mark either mark 0 or up to 9 checkboxes.

Individuals of group 1 was presented a short sentence right before the question: *On average, individuals allow 1 of the following items to be derived.* Individuals of group 2 was presented the same

sentence, however, it stated that individuals usually allow six of the items to be derived: *On average, individuals allow 6 of the following items to be derived*. With our survey software, we were able to collect the average time, individuals spent to read the short sentence and to answer the question. On average, individuals of group 1 took 33.74 seconds (median 24.55 seconds) and individuals of group 2 took 32.10 seconds (median: 29.58 seconds) to read the sentence and to answer the question. The difference of the timings between both groups is non-significant (p-value=0.39).

Participants: All in all, we had 61 participants in group 1 and 78 participants in group 2 who took part in our survey. Demographics of the participants are depicted in Table 5.

	Group 1 (1 item marked)	Group 2 (6 items marked)
Age	M:34.54 years Sd: 12.89 years	M:34 years Sd:13.84 years
Gender (male = 1; female = 2)	M:1.54 Sd:0.50	M:1.54 Sd:0.50
Cognitive ability (0=no answer correct; 3=all answers correct)	M:1.02 Sd:1.19	M:0.81 Sd:1.14
Privacy concerns (1=strongly disagree;7=strongly agree)	M:4.99 Sd:1.66	M:5.10 Sd:1.47

Table 5. Demographics of the participants of study 2 (M: mean; Sd: standard deviation)

Analysis: To analyze the results, we counted how many checkboxes the individuals marked. We did not check on what checkboxes the individuals marked, but only the number of marked checkboxes. With this, we can state how much information an individual would actually disclose.

3.2.3 Results

The results show that our hypothesis is supported. On average, individuals marked 2.22 checkboxes when the low anchor was presented and 3.12 checkboxes when the great anchor was presented. An increase of 40.54 percent. The difference is also significant. In addition, we calculated the median value. The median value of group 1 is 1, whereas the median of group 2 is 3. That means, regarding the median value, individuals marked two checkboxes more when the high anchor was presented in comparison to the low anchor. Details are provided in Table 6.

	Group 1	Group 2	Difference
Mean value	2.22	3.12	p-value < 0.025
Median	1	3	-
Maximum	9	6	-
Minimum	0	0	-

Table 6. Results of study 2 (number of checkboxes marked)

Besides the amount of information to be disclosed, also the accuracy of disclosure is important to better understand how individuals manage their privacy (Son and Kim 2008). Therefore, in the following two sections, we present two studies concerning the influence of the anchoring-effect on the accuracy of the disclosed information.

3.3 STUDY 3: ACCURACY OF DISCLOSURE WITH UNCERTAIN INFORMATION (NUMBER OF ONLINE ACCOUNTS)

When disclosing information, individuals do not only alter the amount of disclosure but also the accuracy. With more accurate information individuals can often gain more benefits. On the other hand, with more inaccurate information, individuals can better protect their privacy (Son and Kim 2008). In particular, providing inaccurate information might have two reasons: Either because the individual is uncertain about the correct personal information, e.g. when a request for personal information is made, the individual is *uncertain* about. Or because the individual wants to protect her privacy and discloses inaccurate information, although she is *certain* about the correctness of the information (Wheless

1976).

In study 3, we investigate in how far the anchoring-effect takes place when the individual is *uncertain* about the correctness of the disclosed personal information. In study 4, we then investigate the influence of the anchoring-effect, when the individual is *certain* about the personal information to be disclosed.

3.3.1 Hypothesis

Individuals can provide personal information online although not being sure if the information is correct (Wheless 1976). For example, individuals might not know for sure, how many online-accounts they have. If one is asking individuals about the number of their online-accounts, individuals will have to guess. Thereby, they do not aim to protect their privacy by providing a wrong number of online-accounts, however, they rather do not know the correct number of online-accounts.

When guessing, the individual is in a state of uncertainty (Kahneman et al. 1982; Tversky and Kahneman 1974). Especially in such a state, the anchoring-effect takes place (van Exel et al. 2006). Individuals will use the anchor as a starting point to then come to a final guess on how many online-accounts they have. Individuals thereby do not even have to be aware of that they are uncertain about the answer to the question. That means, that individuals do not have to actively use the anchor – they might do so without even being aware of it. Using the example of online accounts: If one is providing a random number when being asked for the number of online accounts, then this number will be used as an anchor to then finally guess the number of online accounts – even if this number is completely irrelevant (Tversky and Kahneman 1974). We therefore hypothesize:

H3: Individual's accuracy of disclosed information, where the individual is uncertain about, is influenced by an irrelevant anchor.

To test the hypothesis, we conducted a survey.

3.3.2 Methodology

Conduct: To test the hypothesis, we asked individuals to type in the last two digits of their cell phone number which is obviously completely irrelevant in the context of the number of online-accounts. This is similar to a previous experiment where individuals should write down the last digit of their social security number (Ariely 2010). Comparable to other studies on the anchoring-effect, we then asked individuals if the number of online accounts they have is above or below that number. Afterwards, they should write down the actual number of online accounts (Furnham and Boo 2011). Different than to the two studies before, individuals were not separated into two groups on a random basis.

Participants: 142 participants took part in our survey. Although individuals were not separated into two groups, based on a random basis, individuals were separated into two groups based on the results. Group 1 consisted of 74 participants and group 2 of 68 participants. More information can be found in the following paragraph. Demographics of the participants are depicted in Table 7.

	Group 1 (small cell phone number)	Group 2 (great cell phone number)
Age	M:39.68 years Sd: 12.16 years	M:38.78 years Sd:13.04 years
Gender (male = 1; female = 2)	M:1.51 Sd:0.50	M:1.55 Sd:0.50
Privacy concerns (1=strongly disagree;7=strongly agree)	M:5.52 Sd:1.31	M:5.39 Sd:1.18
Cognitive ability (0=no answer correct; 3=all answers correct)	M:1.58 Sd:1.38	M:1.38 Sd:1.24

Table 7. Demographics of the participants of study 3 (M: mean; Sd: standard deviation)

Analysis: To analyze the results, we first cleaned the data. We did this by removing all participants

who gave us an unrealistic number of online accounts (such as more than one million online accounts) or who more provided more than two digits of their cell phone number.

To then analyze in how far the provided digits of the cell phone number have an effect on the number of online accounts, we needed to separate the participants. We did this by calculating the median value of the provided digits of the cell phone number. The median in this study was 55. We then had one group, who reported cell phone numbers that were 55 or below (group 1) and one group that reported cell phone numbers that were above 55 (group 2). We then were able to compare the number of provided online accounts between these two groups.

3.3.3 Results

The results indicate that our hypothesis is supported. On average, in group 1, who provided cell phone numbers including or below 55, the number of online accounts is 11.93. In comparison, in group 2, the number of online accounts is 21.15. An significant increase by 77.28 percent. The median value in group 1 is 6 and in group 2, the median value is 10. This further indicates that individuals who provided a cell phone number above 55 also state that they have more online accounts (see Table 8).

	Group 1	Group 2	Difference
Mean value	11.93	21.15	p-value < 0.05
Median	6	10	-
Maximum	170	200	-
Minimum	1	0	-

Table 8. Results of study 3 (number of online accounts)

3.4 STUDY 4: ACCURACY OF DISCLOSURE WITH CERTAIN INFORMATION (ANNUAL GROSS INCOME)

In study 3, we have considered the anchoring-effect when the individual is uncertain about the accuracy of the information. In this study 4, we investigate in how far the anchoring-effect still takes place, when the individual is certain about the accuracy of the information to be disclosed.

3.4.1 Hypothesis

Individuals can disclose information they are certain about. For example, their gross annual income, their year of birth or their own cell phone number. This kind of information is not guessed by the individual, rather they are certain about it. In case individuals are asked to disclose such information, they can either tell the truth, i.e. accurate information, or they lie and disclose inaccurate information (Son and Kim 2008). To protect their privacy, individuals would rather lie and disclose inaccurate information. When telling the truth, individuals would more aim to gain the expected benefits.

However, no matter if individuals want to protect their privacy by providing inaccurate information or to gain benefits by providing accurate information: the anchoring-effect will not influence the content of the information. The reason is because the anchoring-effect usually then applies when individuals are uncertain about the information (van Exel et al. 2006). However, in this case, individuals are certain about the information to be disclosed. They either will tell the accurate information they are certain about or they will disclose inaccurate information, yet, then being certain about that is it inaccurate. We therefore hypothesize:

H4: Individual's accuracy of disclosed information where the individual is certain about the information will not be influenced by an anchor.

We conducted a survey to research on that hypothesis.

3.4.2 Methodology

Conduct: To test the hypothesis, we asked individuals to provide us their gross annual income in US-Dollar. Here, similar to other studies (Furnham and Boo 2011), we first provided individuals an annual gross income in US-Dollar. We then asked, if individuals' gross income is above or below that annual income. Afterwards, they should state their actual gross income in US-Dollar.

Individuals of group 1 was said that the annual gross income of a Chinese worker is \$4,320 per year. In group 2, it was said, that a Chinese workers' gross income \$24,320 per year. Both mentioned annual gross incomes should serve as a potential anchors.

Participants: All in all, we had 60 participants in group 1 and 66 participants in group 2 taking part in our survey. Descriptive data of the participants is depicted in Table 9.

	Group 1 (low income)	Group 2 (high income)
Age	M:34.17 years Sd: 10.55 years	M:34.53 years Sd:11.60 years
Gender (male = 1; female = 2)	M:1.45 Sd:0.50	M:1.53 Sd:0.50
Privacy concerns (1=strongly disagree;7=strongly agree)	M:5.45 Sd:1.34	M:5.30 Sd:1.40
Cognitive ability (0=no answer correct; 3=all answers correct)	M:1.07 Sd:0.86	M:1.21 Sd:1.03

Table 9. Demographics of the participants of study 4 (M: mean; Sd: standard deviation)

Analysis: To analyze the results, we checked on the mean and median value of the given annual gross income by the individuals. We calculated both values for each group – group 1 and group 2. We also checked on in how far both groups have provided values that differ significantly from each other by conducting a t-test.

3.4.3 Results

The results show that our hypothesis is supported. Based on the findings, an anchoring-effect does not take place when it comes to information the individual is certain about. Although the average value of gross income in group 1 is 6.13 percent lower than the income in group 2, that difference is not significant. Furthermore, the median value of group 1 is \$4,000 higher than in group 2 which stands in contrast to the mean value and which supports our hypothesis. Further details are given in Table 10.

	Group 1	Group 2	Difference
Mean value	\$35,473.63	\$37,787.40	p-value > 0.05
Median	\$35,000	\$31,000	-
Maximum	\$100,000	\$150,000	-
Minimum	\$0	\$1	-

Table 10. Results of study 4 (annual gross income)

In the following section, the results of all four studies are discussed in light of current theory and practice.

4 OVERALL DISCUSSION

Understanding why individuals disclose a certain amount of information that is either correct or incorrect is vital to better understand what determines an individuals' management of privacy (Son and Kim 2008). Since previous research has more relied on a rather rational perspective for individuals (Dinev et al. 2015), we have included the anchoring-effect as a cognitive bias in this study (Tversky and Kahneman 1974). The assumption was that the anchoring-effect has an influence on the amount and partly the accuracy of disclosure. Our research confirms that suggestion, giving us the opportunity to answer our research question.

4.1 ANSWERING THE RESEARCH QUESTION

Our research question was about the influence of the anchoring-effect on the amount and the accuracy of disclosure of personal information. After having developed four hypotheses, we can state that the anchoring-effect indeed influences the amount and partly the accuracy of personal information. In particular, in hypothesis 1, we have seen that when being asked to disclose personal information into a textbox, the size of the textbox serves as an anchor. The bigger the textbox, the more information is disclosed. In study 2, the results indicate that more information is disclosed by activating checkboxes, when stating how many checkboxes other individuals have activated. Both hypotheses answer the first part of the research question which is that the anchoring-effect indeed influences the amount of disclosure.

In hypothesis 3, the results indicate that the accuracy of information is also influenced by an anchor, when the individuals are uncertain about the information to be disclosed. In this case, we have used the number of online-accounts, where the individuals might be uncertain of and used the cell-phone number as an anchor. In hypothesis 4, we have shown that the anchoring-effect does not influence the accuracy of information when the individual is certain about that information. Therefore, these hypotheses show that the accuracy of information is influenced by an anchor as long as the individual is uncertain about the information.

Contributions that are based on these results are given in the following section.

4.2 IMPLICATIONS FOR THEORY

Cognitive biases need to be taken into account when doing research on privacy. With this research, we address the lack of considering cognitive biases in privacy research. When conducting future research, scholars should discard the assumption that the individual is a fully rational agent (Dinev et al. 2015) – they should rather take into account that this is not the case.

When doing so, scholars do not need to implement all cognitive biases. It would be more appropriate to on the one hand include cognitive biases which are suitable in that particular research context. For example, the anchoring-effect seemed to be suitable in the context of actual disclosure. However, other cognitive biases might be suitable in other contexts (Dinev et al. 2015). On the other hand, scholars should generally discuss the effect of possible cognitive biases in their studies. For example, by considering cognitive biases in their limitations section or as control variables in their empirical studies.

When doing research on the amount of actual disclosure, the anchoring-effect needs to be considered. To understand the amount of disclosure, privacy risks and benefits are the main influencing variables (Dinev and Hart 2006). With this, scholars have emphasized that the individual is a rational agent and as a result, this view is not very effective, when also considering cognitive biases. More recent research has therefore challenged that perspective by showing that cognitive biases, such as loss aversion, influence beliefs such as benefits or privacy risks (Choi et al. 2018).

With our study, we contribute to this recent research stream. On the one hand, we present the anchoring-effect as an additional cognitive bias that influences privacy-related decisions. On the other hand, we particularly show that the anchoring-effect is directly influencing the amount of disclosure. Individuals not only consider beliefs such as benefits or privacy risks or have cognitive biases which influence such and other beliefs. There are rather cognitive biases such as the anchoring-effect which directly influences the amount of disclosure. Therefore, to better understand the amount of disclosure, scholars need to consider the anchoring-effect.

This could be done by evaluating the effect of possible anchors. Examples of possible anchors refer

to the size of the textboxes, provided information in questions or possible self-generated anchors of the participants. Scholars could also try to eliminate all possible anchors. For example, by trying to create surveys where possibly no anchor exists or by asking individuals about their self-generated anchors and then to subtract out the effect of this self-generated anchor.

On the other hand, previous studies on actual disclosure (e.g., Berendt et al. 2005; Choi et al. 2018; Joinson et al. 2010) might have to be considered under the consideration of the anchoring-effect. Although such studies have brought privacy research a huge step forward, when referencing these studies or trying to use them as a blueprint, scholars might want to also consider the anchoring-effect that might bias the amount of information being disclosed.

The accuracy of disclosed information is influenced by the anchoring-effect. In privacy research, accuracy of disclosure is one important component when researching on disclosure of information (Posey et al. 2010). Especially, when scholars try to understand why individuals falsify information to protect their privacy (Son and Kim 2008). Previous studies including cognitive biases such as the optimistic bias have focused on protecting privacy, yet, have not included providing falsified information (Baek et al. 2014). Other studies have either fully excluded any cognitive biases (Son and Kim 2008) or studies which did include cognitive biases have more focused on beliefs (e.g., Choi et al. 2018).

With our study, we extend his research stream by including the anchoring-effect. We contribute, by showing that the anchoring-effect partly influences the accuracy of information to be disclosed. In particular, we suggest that a) the unconscious falsification of information, i.e. when the individual is uncertain of the information to be disclosed, is influenced by an anchor and b) the conscious falsification of information, i.e. when the individual is certain about the information to be disclosed, does not depend on an anchor. Therefore, when relying on research on falsification of information (Son and Kim 2008), scholars should not only rely on rational factors, or on cognitive biases that influence beliefs but rather should a) consider if the individual is unconsciously falsifying information and b) if they are consciously doing so, then they should consider the anchoring-effect. Therefore, one possibility to avoid the effect of a possible anchor when doing research on accuracy of disclosure, is to ask for information where the individual can be certain of.

4.3 IMPLICATIONS FOR PRACTICE

Individuals' privacy-related decisions depend on the amount and the accuracy of their disclosed information. At the same time, organizations rely on as much personal information of individuals that is as accurate as possible to make their business work (Son and Kim 2008). Based on previous research, organizations should then try to minimize privacy risks as well as to maximize benefits (Dinev and Hart 2006). However, since the individuals is not a full rational agent whose decisions are not fully rational and logical, cognitive biases can also influence the amount and the accuracy of disclosure. Based on our results, we therefore suggest the following practical implications for organizations:

To increase the amount of disclosure, organizations might include anchors. Organizations need as much information as possible from their customers to make their business work (Son and Kim 2008). Since individuals are not always fully rational agents, striving for maximum utility, organizations can exploit this and implement anchors to bring the individual to disclose more information. Possible anchors include the size of a textbox or stating that others have already disclosed that amount of information. On the other hand, there might also be cases where organizations want less information from their customers. For example, when individuals complain about a product or a service. Then, again the organization could implement an anchor which brings the individual to disclose less information, such as a small textbox.

To increase accuracy of disclosure, organizations might refrain from including anchors. Organizations also need as accurate information as possible. Our results suggest that in such cases, organizations should refrain from including anchors – especially when the individuals are uncertain about the information to be disclosed.

Generally, organizations need to decide if and how they want to manipulate customers by anchors or not. Our results suggest that when considering the anchoring-effect, organizations can manipulate individuals regarding their amount and accuracy of disclosure. From an ethical point of view, it might be questionable, in how far organizations should include an anchor to increase the amount and the accuracy of the information to be disclosed. Therefore, we want to highlight that organizations should also think about in how far they should include an anchor or if they want to keep distance from doing so, even when this means that organizations might have to give up information of their customers and to relinquish on the highest correctness of the information. Organizations could thereby also use anchors to decrease the amount and the accuracy of information to be disclosed. This would be contra-productive to their own goals, however, they would try to bring individuals to better protect their privacy.

4.4 LIMITATIONS

This study also has several methodological and theoretical limitations. From a methodological point of view, we only investigated particular anchors. Other forms of anchors might not have an effect on the amount or the accuracy of disclosure. However, we tried to keep that effect to a minimum by conducting four instead of only one study. Also, we only rely on a sample from mTurk. Although mTurk is sometimes considered to be even superior to other research methods (Lowry et al. 2016), using other samples might still widen the range of participants and might yield to further insights into the anchoring-effect. Furthermore, actual disclosure in a survey can be different to actual disclosure in the real world. In a survey, individuals might be more or less sensitive to giving information than in a real-world scenario. We tried to limit this effect by conducting several studies, however, future research might also try to research on the anchoring-effect in a more realistic setting. In addition, it is discussable if all results are good proxies for the amount and the accuracy of disclosure. For example, in how far the number of checkboxes or the number of words actually represent the amount of disclosure needs to be discussed further. We consider this study to be a first step into such a direction in light of the anchoring-effect. Plus, we use the number 55 to split participants into two groups in study 3. Since 55 is not the middle in a range between 0 and 99, it might be that the number of online accounts is not equally distributed. Still, we think that our results provide first evidence that the anchoring-effect exists in such a setting.

From a theoretical point of view, our results are limited to the actual disclosure of information in an online context with information that is less sensitive. In how far the anchoring-effect also influences other concepts in privacy research or information that is more sensitive would be subject to future research. However, with our results we make a first step towards a deeper understanding of the anchoring-effect in the domain of privacy.

4.5 FUTURE RESEARCH

Based on our findings, we suggest several avenues for future research.

One, the privacy calculus with benefits and privacy risks is the dominant theory in privacy research (Dinev et al. 2015). However, it relies on the assumption, that individuals rationally assess benefits and privacy risks and then come to a conclusion what information to disclose. Based on our results, we ask scholars to include the anchoring-effect as a cognitive bias into the privacy calculus to also consider that

effect on the dependent variable. Research questions that could be asked might be, in how far the effect of benefits and privacy risks is diminished when including the anchoring-effect or how much of the dependent variable is better explained when including the anchoring-effect.

Second, many previous studies have researched on the willingness to pay to protect their privacy or the willingness to sell own information when giving up privacy (for a review please see Wagner et al. 2018). Most of these studies have in common that they provide the individual a certain amount of money and ask them if they were willing to pay that price to protect their privacy or if it is an acceptable price to give up privacy. Based on these answers, scholars define a price for privacy. Our research suggests that this price might be biased by the anchoring-effect: individuals use the mentioned price as an anchor to come to a final decision. We therefore ask scholars to investigate, in how far the anchoring-effect takes place, when considering the willingness to protect or the willingness to sell in the domain of privacy.

Third, in previous studies, questions that were being asked to consider the anchoring-effect were usually outside the scope of the individual. For example, the percentage of African countries in the UN or the freezing point of Vodka. In this study, we were asking for personal information that was related to the individual, e.g. the number of online accounts. In comparison to previous studies, the strength of the anchoring-effect was rather small. Future research might want to find out in how far this is because the information that was being provided by the participants was not outside the scope of the participants but was rather personal.

Fourth, in contrast to the majority of previous studies on the anchoring-effect (Furnham and Boo 2011), this study did not solely rely on numerical values as the anchor but also on textboxes as anchors. Future research in the privacy-domain might try to find possible further anchors besides numerical values. One example might be the color of a textbox.

Fifth, (2015) ask not only for the influence of the anchoring-effect on disclosure of information, but also on beliefs such as privacy risks or benefits. We want to emphasize that call and also ask scholars to focus on beliefs in the privacy domain and the influence of an anchor on those beliefs.

Sixth, our study has focused on actual disclosure, as it is requested by previous research (Smith et al. 2011). However, given the vast majority of studies that have focused on intention to disclose, one fruitful future research avenue would be to include the anchoring-effect in a study focusing on intention to disclose, to better be able to evaluate previous studies researching on the intention to disclose.

5 CONCLUSION

In this study, we refrained from the common assumption of a rational dealing individual who comes to rational and logical decisions when disclosing information. Instead, we included the anchoring-effect as a cognitive bias. Our results indicate that the anchoring-effect in particular has an influence on the amount and partly on the accuracy of disclosure. With this, we contribute to theory among others by stating that the anchoring-effect needs to be considered when conducting research on disclosure of information by individuals.

6 APPENDIX

Construct	Items	Author(s)
Privacy concerns (1=strongly disagree; 7=strongly agree)	I am concerned that the information I submit on the Internet could be misused.	Dinev and Hart (2006)
	I am concerned that a person can find private information about me on the Internet.	
	I am concerned about submitting information on the Internet, because of what others might do with it.	
	I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.	
Cognitive ability (0=no answer correct; 3=all answers correct)	A bat and a ball cost \$1.10 in total. The bat costs \$1.00 more than the ball. How much does the ball cost? _____ cents	Frederick (2005)
	If it takes 5 machines 5 minutes to make 5 widgets, how long would it take 100 machines to make 100 widgets? _____ minutes	
	In a lake, there is a patch of lily pads. Every day, the patch doubles in size. If it takes 48 days for the patch to cover the entire lake, how long would it take for the patch to cover half of the lake? _____ days	

Table 11. Questionnaire

7 REFERENCES

- Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., and Schaub, F. 2017. "Nudges for Privacy and Security," *ACM Computing Surveys* (50:3), pp. 1–41.
- Alashoor, T., Lambert, L. S., and Farivar, S. 2016. "A Review of Measures of Disclosure Outcomes in the IS Privacy Literature," in *Proceedings of the Twenty-second Americas Conference on Information Systems*, B. Shin, R. Nickerson and R. Sharda (eds.), San Diego, USA, pp. 1–5.
- Ariely, D. 2010. *Predictably irrational: The hidden forces that shape our decisions*, New York: Harper Perennial.
- d. Ariely, Loewenstein, G., and d. Prelec 2003. "'Coherent Arbitrariness': Stable Demand Curves Without Stable Preferences," *Quarterly Journal of Economics* (118:1), pp. 73–106.
- Baek, Y. M., Kim, E.-m., and Bae, Y. 2014. "My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns," *Computers in Human Behavior* (31), pp. 48–56.
- Bahník, Š., Englich, B., and Strack, F. 2017. "Anchoring Effect," in *Cognitive illusions: Intriguing phenomena in thinking, judgment and memory*, R. Pohl (ed.), London, New York: Routledge, pp. 223–241.
- Bazerman, M. H., and Moore, D. A. 2013. *Judgment in managerial decision making*, Hoboken, NJ: Wiley.
- Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1042.
- Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., and Seeam, A. 2016. "Pervasive eHealth services a security and privacy risk awareness survey," in *International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, C. Onwubiko and T. Owens (eds.), London, United Kingdom, pp. 1–4.
- Berendt, B., Günther, O., and Spiekermann, S. 2005. "Privacy in e-commerce," *Communications of the ACM* (48:4), pp. 101–106.
- Bodenhausen, G. V., Mussweiler, T., Gabriel, S., and Moreno, K. N. 2001. "Affective influences on stereotyping and intergroup relations," in *Handbook of affect and social cognition*, Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers, pp. 319–343.
- Cavusoglu, H., Phan, T. Q., Cavusoglu, H., and Airoidi, E. M. 2016. "Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook," *Information Systems Research* (27:4), pp. 848–879.
- Chapman, and Johnson 1999. "Anchoring, Activation, and the Construction of Values,"

- Organizational behavior and human decision processes* (79:2), pp. 115–153.
- Cho, H., Lee, J.-S., and Chung, S. 2010. “Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience,” *Computers in Human Behavior* (26:5), pp. 987–995.
- Choi, B., Wu, Y., Yu, J., and Land, L. 2018. “Love at First Sight: The Interplay Between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management,” *Journal of the Association for Information Systems* (19:3), pp. 124–151.
- Cialdini, R. B. 2010. *Influence: Science and practice*, Boston, Mass.: Pearson.
- Dinev, T., and Hart, P. 2006. “An extended privacy calculus model for e-commerce transactions,” *Information Systems Research* (17:1), pp. 61–80.
- Dinev, T., McConnell, A. R., and Smith, H. J. 2015. “Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box,” *Information Systems Research* (26:4), pp. 636–655.
- Enough, B., and Mussweiler, T. 2001. “Sentencing Under Uncertainty: Anchoring Effects in the Courtroom1,” *Journal of applied social psychology* (31:7), pp. 1535–1551.
- Epley, N., and Gilovich, T. 2006. “The anchoring-and-adjustment heuristic: why the adjustments are insufficient,” *Psychological science* (17:4), pp. 311–318.
- Ermakova, T., Fabian, B., Bender, B., and Klimek, K. 2018. “Web Tracking – A Literature Review on the State of Research,” in *Hawaii International Conference on System Sciences 2018 (HICSS-51)*, T. Bui (ed.), Hilton Waikoloa Village, Hawaii.
- Frederick, S. 2005. “Cognitive Reflection and Decision Making,” *Journal of Economic Perspectives* (19:4), pp. 25–42.
- Furnham, A., and Boo, H. C. 2011. “A literature review of the anchoring effect,” *The Journal of Socio-Economics* (40:1), pp. 35–42.
- Gerlach, J., Widjaja, T., and Buxmann, P. 2015. “Handle with care: How online social network providers’ privacy policies impact users’ information sharing behavior,” *The Journal of Strategic Information Systems* (24:1), pp. 33–43.
- Gerlach, J. P., Buxmann, P., and Dinev, T. 2019. ““They’re All the Same!” Stereotypical Thinking and Systematic Errors in Users’ Privacy-Related Judgments About Online Services,” *Journal of the Association for Information Systems* (20:6), pp. 787–823.
- Haselton, M. G., Nettle, D., and Andrews, P. W. 2015. “The Evolution of Cognitive Bias,” in *The Handbook of Evolutionary Psychology*, D. M. Buss (ed.), Hoboken, NJ, USA: John Wiley & Sons, Inc, pp. 724–746.
- Hollenbaugh, E. E., and Ferris, A. L. 2015. “Predictors of honesty, intent, and valence of Facebook self-disclosure,” *Computers in Human Behavior* (50), pp. 456–464.
- Hui, K.-L., Teo, H.-H., and Lee, S.-Y. T. 2007. “The value of privacy assurance: An exploratory field experiment,” *MIS Quarterly* (31:1), pp. 19–33.
- Jensen, C., Potts, C., and Jensen, C. 2005. “Privacy practices of Internet users Self-reports versus observed behavior,” *International Journal of Human-Computer Studies* (63:1-2), pp. 203–227.
- Joinson, A., Reips, U.-D., Buchanan, T., and Schofield, C. B. P. 2010. “Privacy, Trust, and Self-Disclosure Online,” *Human-Computer Interaction* (25:1), pp. 1–24.
- Kahneman, D., Slovic, P., and Tversky, A. 1982. *Judgment under uncertainty: Heuristics and biases*, Cambridge: Cambridge Univ. Press.
- Karwatzki, S., Trenz, M., Tuunainen, V. K., and Veit, D. 2017. “Adverse consequences of access to individuals’ information: An analysis of perceptions and the scope of organisational influence,” *European Journal of Information Systems* (26:6), pp. 688–715.
- Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. “Thinking Styles and Privacy Decisions: Need for Cognition, Faith into Intuition, and the Privacy Calculus,” in *Wirtschaftsinformatik 2015*, O. Thomas and F. Teuteberg (eds.), Osnabrück, Germany.
- Li, H., Sarathy, R., and Xu, H. 2011. “The role of affect and cognition on online consumers’ decision to disclose personal information to unfamiliar online vendors,” *Decision Support Systems* (51:3), pp. 434–445.
- Lowry, P. B., D’Arcy, J., Hammer, B., and Moody, G. D. 2016. ““Cargo Cult” science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels,” *Journal of Strategic Information Systems* (25:3), pp. 232–240.

- Mussweiler, T., and Strack, F. 1999. "Hypothesis-Consistent Testing and Semantic Priming in the Anchoring Paradigm: A Selective Accessibility Model," *Journal of Experimental Social Psychology* (35:2), pp. 136–164.
- Mussweiler, T., and Strack, F. 2001. "The Semantics of Anchoring," *Organizational behavior and human decision processes* (86:2), pp. 234–255.
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.
- Ployhart, R. E., and Vandenberg, R. J. 2010. "Longitudinal Research: The Theory, Design, and Analysis of Change," *Journal of Management* (36:1), pp. 94–120.
- Posey, C., Lowry, P. B., Roberts, T. L., and Ellis, T. S. 2010. "Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities," *European Journal of Information Systems* (19:2), pp. 181–195.
- Pu, Y., and Grossklags, J. 2015. "Using Conjoint Analysis to Investigate the Value of Interdependent Privacy in Social App Adoption Scenarios," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- Smith, J. H., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 980–1015.
- Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503–529.
- Steelman, Z. R., Hammer, B. I., and Limayem, M. 2014. "Data Collection in the Digital Age: Innovative Alternatives to Student Samples," *MIS Quarterly* (38:2), pp. 355–378.
- Strack, F., and Mussweiler, T. 1997. "Explaining the enigmatic anchoring effect: Mechanisms of selective accessibility," *Journal of Personality and Social Psychology* (73:3), pp. 437–446.
- Sun, H. 2013. "A longitudinal study of herd behavior in the adoption and continued use of technology," *MIS Quarterly* (37:4), p. 1013.
- Sundar, S. S., Kang, H., Wu, M., Go, E., and Zhang, B. 2013. "Unlocking the privacy paradox," in *CHI '13 Extended Abstracts on Human Factors in Computing Systems on*, W. E. Mackay, S. Brewster and S. Bødker (eds.), Paris, France, ACM Press, p. 811.
- Tang, J.-H., and Wang, C.-C. 2012. "Self-disclosure among bloggers: re-examination of social penetration theory," *Cyberpsychology, behavior and social networking* (15:5), pp. 245–250.
- Tomczak, P., and Traczyk, J. 2017. "The mechanism of non-numerical anchoring heuristic based on magnitude priming: is it just the basic anchoring effect in disguise?" *Polish Psychological Bulletin* (48:3), pp. 401–410.
- Tversky, A., and Kahneman, D. 1974. "Judgment under Uncertainty: Heuristics and Biases," *Science* (185:4157), pp. 1124–1131.
- van Exel, N.J.A., Brouwer, W.B.F., van den Berg, B., and Koopmanschap, M. A. 2006. "With a little help from an anchor," *The Journal of Socio-Economics* (35:5), pp. 836–853.
- Wagner, A., Krasnova, H., Abramova, O., Buxmann, P., and Benbasat, I. 2018. "From Privacy Calculus to Social Calculus: Understanding Self-Disclosure on Social Networking Sites," in *Proceedings of the Thirty ninth International Conference on Information Systems*, R. Baskerville and R. Nickerson (eds.), San Francisco, CA, USA.
- Wakefield, R. 2013. "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems* (22:2), pp. 157–174.
- Wegener, D. T., Petty, R. E., Detweiler-Bedell, B. T., and Jarvis, W.B. G. 2001. "Implications of Attitude Change Theories for Numerical Anchoring: Anchor Plausibility and the Limits of Anchor Effectiveness," *Journal of Experimental Social Psychology* (37:1), pp. 62–69.
- Wheless, L. R. 1976. "Self-disclosure and interpersonal solidarity: Measurement, validation, and relationships," *Human Communication Research* (3:1), pp. 47–61.

Paper IX

PERCEIVED INFORMATION SENSITIVITY AND INTERDEPENDENT PRIVACY PROTECTION

A QUANTITATIVE STUDY

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Tim Weitzel

University of Bamberg

electronic markets (29:3), pp. 359–378 (2019)

<https://link.springer.com/article/10.1007/s12525-019-00335-0>



Chapter IV

Privacy Turbulence

Paper X

**STRENGTH OF TIES AS AN
ANTECEDENT OF PRIVACY
CONCERNS
A QUALITATIVE RESEARCH STUDY**

Jakob Wirth
University of Bamberg

Proceedings of the 23rd Americas Conference on Information Systems (2017), D. Strong and J. Gogan (eds.), Boston, MA, USA
<https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/13/>

Paper XI

**DRIVERS OF EMAIL TRACKING
PRIVACY PROTECTION
BEHAVIOR**
A TWO-WAVE QUANTITATIVE STUDY

Jakob Wirth

University of Bamberg

Christian Maier

University of Bamberg

Sven Laumer

Friedrich-Alexander-Universität Erlangen-Nürnberg

Tim Weitzel

University of Bamberg

DRIVERS OF EMAIL TRACKING PRIVACY PROTECTION BEHAVIOR

A TWO-WAVE QUANTITATIVE STUDY

Abstract

Email tracking violates individual privacy. By tracking an email, the sender can collect information about whether, when and where an email has been opened. Despite this invasion of their privacy, it is indicated that most people do not protect themselves against email tracking. This study aims to identify, what factors influence email tracking protection behavior and applies the protection motivation theory (PMT), which suggests that appealing to people's fear motivates them to protect themselves against email tracking. A fear appeal is a message designed to frighten people and to show them, how to protect themselves against a threat. This study incorporates fear appeal and other concepts from PMT in the research model design, which is then tested in a two-wave quantitative behavioral study. Among other findings, the results indicate that fear appeal significantly influences individual email tracking protection behavior. This research study contributes to the research area of email tracking by identifying factors influencing email tracking behavior and demonstrating the value of applying PMT in privacy research.

Keywords: privacy, email tracking, protection motivation theory, fear appeal, two-wave study, behavior

1 INTRODUCTION

Individuals face a range of privacy threats through, for instance, e-mail tracking (Englehardt et al. 2018). Possible consequences include identity theft, drawing sensitive inferences from individuals' information, manipulation or discrimination. All this makes privacy a central issue of our times (Acquisti et al. 2015). Yet, privacy behavior is surprisingly diverse. Not everyone protects their privacy, and many provide authentic personal information on the Internet. Others, yet, offer wrong information about themselves purposefully to protect their privacy (Son and Kim 2008). Better understanding why individuals behave in such different ways is an important first step to improve privacy protection.

Email tracking violates the privacy of the email recipient (Englehardt et al. 2018). Email tracking is a technology a sender can use to collect information about the recipient such as whether, what time, and where the email is opened (Bender et al. 2016; Brunet 2017; Fabian et al. 2015; Merchant 2017). Studies indicate that 99 percent of electronic newsletters (Brunet 2017) and roughly every fifth conversational email is tracked (Merchant 2017). Email tracking can be potentially harmful to individuals. For example, burglars can use email tracking to determine whether potential victims are at home. If a burglary target opens emails from a remote location, the burglar could deduce that the target is likely not at home (Xu et al. 2018).

However, despite these disadvantages and even though it is possible to prevent email tracking, surveys indicate that email tracking is pervasive and that most users do not protect themselves (Xu et al. 2018). Assuming users want to avoid disadvantages (van Eerde and Thierry 1996), there is a need to understand what factors drive email tracking protection behavior. Based on the protection motivation theory (PMT) (Rogers and Prentice-Dunn 1997), protection behavior is strongly influenced by a so-called fear appeal (Boss et al. 2015). A fear appeal is a message intended to increase individuals' fear of a threat while also providing information on how to protect against the threat. In the present case, a fear appeal could make people afraid of the threat of burglars using information gleaned from email

tracking technology to determine whether potential targets are at home, and describe how they can protect themselves against email tracking. Hence, applying the PMT and including a fear appeal might help explaining why individuals obviously do not protect themselves against email tracking (Xu et al. 2018).

Previous research on email tracking, a major threat to individual privacy (Bender et al. 2016; Bonfrer and Drèze 2009; Englehardt et al. 2018; Fabian et al. 2015; Xu et al. 2018), has not investigated what drives individual email tracking protection behavior and has called for further research into these drivers. In this paper, we apply PMT and assess the fear appeal as a step toward filling this research gap. Our research question is:

To what degree do fear appeals influence individual email tracking protection intention and behavior?

The protection motivation theory (PMT) has often been used inadequately in IS research (Boss et al. 2015). Several concepts have been lacking, relationships have been used incorrectly and additional concepts have been added without showing how they contribute to PMT. Boss et al. (2015) have therefore made recommendations on how to use PMT adequately, such as by including a fear appeal and by using the full nomology of PMT. Although the authors study has brought us a huge step forward when applying PMT in an IS context, their results are limited to a security context. In this research study, we conduct research in a privacy context. Although these areas of research are related, they are still distinct (Dincelli et al. 2017; Smith et al. 2011). Hence, Boss et al.'s (2015) findings may not be simply transferred to the context of email tracking in the privacy-related domain. However, although PMT has also been used in the privacy literature (e.g. Alashoor et al. 2017; Kim 2016; Mousavizadeh and Kim 2015) none of the studies has used the full nomology of PMT or included a fear appeal.

To fill this gap, this study applies the core version of PMT with its full nomology and a fear appeal in a privacy-related context, thus contributing to research in two ways. First, it contributes to the email tracking research stream (e.g. Bender et al. 2016; Fabian et al. 2015) by applying PMT to identify the drivers of email tracking protection behavior. Our contextualized implications provide new insights into the effects of PMT, making the overall results more robust (Hong et al. 2014). In particular, we show that a) several concepts of PMT are more influential in a high fear appeal context, b) one concept of PMT is more influential in a low fear appeal context, and c) fear appeal in general promotes email tracking behavior.

Second, our research applies PMT in a privacy-related context. Previous privacy research has failed to include a fear appeal when applying PMT. Following Boss et al.'s (2015) recommendation to include the fear appeal when applying PMT, we contribute to privacy research in general by demonstrating a) the value of including a fear appeal, b) that disregarding select concepts of PMT can lead to unexpected results (e.g. Marett et al. 2011; Mohamed and Ahmad 2012), and c) that the intention-behavior gap in privacy research (Smith et al. 2011) may be better understood when including a fear appeal.

The remainder of this paper is structured as follows. First, we summarize email tracking scholarship and identify relevant research gaps. We then discuss PMT and present our research model. Afterwards, we explain the methodology and results of our two-wave quantitative study and discuss their implications for email tracking research, research on PMT in the domain of privacy and for practical application.

2 EMAIL TRACKING

Email tracking is extremely prevalent. Studies show that 99 percent of newsletters sent by organizations and 19 percent of conversational emails are tracked (Brunet 2017; Merchant 2017). Email

tracking is defined as a technology which allows an email sender to gather information about the recipient who discloses information unintentionally (Bender et al. 2016). The email sender may be an individual or an organization. The information gathered about the recipient may include the IP address, the geo-location, whether and when the email was opened, the operating system, device and provider used to open the email. Recipients might know that emails can be tracked, but usually do not know when it is happening, have not consented to it, do not know what kind of information is disclosed or that no action must be taken on their part to disclose the information (Bender et al. 2016; Karwatzki et al. 2017).

2.1 FUNCTIONAL PRINCIPLE

The functional principle of email tracking follows six steps illustrated in Figure 1.

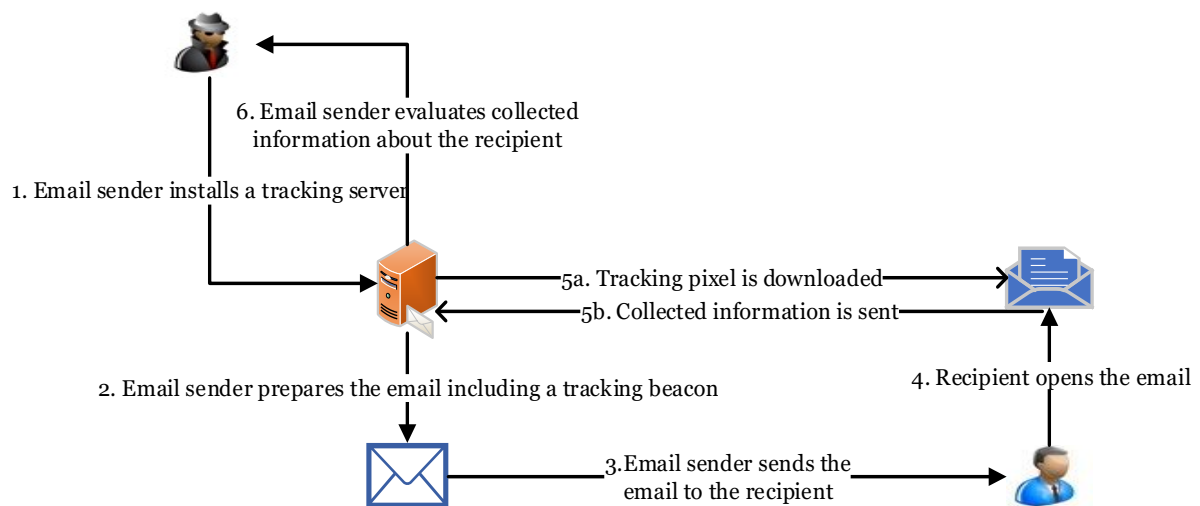


Figure 1. Functional principle of email tracking (Bender et al. 2016)

First, the *email sender installs a tracking server* with logging-software which enables the email sender to gather information about the recipient. Second, the *email sender prepares an email including a tracking beacon* which tracks the recipient. To implement the tracking beacon the email needs to be formatted in HTML format. The tracking beacon is typically a small, usually 1x1 pixel, invisible image in the email. This image is stored on the tracking server and the link to it is individualized so it can be traced back to the recipient. Third, the *email sender sends the email to the recipient*. Regardless of whether the email is individual or a mass email such as a newsletter, the tracking beacon is individualized. Receiving an email without opening it will not activate the tracking beacon (Bender et al. 2016). Fourth, the *recipient opens the email*. Depending on the email program and settings, images may or may not be downloaded automatically. If images are not downloaded automatically and the recipient does not give the program permission to do so, the image will not be downloaded, and tracking will not occur. If images are downloaded automatically or the recipient downloads the images manually, in step five, the *tracking pixel is downloaded* from the tracking server and *collected information is sent* to the tracking server. Sixth, the *email sender evaluates collected information about the recipient* stored on the tracking server and can use the information in various ways. To protect their privacy and to subsequently avoid further negative consequences, recipients can rely on measures to protect themselves against email tracking.

2.2 PROTECTION MEASURES

There are several ways recipients can protect themselves against email tracking, but they are not all equally effective. *Disabling automatic image download* is the most effective way to protect against email tracking. Another protection measure involves implementing a proxy server. However, tracking

still occurs and installing and operating a proxy server is expensive and complex. A further measure would be to selectively block the tracking content of emails. However, this does not yet work perfectly and promising solutions are not yet on the market (Bender et al. 2016). Disabling automatic image download is the only effective solution currently available, but may result in emails not being displayed correctly if all images are blocked. In this study, we consider *disabling automatic image download* as the privacy protection behavior recipients can adopt to protect themselves against email tracking. In the following section, we review previous research on email tracking and identify research gaps.

2.3 REVIEW OF RESEARCH ON EMAIL TRACKING AND RESEARCH GAPS

Previous research into email tracking falls into several categories: 1) *Mechanisms to protect against email tracking*. Two studies have been conducted in this category. On the one hand, there is an algorithm that filters tracking elements in emails to protect against email tracking without blocking other images not containing tracking elements. However, this solution is not yet available on the market (Bender et al. 2016). On the other hand, Fabian et al.'s (Fabian et al. 2015) review of email tracking literature provides deep insights into methods, detection and usage of email tracking. 2) *Privacy implications of email tracking*. It has been shown that the connection between surfing the web and being tracked via email can lead to further privacy implications (Englehardt et al. 2018). Privacy concerns of individuals in the context of email tracking have also been the subject of research (Xu et al. 2018). 3) *Evaluating email tracking campaign effectiveness*: Scholars have provided and evaluated a live monitoring tool (Bonfrer and Drèze 2009) and have researched the general effectiveness of email tracking (Hasouneh and Alqeed 2010) from the perspective of the email sender.

Mapping these three research streams to the example of the burglar from the introduction, extant research has focused on 1) what residents can do to protect against email tracking (mechanisms to protect against email tracking), 2) the danger that burglars can use information collected by email tracking to burglarize residents (privacy implications of email tracking), and 3) how the burglar can evaluate whether email tracking has been effective (evaluating email tracking campaign effectiveness). However, the question of what drives a resident to protect him- or herself against email tracking to avoid potential burglary has been neglected. Hence, the first research gap our study intends to fill is what drives email tracking protection behavior. To do so, we apply protection motivation theory (PMT).

3 THE PROTECTION MOTIVATION THEORY

The Protection Motivation Theory (PMT) has been applied in privacy- and in security-related studies. Although privacy and security are related areas of research, they are distinct (Dincelli et al. 2017; Smith et al. 2011). In fact, Smith et al. (2011) point out explicitly, that security and privacy are related, but security is not privacy. In the domain of IS, security is more about taking measures to protect information. For example, backing up a hard drive to avoid subsequent data loss is a security measure. In contrast, privacy issues are related to the collection and improper use of personal information. For example, collecting and using private information to personalize advertisements is a privacy issue. This difference justifies treating security- and privacy-related behavior differently as well (Dincelli et al. 2017).

Since this research study focuses on the privacy-related domain, we concentrate on privacy-related research which has applied PMT. We begin by using Boss et al.'s (2015) study as a basis to determine to what degree their results in the security-related domain are applicable to the privacy-related domain.

3.1 PROTECTION MOTIVATION THEORY IN THE DOMAIN OF PRIVACY

The core version of PMT applied to the context of email tracking has four processes: 1) the threat appraisal process through which individuals evaluate to what degree email tracking is an actual threat;

2) the coping appraisal process, through which individuals evaluate to what degree they are able to disable automatic image download to protect against email tracking; 3) the behavior process, which is the degree to which the intention to protect against email tracking results in actual behavior; 4) the fear appeal process, which is how survey participants react when the threat of email tracking is made real and disabling automatic image download is presented as an effective response to protect against email tracking. It is important to consider the difference between the fear appeal and the threat appraisal process. Whereas the fear appeal is there to trigger individuals to consider an actual threat and to receive a message which shows them how to protect against the threat, the threat appraisal process is merely the evaluation of the threat (Boss et al. 2015; Rogers and Prentice-Dunn 1997).

To evaluate previous research in the privacy-related domain which applied PMT, we conducted a literature review.

3.2 LITERATURE REVIEW ON THE PROTECTION MOTIVATION THEORY IN THE DOMAIN OF PRIVACY

The literature review was conducted by searching for articles in the AIS electronic library as well as in the EBSCO Business Host. We used “*protection motivation theory*” as well as “*privacy*” as our keywords. The results (see Table 5 in the appendix) reveal that processes 1 and 2 have been used and supported in many privacy studies, but several concepts have been disregarded for both processes. Furthermore, processes 3 and 4 have been neglected by most previous studies in the privacy-related field. Leaving out process 3, the behavior process, has led to an incomplete view on protection behavior because only intentions were measured instead of actual behavior (Smith et al. 2011). Leaving out process 4, the fear appeal process, might also be problematic since no threat was made real and no effective response was provided (Boss et al. 2015).

With this knowledge in mind, we apply the full nomology of PMT including all four processes in the context of privacy and depict it in a research model.

4 RESEARCH MODEL

In this study we apply the full nomology of PMT to identify what drives email tracking protection behavior. We include 1) the threat appraisal process, 2) the coping appraisal process, 3) the behavior process and 4) the fear appeal process. We apply PMT to explain why individuals have a certain protection intention and subsequent protection behavior. The protection intention is being motivated to conduct an effective recommended response against a threat and the subsequent actual behavior is actually responding (Boss et al. 2015). In our case, the protection intention of individuals is the intention to disable automatic image download. The subsequent behavior is disabling automatic image download. All other constructs remain as originally developed by PMT. However, in general, all constructs are privacy-related since they are all adapted to the context of email tracking in the domain of privacy. This is in line with previous research and follows the suggestions of Boss et al. (2015), who recommend not changing the name of the constructs, independent of the context one is researching on. In addition, we also control for the effect of privacy concerns on the behavior of disabling automatic image download. The reason is that privacy concerns is the central concept in privacy research (Smith et al. 2011) and its possible effect should therefore be evaluated. Figure 2 depicts the research model including all four processes. In the following, the hypotheses for each process are explained.

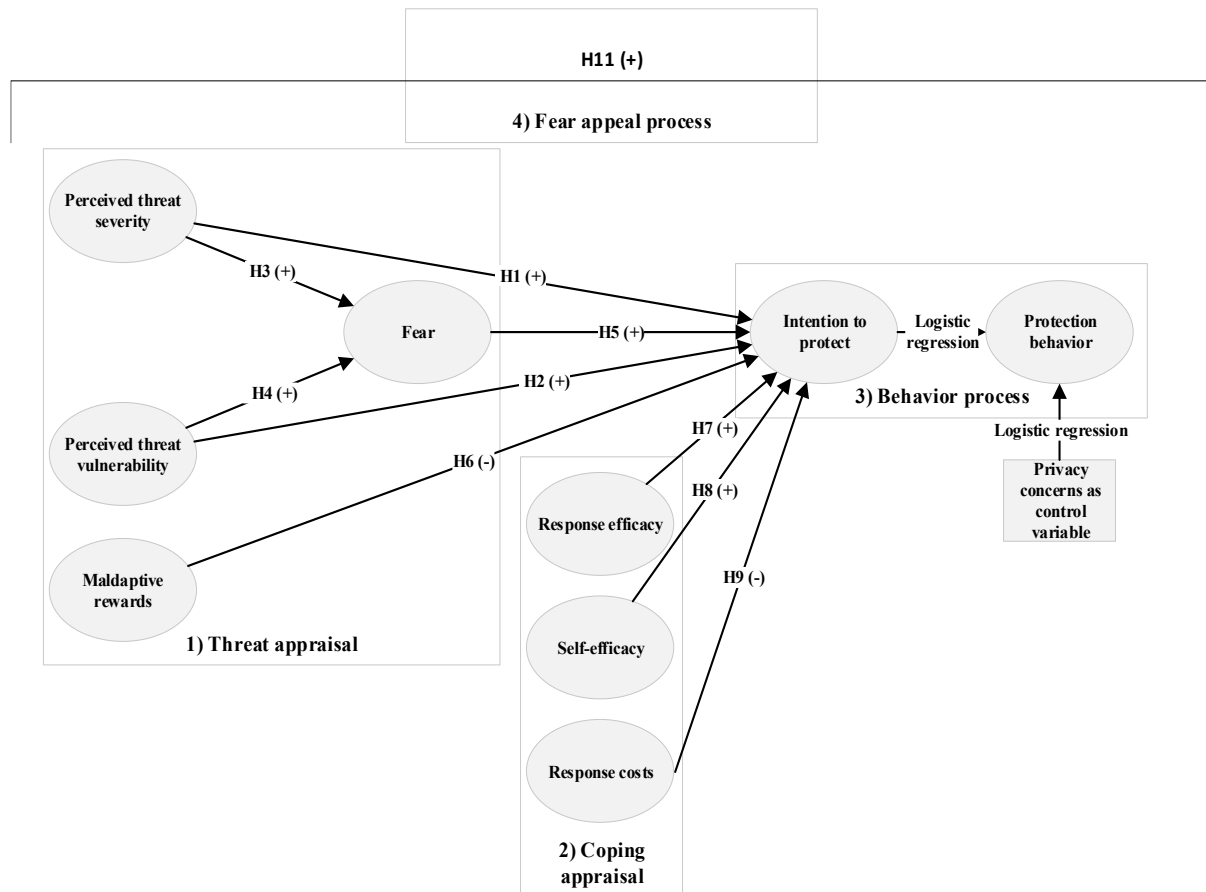


Figure 2. Research model based on the Protection Motivation Theory (Boss et al. 2015; Rogers and Prentice-Dunn 1997)

4.1 THREAT APPRAISAL PROCESS

In this process, individuals evaluate how much email tracking could threaten them and whether the level of fear of email tracking outweighs the possible maladaptive rewards. A threat is a source of danger which causes loss of control over authentic personal information, resulting in harm to the individual (Floyd et al. 2000). In particular, individuals assess the perceived threat severity, meaning how significant email tracking could be to them and what possible harm email tracking might cause to them. On the other hand, they also evaluate the perceived threat vulnerability by considering their own susceptibility to email tracking. Email tracking can be severe in terms of privacy violation and subsequent disadvantages. Individuals who do not disable automatic image download are also vulnerable to email tracking. Individuals do not want to experience any disadvantages, including through email tracking, because they try to minimize disadvantages and to maximize advantages (van Eerde and Thierry 1996). They also do not want to be vulnerable to email tracking to avoid any subsequent disadvantages (Englehardt et al. 2018), which leads to a higher intention to protect themselves against email tracking. In line with PMT we hypothesize:

H1: The higher the perceived threat severity, the higher the intention to disable automatic image download.

H2: The higher the perceived threat vulnerability, the higher the intention to disable automatic image download.

Based on the evaluation of the severity and vulnerability of email tracking, individuals generate a certain level of fear against email tracking. Fear is thereby defined as "a relational construct aroused in response to a situation that is judged as dangerous" (Rogers 1975, p. 96). If individuals think that email

tracking is a severe threat and if they think they are vulnerable to that threat, then that threat is considered to be dangerous and fear is the natural response to that judgement. In line with PMT we hypothesize:

H3: The higher the perceived threat severity, the higher the fear.

H4: The higher the perceived threat vulnerability, the higher the fear.

In case individuals are frightened, i.e. have a certain level of fear due to email tracking, they are more likely to be motivated to disable automatic image download to reduce their level of fear against that threat (Boss et al. 2015; Osman et al. 1994; Rogers 1975; Witte 1992). Disabling automatic image download will help individuals to reduce threat severity and threat vulnerability which will then reduce their level of fear. In line with PMT we hypothesize:

H5: The higher the fear, the higher the intention to disable automatic image download.

Maladaptive rewards present an evaluation of the received benefits of not disabling automatic image download (Boss et al. 2015; Rogers and Prentice-Dunn 1997). For example, individuals might want to make sure that their emails are displayed correctly, which is easier when automatic image download is not disabled. Hence, it is not about the effort to disable automatic image download, but it is about the disadvantages that come along when disabling automatic image download. Since individuals try to gain as much positive outcomes as possible (van Eerde and Thierry 1996), individuals have a lower intention to disable automatic image download when maladaptive rewards are high. In line with PMT we hypothesize:

H6: The higher the maladaptive rewards, the lower the intention to disable automatic image download.

4.2 COPING APPRAISAL PROCESS

In this process, individuals evaluate to what degree they are capable of protecting themselves against email tracking. Their efficacy must outweigh the possible costs of disabling automatic image download. Individuals thereby assess their *response efficacy*, which is the degree to which disabling automatic image download is a sufficient response to mitigate email tracking. At the same time, individuals also assess their *self-efficacy*, which is their capability to conduct the response. Disabling automatic image download can be technically difficult, e.g. because settings vary, look different and are located in different places across email programs and web clients. Individuals, who assess their self-efficacy to disable automatic image download as high will have a higher intention to do so because they believe they can do so, which is a necessary prerequisite (Boss et al. 2015; Rogers and Prentice-Dunn 1997). Also, if individuals think that disabling automatic image download is an effective response they will do so in order to diminish the disadvantages they are trying to avoid (van Eerde and Thierry 1996). In line with PMT we hypothesize:

H7: The higher the response efficacy, the higher the intention to disable automatic image download.

H8: The higher the self-efficacy, the higher the intention to disable automatic image download.

In addition to efficacy, individuals also rate the response costs, which are expenditures associated with disabling automatic image download (Boss et al. 2015). For example, for some individuals it can be time consuming to learn how to disable image download. Individuals try to minimize costs and to maximize benefits (van Eerde and Thierry 1996). If response costs exceed the response efficacy and self-efficacy, it means that the costs exceed the benefits. Individuals who perceive the response costs as high are less likely to disable automatic image download to avoid these response costs. We hypothesize:

H9: The higher the response costs, the lower the intention to disable automatic image download.

4.3 BEHAVIOR PROCESS

Privacy research usually investigates intentions (Smith et al. 2011). However, in the context of privacy research, studies show an intention-behavior gap, i.e. individuals often state their intention to protect their privacy but behave to the contrary (Smith et al. 2011). Although intention is often not a good predictor of behavior, it is still considered to be the best one (Milne et al. 2000). Individuals, who are motivated to disable automatic image download are more likely to actually disable automatic image download. In line with PMT we hypothesize:

H10: A high intention to disable automatic image download leads to actual behavior of disabling automatic image download.

4.4 FEAR APPEAL PROCESS

To conduct threat and coping appraisal processes, individuals need to face email tracking as a real threat and disabling automatic image download as a viable recommendation on how to effectively protect against email tracking as a threat. When applying PMT, scholars should therefore include a *fear appeal* which is defined as a “*persuasive message designed to scare people by describing terrible things that will happen to them if they do not do what the message recommends*” (Witte 1992, p. 329). When including a fear appeal into PMT scholars use it to manipulate individuals. A fear appeal is usually divided into both “high” and “low” fear appeals (Boss et al. 2015; Milne et al. 2000).

Based on previous research (Boss et al. 2015), such a fear appeal does not only affect the fear concept, nor only some of the relationships of the entire model. Rather, a fear appeal serves as a central moderator of the entire model and a high fear appeal will lead to a better explanation of the entire model than a low fear appeal (McClendon and Prentice-Dunn 2001), in terms of higher explanatory power, more supported hypotheses and a better overall model fit (Boss et al. 2015). The fear appeal will lead individuals to consider email tracking as an actual threat and to consider disabling automatic image download an effective response. In line with previous research (Boss et al. 2015), we give several possible hypotheses why this is the case. For example, individuals experiencing a high fear appeal will be more salient to email tracking as a threat. Hence, they will be more likely to consider the severity of the threat resulting in a stronger relationship between threat severity and intention to disable automatic image download. Similarly, individuals experiencing a high fear appeal will also be given recommendations on how to protect against the threat. Hence, they will have a higher response efficacy, leading to a stronger relationship between response efficacy and protection intention. Furthermore, individuals who are experiencing a high fear appeal have knowledge about the threat and effective responses to mitigate the threat. If these individuals have the intention to protect against email tracking, they are more likely to actually do so because they know about the threat and the effective response. Therefore, in line with previous research we hypothesize:

H11: The research model better explains intention to disable automatic image download and behavior of disabling automatic image download for individuals who are in a high fear appeal context than for individuals who are in a low fear appeal context.

To summarize, our research model – based on PMT – consists of four processes. The threat appraisal process and the coping appraisal process lead to the intention to disable automatic image download. The third process is the behavior process, through which intention becomes actual behavior. To trigger the threat appraisal process and the coping appraisal process, a high fear appeal, the fourth process, is introduced to evaluate its impact on the effects of all relationships in the research model. The following

section describes the methodology we used to evaluate our research model.

5 METHODOLOGY

In this study, we aim to understand the influence of a fear appeal on protection intention and behavior in the context of email tracking, which represents a major threat to individual privacy (Brunet 2017; Merchant 2017; Xu et al. 2018). To evaluate our research model, we conducted a two-wave quantitative study illustrated in Figure 3 below²⁰.

5.1 TWO-WAVE QUANTITATIVE STUDY

Before the start of the study, we cleaned our pool of email addresses gathered from two different sources: First, participants in earlier anonymous scientific surveys had been asked after those earlier studies if they were interested in participating in future surveys and, if so, to provide their email address; Second, we asked participants in an annual survey about working conditions we conduct together with a project partner whether they wish to be invited by email to participate in any future studies. The individuals who provided their email addresses via these two channels comprise our participant pool. This is a valid methodology that has also been used in several articles in journals of the basket of eight (anonymous references).

Participants from both channels represent a population that varies in terms of age, gender, profession and education. Since email tracking affects all individuals independent of such demographics, we are better able to depict this population with our sample than if we had used a student sample. This variance makes our findings better generalizable.

In total, our pool included 1,639 potential survey participants. We cleaned this list by removing invalid and duplicate email addresses, leaving 1,615 email addresses. Every email address was assigned an individualized token to anonymize the responses, while being able to relate responses to that token. An overview of the study process is provided in Figure 3.

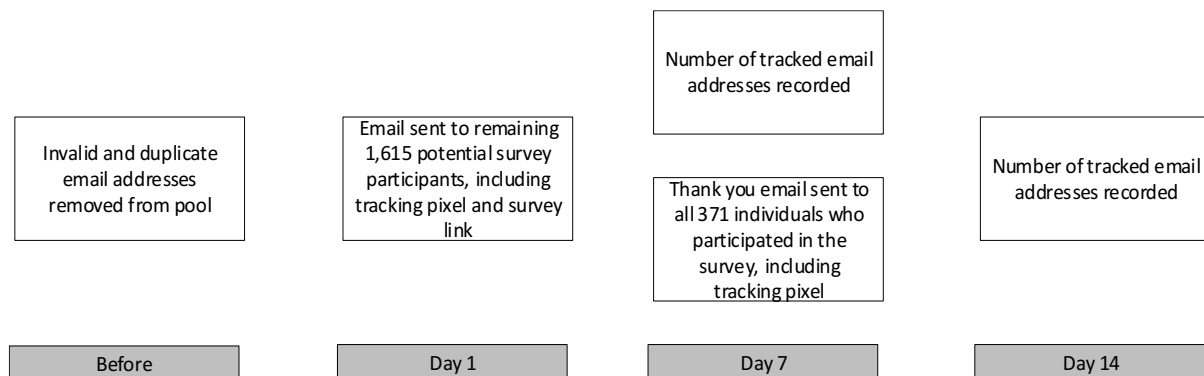


Figure 3. Study process

On day 1, we sent an email to the 1,615 individuals in our survey pool inviting them to take part in our survey. We incentivized participation by announcing that three participants drawn at random would win technical products. The link to the survey was associated with the participants' individual token and individuals were told they had seven days to participate in the survey. The email included a tracking pixel, so we would know if respondents are trackable. In compliance with the law, we informed recipients in the footer that the email contained a tracking element and included an opt-out link. Most emails with tracking pixels, such as newsletters or conversational emails, do not include this disclaimer,

²⁰ The entire study has been confirmed by the ethical board of our university.

and none of the participants used the link to opt out.

On day 7, we took a snapshot of survey participation and tracked email addresses. 371 out of the 1,615 individuals participated in our survey. A detailed procedure of the evaluation of the survey and the number of tracked email addresses is provided in the following sections. We also sent all 371 survey participants an email thanking them for taking part in the survey and again included a tracking pixel. This enabled us to measure actual privacy-related behavior.

On day 14, we took another snapshot of tracked email addresses to determine how many participants were still trackable.

To implement our survey, we used the software Limesurvey, which we hosted on our own server, and standardized items (see Table 3 in the appendix).

5.2 IMPLEMENTATION OF EMAIL TRACKING

In all emails sent out to the participants we included a 1x1 invisible tracking pixel in the email. We also included a logo of our department as well as the logo of our university to distract participants from our tracking pixel. When participants open their email with automatic image download enabled or manually downloaded images, we were able to track them using Google Analytics tracking functionality. We attached the following img-src to the source-code of the email:

```

```

TID: The ID one needs to use Google Analytics. This ID is set by Google and cannot be changed.

CID: The ID or individualized token assigned to each individual participant to track them.

This invisible tracking pixel enables various kinds of information to be collected (see section two): the IP address, the geo-location, whether and when the email was opened, the operating system, device and provider used to open the email. All this information would have been collected without the consent of the receiver of the email, i.e. the receiver would not know if and what kind of information is collected by the sender. However, to protect the privacy of the participants we only analyzed, if the email had been opened. All other information was not collected because it was irrelevant for this study. Thus, our study did not violate the privacy of the participants. However, we could have been violating it and the participants would not have known if and what kind of information we were collecting. Therefore, even though our study did not violate the privacy of the participants, it represents the real danger of such a violation. Actually collecting additional information from the participants would not have changed the results of this study since the participants would not have known what kind of information was collected.

This kind of email tracking enabled us to monitor whether a participant had filled out the survey and whether he or she has been tracked via email. Since we used individualized anonymous tokens, we do not know whose email address were tracked and which participants took part in the survey. This ensures absolute anonymous survey participation.

5.3 IMPLEMENTATION OF FEAR APPEAL

In line with previous research, when filling out the survey, we randomly assigned participants to either a high fear appeal or a low fear appeal context. To do so, we used the software Limesurvey to assign a hidden value 0 or 1 to every participant who took part in the survey. Based on that value, individuals were either assigned to a low fear appeal (value 0) or to a high fear appeal (value 1). Based

on this random assignment, individuals were directed either to a page filled with information with low fear appeal or to a page with high fear appeal (see section on fear appeals in the appendix). Afterwards, all participants were directed to the questions of the survey which were identical for all participants.

This is a quasi-experimental design with a between-subjects design. A within-subject design would have meant that participants need to fill out the survey twice – once with a low fear appeal and once with a high fear appeal. However, that would have distorted the results since the fear appeal and subsequent fear would have had an influence on the second survey. Therefore, in line with previous research (Boss et al. 2015) we decided to use a between-subjects design such that participants were either assigned to a low fear appeal or to a high fear appeal.

Of the 1,615 individuals to whom the link was sent, 371 responded to our survey. Of these participants, 196 participants were assigned to a low fear appeal and 175 participants were assigned to a high fear appeal, based on the random assignment of the value 0 or value 1 by the survey-software. A manipulation check was done afterwards to consider if high and low fear appeal actually led to low and high fear.

As discussed above, this study differentiates between low and high fear appeal to understand how fear appeals influence protection intention and behavior. By definition, a low fear appeal triggers individuals about a certain threat without evoking great fear of the threat or providing a viable solution to avoid the threat. In contrast, a high fear appeal is a “*persuasive message designed to scare people by describing terrible things that will happen to them if they do not do what the message recommends*” (Witte 1992, p. 329) and that provides a detailed way to cope with the threat. Briefly put, previous research shows that a low fear appeal frightens people a little and provides a rudimentary solution, whereas a high fear appeal scares individuals a lot and provides a detailed solution to the threat (Boss et al. 2015).

In our study, we informed participants exposed to a low fear appeal that tracking itself is common today. We mentioned email tracking and web tracking using cookies, pointing out that privacy can be threatened by email tracking, but did not discuss consequences. We also signalled that disabling automatic image download protects against email tracking, but did not provide any further instructions (see section on fear appeals in the appendix).

In contrast, we warned participants exposed to a high fear appeal that email tracking is a major threat to their privacy, detailing what information can be gathered through email tracking, including geolocation. We detailed the potential consequences of such loss of privacy, including price discrimination or being monitored by a burglar. We warned that 99 percent of newsletters and roughly every fifth conversational email contains a tracker, concluding that every survey participant has with almost absolute certainty been exposed to email tracking. Finally, we provided detailed information on how they can protect themselves against email tracking, including manuals about how to disable automatic image download for major email providers and email applications (see section on fear appeals in the appendix).

5.4 EVALUATION OF RESULTS

Of the 1,615 recipients of our email, 371 participated in our survey (see demographics in Table 1).

Age (M: 45.0 SD: 10.99 years)	<25	3.1	Sex	Female	65.8
	25-34	17.5		Male	34.2
	35-44	24.0	Main account*	Yes	79.4
	45-54	34.8		No	20.6
	>54	20.6			

* Participants use the email account the survey was sent to as their main account

Table 1. Demographics of 371 participants (in percent)

To evaluate the results, we use a partial least squares (PLS) approach for processes 1 – 3 (threat appraisal process, coping appraisal process and fear appeal process) by applying the software SmartPLS 3.2.6 (Hair et al. 2017). This approach is suitable for investigating privacy-related concepts where answers might skew the normal distribution (Turel et al. 2011). For process 4 (behavior process), we conduct a logistic regression. The reason is that the outcome variable – protection behavior – is binary and the input variable – protection motivation – is continuous, which makes logistic regression the correct tool to evaluate the data (Peng et al. 2002).

6 RESULTS

In this section, we 1) describe the results of our study, 2) discuss the degree to which fear, as our manipulation check, was triggered through our fear appeal, 3) discuss the potential of common method bias, 4) discuss our measurement model, 5) discuss our structural model, following a procedure recommended by Boss et al. (2015) and 6) discuss the results of the logistic regression. Common method bias and the measurement model is evaluated for all participants, while the structural model, including model fit, is calculated separately for the high and low fear appeal context.

6.1 DESCRIPTIVE RESULTS

We sent our invitation email to 1,615 individuals. We received 59 bounce responses because the mailbox was full, or the email address no longer exists. Of the remaining 1,556 email addresses, 797 were trackable – a ratio of 51.2 percent. None of the participants used the link provided in the footer to opt out of email tracking.

Of the 371 participants who took part in the survey, even 73.6 percent were trackable after the first survey. One reason for this could be that these participants also opened the e-mail to participate in the survey - unlike others who may not have opened the e-mail in the first place. A closer look at the results for the 371 participants reveals that there are differences depending on which e-mail provider the participants use. Based on the participants' e-mail addresses, the five largest e-mail providers are, in descending order: Gmail, gmx, web, t-online and yahoo. Differences become apparent e.g. between Gmail and web. While 92.4 percent of the participants who have their email address on Gmail were trackable, it is merely 62.0 percent for participants who use GMX. After sending the second e-mail, it becomes apparent that the number of trackable participants has decreased for all providers. But even here differences can still be seen. For example, the share of GMail users is now 73.4 percent, but that of users of GMX only 40.5 percent. One reason for this different tracking behavior could be that the participants have different technical knowledge. We therefore evaluated the self-efficacy, i.e. the ability to protect against email tracking, among the participants of the five providers. Here, however, no significant differences can be seen across the individual groups ($p\text{-value} > 0.05$). Another way to describe the data is how many participants have reported to disable automatic image download but were still trackable. In the first survey, 153 out of 371 participants reported having disabled the automatic image-download for the email address the invitation email was sent to. Of these 153 email addresses, however, 101 participants (66.0 percent) were trackable, which means that they either manually downloaded our tracking pixel or automatic download was still enabled.

The second email was sent to all 371 survey participants. Among participants who received a low

fear appeal, 70.21 percent were still trackable, representing a 29.81 percent decrease. Among participants who received a high fear appeal, 76.52 percent were still trackable, representing a 23.48 percent decrease. It is surprising that a greater percentage of participants exposed to a low fear appeal prevented tracking than the percentage of participants exposed to a high fear appeal, but a t-test (p-value of 0.240) indicates that the difference is statistically insignificant.

6.2 MANIPULATION CHECK

Fear, which is part of our research model, is used as a manipulation check. Our assumption was that the low and high fear appeals would cause different levels of fear (Boss et al. 2015). The mean value of fear among participants assigned to a low fear appeal was 3.089, the mean value of fear among participants assigned to a high fear appeal was 3.532. With these values, we are on par with other studies, which also included a fear appeal in their study (Boss et al. 2015). This leads us to the conclusion that individuals' level of fear is strong enough to consider protecting against the threat causing that fear. A t-test (p-value of 0.002) indicates that this difference is significant and, therefore, that the manipulation of fear via fear appeal worked.

6.3 COMMON METHOD BIAS

By checking for common method bias, we can evaluate to what degree our results are distorted (Schwarz et al. 2017). We used the Harman's Single-Factor Test, which shows that 24.9 percent of variance is explained by one factor, which is below the threshold of 50.0 percent. The unmeasured latent method construct explains a delta of R^2 of 0.002. As the average R^2 without the CMB is 0.773, we have a ratio of 1:372 (Chin et al. 2012). These tests therefore show no indication of common method bias in our data (Liang et al. 2007).

6.4 MEASUREMENT MODEL

To evaluate the measurement model when using reflective indicators as in our study, one needs to account for indicator reliability, construct reliability and discriminant validity.

	Mean (Low)	SD (Low)	Mean (High)	SD (High)	Mean (All)	SD (All)	AVE	CR	1	2	3	4	5	6	7	8
1 Perceived threat vulnerability	4.545	1.480	4.871	1.397	4.621	1.447	0.831	0.937	0.912							
2 Perceived threat severity	5.478	1.537	5.564	1.353	5.534	1.433	0.778	0.913	0.200	0.822						
3 Fear	3.089	1.481	3.532	1.455	3.368	1.549	0.811	0.928	0.481	0.240	0.901					
4 Maladaptive rewards	3.217	1.736	2.968	1.647	3.081	1.699	0.693	0.871	0.258	-0.048	0.305	0.832				
5 Response efficacy	4.743	1.268	5.092	1.373	4.928	1.335	0.837	0.939	0.054	0.182	0.145	0.006	0.915			
6 Self-efficacy	5.038	1.833	4.956	1.863	5.072	1.802	0.933	0.977	0.157	0.296	0.145	0.084	0.142	0.966		
7 Response costs	2.704	1.452	2.610	1.468	2.655	1.474	0.874	0.954	0.144	-0.015	0.317	0.52	-0.12	-0.01	0.935	
8 Intention	4.856	1.843	5.112	1.681	5.003	1.778	0.927	0.974	0.071	0.313	0.215	-0.208	0.252	0.228	-0.185	0.963

Table 2. AVE, CR and bivariate correlations

To evaluate indicator reliability, each indicator should explain more than 50 percent of the variance of the latent variable. Therefore, each value needs to be at least 0.707 (Carmines and Zeller 2008) which is the case in our study (see Table 3 in the appendix). Each loading is also significant with $p < 0.001$. To account for construct reliability, the average variance extracted (AVE) should be greater than 0.5 and the composite reliability (CR) should be greater than 0.7 (Fornell and Larcker 1981). Both conditions are fulfilled, as illustrated in Table 2. Discriminant validity, a measure of whether constructs differ from

each other, is true if the square root of the AVE is greater than the correlation of the constructs with each other (Fornell and Larcker 1981; Hulland 1999). This is also the case in our study (see Table 2). Additionally, we also computed the heterotrait-monotrait ratio (HTMT) (Henseler et al. 2014). When using the most conservative approach $HTMT_{0.85}$ we do not observe any lack of discriminant validity, since the highest correlation is between response costs and maladaptive rewards with 0.634. As all requirements have been fulfilled, we can state that our measurement model is valid.

6.5 STRUCTURAL MODEL

Following Boss et al. (2015), we assessed our results based on high fear appeal vs. low fear appeal to evaluate our structural model. In terms of the overall model fit (Henseler et al. 2016), the test of the saturated model shows that standardized root mean square (SRMR) residual is 0.059 for the high fear appeal and 0.061 for the low fear appeal. Since SRMR should be below 0.08 (Hu and Bentler 1999), we can conclude the overall model fit is given for both contexts, with slightly better results for the high fear appeal model.

As depicted in Figure 4, several of the hypotheses are not supported for the participants of the low fear appeal. On the other hand, more hypotheses are supported for the high fear appeal context. Furthermore, the R^2 of the intention to disable automatic download for the low fear appeal accounts to 22.0 percent and to 34.8 percent for the high fear appeal. For the behavior process including the control variable, the results are displayed separately in the logistic regression model. Overall, in a high fear appeal context, the overall model fit is better and more hypotheses are supported. Also, R^2 of the protection intention is higher in a high fear appeal context.

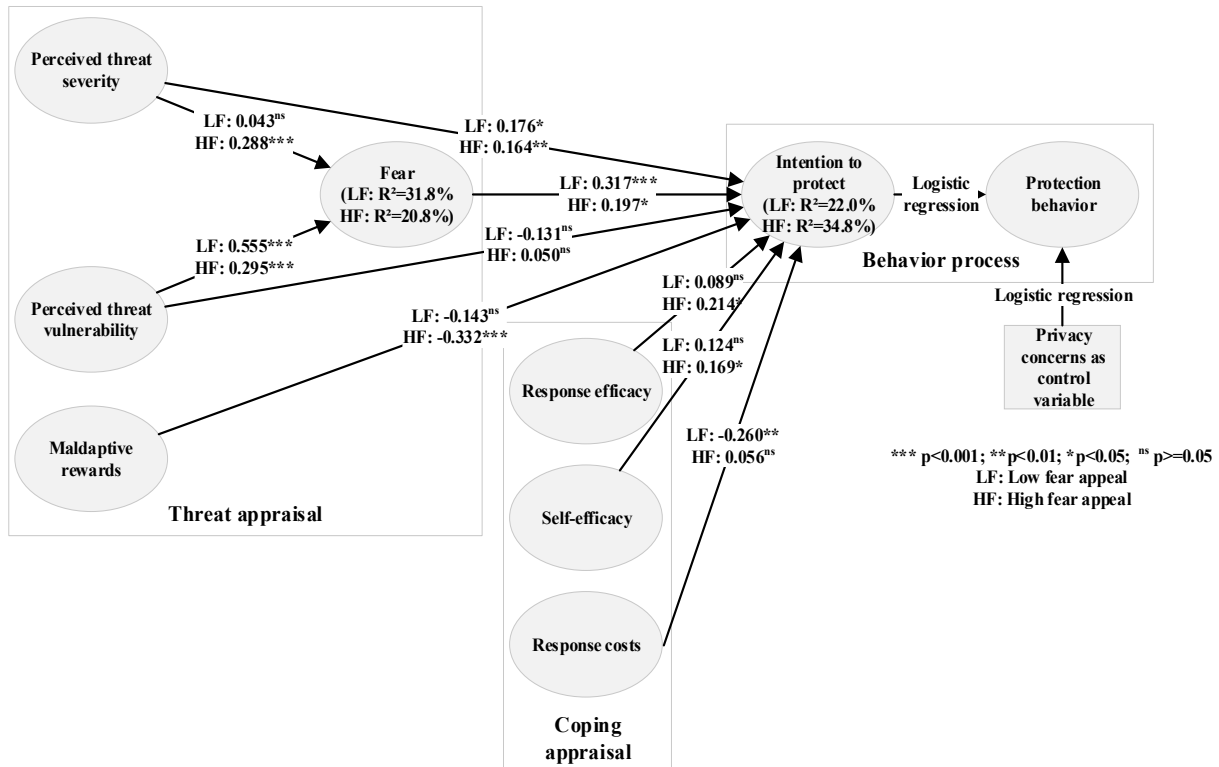


Figure 4. Structural Model

Four out of ten hypotheses (H1, H4, H5, H9 and H10) are supported for the low fear appeal and seven out of ten hypotheses (H1, H3, H4, H5, H6, H7 and H8) are supported for the high fear appeal. Thus, H9 and H10 are only supported for the low fear appeal context and H3, H6, H7 and H8 are only supported for the high fear appeal context. Only H2 is not supported in either fear appeal context. In the

following, we will first consider the logistic regression to investigate H10. Afterwards, we will conduct two post-hoc analyzes to better understand the effects concerning H10 as well as of H2.

6.6 LOGISTIC REGRESSION TO EVALUATE THE BEHAVIOR PROCESS

To evaluate hypothesis H10, i.e. the effect of the intention to disable automatic image download on the actual behavior to do so, we conducted logistic regression. The reason is that for binary variables, PLS is possible but not recommended because of its nearity, normality and continuity (Peng et al. 2002). What is more recommended in such a setting is logistic regression. This calculation method makes it possible to find out in how far there is an effect of one or more continuous income variables on a binary outcome variable (Peng et al. 2002). In more detail, the logistic regression makes it possible to calculate odds ratios. Such an odds ratio displays a value which states if the input variable increases by one unit, what is then the probability that the outcome variable will change from 0 to 1.

In this study the behavior to disable automatic image download is a binary variable and the input variable, the intention to disable automatic image download, is continuous. To conduct logistic regression in this research study, we used the latent variable scores from the software SmartPLS for the continuous income variable. The outcome variable was set to 0 (not protecting against e-mail tracking by not disabling automatic image download) and 1 (protecting against e-mail tracking by disabling automatic image download). The odds ratios therefore tell us: If the intention to disable automatic image download is increased by one unit, in how far increases or decreases the probability that the individual will now also protect against automatic image download in comparison to not protecting against it.

Following the study of Boss et al. (2015), this relationship is tested for the low fear appeal context as well as for the high fear appeal context. We use SPSS version 25 to calculate the logistic regression model. Based on Peng et al. (2002), four criteria should be presented to on the one hand make sure, that the results are valid and on the other hand to also present the actual results. We follow these recommendations and first present these criteria of the low fear appeal context, followed by the high fear appeal context.

6.6.1.1 Low fear appeal context

The overall model evaluation in the low fear appeal context shows that the model is valid. The chi-square is 17.680 and is significant ($p\text{-value} < 0.001$). Therefore, the overall model is valid. The statistical tests of the individual predictors are evaluated by the wald-chi-square test and the corresponding significance. The wald-value is 15.178 and the value is also significant ($p\text{-value} < 0.001$). Therefore, the individual predictor which is intention to disable automatic image download is significant. Furthermore, the goodness-of-fit statistics show that Nagelkerkes R^2 is 0.163 which indicates a high goodness-of-fit. To find out if the odd-ratios are significant, the confidence-interval must not cut 1. This is the case since the confidence intervals' lower value is 1.472 and the upper value is 3.220. We therefore conclude that the overall logistic regression model in the low fear appeal context is valid and the results are significant.

The actual results show that $\text{Exp}(B)$ is 2.177. That means that the probability that an individual is protecting against e-mail tracking when the intention to do so is increased by one unit, is more than twice as high or, in other words, is increased by 117,7 percent.

6.6.1.2 High fear appeal context

For the high fear appeal context, the same calculations need to be conducted. However, the results show that the overall logistic model is neither valid nor are the results significant. The chi-square is 2.093 and is non-significant ($p\text{-value}$ is 0.148). Also, the wald-value is 2.021 and not significant ($p\text{-value}$ is 0.155). Furthermore, the Nagelkerkes R^2 is 0.023 and therefore low, indicating no goodness-of-fit statistic. In addition, the odd-ratio is not significant since the confidence interval cuts 1: the lower value

is 0.901 and the upper value is 1.920. We therefore conclude that there is no significant effect of the intention to disable automatic image download on the corresponding behavior in a high fear appeal context.

6.7 POST-HOC ANALYSIS FOR HYPOTHESIS H10

To better understand the surprising non-significant effect of intention on behavior in a high fear appeal context, we conducted three additional tests.

First, we removed the intention to disable automatic image download from the model and evaluated, in how far all remaining concepts have an effect on the behavior. The reason is that obviously the results have shown that the intention to disable automatic image download has no effect on its behavior in a high fear appeal context. It is therefore standing to reason that intention may be the wrong predictor of behavior and instead, beliefs directly influence the behavior. This is also grounded in sources on the intention-behavior gap, showing that intention often does not result in the corresponding behavior and that intention often is a weak predictor of behavior and instead, other concepts become more important (Bhattacharjee and Sanford 2009). However, the results again show no significant effects. The overall logistic model is not valid (chi-square is 11.7; p-value is 0.111), which makes it useless to display any further calculations.

Second, we examined in how far solely fear might have an effect on protection behavior. The reason is that especially in a high fear appeal context, it might be that individuals do not rely their intentions anymore but rather base the behavior on emotions (Mohiyeddini et al. 2009). However, again, the results show no significant effects. The overall model again is not valid (chi-square is 0.449 and p-value is 0.503).

Third, we account for the effect of privacy concerns as a control variable (Smith et al. 2011). The reason is, as already stated before that privacy concerns is the central variable in privacy research (Smith et al. 2011) and therefore the effect should be evaluated. However, again the results show no significant effects. The overall model is not valid (chi-square is 0.114 and the p-value is 0.735).

All in all, the post-hoc analysis provides deeper insight into the relationships of possible antecedents of the behavior of disabling automatic image download. However, none of the postulated antecedents has a significant effect on the behavior of disabling automatic image download.

6.8 POST-HOC ANALYSIS FOR HYPOTHESIS H2

Since H2, i.e. the effect of perceived threat vulnerability on intention to disable automatic image download, is insignificant for the low and high fear appeal context, we conducted a post-hoc mediation analysis following the guidelines of Hair et al. (2017). Here, we first checked on the product of the indirect effects, which is significant for both fear appeal contexts (low: p-value<0.001; high: p-value<0.001). We then continued and checked on the 95 percent confidence interval which must not cut 0. For the low fear appeal the confidence interval is between 0.447 and 0.634; for the high fear appeal the confidence interval is between 0.161 and 0.428. Hence, that condition is fulfilled as well. As the direct effect of perceived threat vulnerability on intention to disable automatic image download is insignificant there is an indirect-only mediation. This means that our results indicate that the effect of perceived threat vulnerability on protection motivation is fully mediated by fear for both levels of fear appeal.

All these results are now discussed in the following.

7 DISCUSSION

Nearly all newsletters and roughly every fifth conversational email use email tracking (Brunet 2017; Merchant 2017). Email tracking violates individual privacy and can result in further disadvantages such as burglars using email tracking to find out when potential targets are not at home. Despite these dangers, it is indicated that most people do not protect themselves against email tracking (Xu et al. 2018). This study aims to shed light on what influences individual email tracking protection behavior. We apply the protection motivation theory (PMT) and use the full nomology of PMT as called for in previous research (Boss et al. 2015). Our results contribute to 1) the context of email tracking by identifying drivers of individual email tracking protection intention and behavior and 2) PMT in the domain of privacy by identifying considerations relevant to using PMT in privacy research:

7.1 CONTRIBUTIONS TO THEORY

7.1.1.1 Email tracking:

Our results help us better understand what motivates individuals to protect themselves against email tracking and provides insights into the protection behavior of individuals. We contribute to email tracking scholarship (Bender et al. 2016; Englehardt et al. 2018; Fabian et al. 2015; Xu et al. 2018) by showing that fear appeal is a central component to understand the intention of individuals to protect themselves against email tracking (Boss et al. 2015). This has the following implications:

Maladaptive rewards become important in a high fear appeal context: In a high fear appeal context, maladaptive rewards have a strong negative effect on protection motivation. This contextualizes PMT to the context of email tracking (Hong et al. 2014). If scholars want to find ways to motivate individuals to protect themselves against email tracking (Bender et al. 2016), then decreasing maladaptive rewards may be key.

Response costs are less important in a high fear appeal context: The effect of response costs is stronger for individuals exposed to a low fear appeal than to individuals exposed to a high fear appeal. That means that if individuals are less frightened about email tracking, response costs influence their protection intention more than for individuals who are more frightened, for whom the negative effect of response costs diminishes. An explanation could be that individuals who are exposed to a high fear appeal perceive lower response costs (see Table 2) (Xu et al. 2018). It is possible that individuals experiencing fear think less about the cost of response and are more focused on their main goal to protect themselves against email tracking. Scholars who want to better understand the effect of response costs on protection intention against email tracking need to check on the fear appeal. If participants have been exposed to a high fear appeal, then our results implicate that PMT can be used in a contextualized version (Hong et al. 2014) omitting response costs.

Fear appeal promotes email tracking protection behavior: Our results show that, overall, 26.98 percent fewer participants were trackable after completing our survey. Although there is no significant difference between the decrease among individuals exposed to a low (29.81 percent) or high (23.48 percent) fear appeal, the overall results support the notion that the fear appeal context significantly influences email tracking protection behavior. However, in both the high and low fear appeal context, actual behavior still remained largely unexplained. To better understand actual behavior in the context of email tracking, future studies must focus on antecedents other than protection intention.

7.1.1.2 Protection motivation theory in the domain of privacy:

So far, we have provided contextualized theory development by showing how PMT needs to be considered differently in the context of email tracking (Hong et al. 2014). However, with our results, we also contribute to the general research stream on privacy:

The research model better explains protection intention in a high fear appeal context: Previous research has called to integrate fear appeal into future research studies (Boss et al. 2015). After several studies in the privacy-related field applied PMT and often reported non-significant hypotheses for several relationships (e.g. Marett et al. 2011; Mohamed and Ahmad 2012), this is the first study to include a fear appeal to report more significant hypotheses and to better explain non-significant hypotheses in the privacy domain. Our results show the research model is better in explaining protection intention when a high fear appeal is included, partially supporting hypothesis H11 (Boss et al. 2015). This is supported by the higher R^2 for protection intention, the higher number of supported hypotheses as well as the better model fit. We therefore recommend that future research applying PMT in the privacy-related field include a high fear appeal or at least explain their rationale for using a low or no fear appeal.

All concepts of the threat and coping appraisal process should initially be included when applying PMT: Our results indicate that all concepts of the threat appraisal as well as the coping appraisal processes should be considered when applying PMT in a privacy-related study. In particular, our results show that the effect of threat vulnerability on the protection intention is mediated by fear, an effect ignored by studies not considering fear (e.g. Chen et al. 2016; Marett et al. 2011; Mousavizadeh and Kim 2015). Also, we have shown that concepts such as maladaptive rewards, response efficacy and self-efficacy have a major impact on protection intention depending on fear appeal. Again, previous studies have also left out some of these concepts (e.g. Chen et al. 2016; Mousavizadeh and Kim 2015), potentially weakening the losing explanatory power of their research model.

We have no evidence that these concepts will have the same effect on protection intention as in our research study, given the email tracking context. However, by considering all concepts, more light can be shed on contexts in which a particular concept is insignificant or whose significance depends on whether a fear appeal is low or high. As Boss et al. (2015) suggested for the security domain, to alter PMT for a given context, the full nomology should be used initially before alterations are suggested. We underscore this advice for the privacy domain, which is related to but distinct from security (Dincelli et al. 2017).

Fear appeal helps explain the intention-behavior gap: The intention-behavior gap has been discussed in technology adoption research (Bhattacharjee and Sanford 2009) as well as in general privacy research (Smith et al. 2011). Our results indicate that in a low fear appeal context, intention significantly influences behavior, whereas in a high fear appeal context, intention is a weak predictor of behavior. Our results therefore *first* support the notion that intention is not equal to behavior. *Second*, our results indicate that there is a difference between individuals being exposed to a high and low fear appeal. Among individuals with high levels of fear caused by a high fear appeal, intention has a weak or no effect on behavior. Rather, other concepts are more important. Considering the logical sequence of intention \rightarrow behavior as something rational, then it might be that these individuals who are frightened are behaving less rationally and more based on fear or other emotions (Mohiyeddini et al. 2009). Hence, we call for researchers to consider other emotions besides fear as possible antecedents of protection behavior (Smith et al. 2011). *Third*, our results indicate the level of fear appeal does not influence the percentage of individuals respond to a fear appeal by protecting themselves against email tracking. Although our manipulation check “fear” finds that our fear appeal resulted in perceived fear, email tracking protection behavior did not differ significantly among individuals exposed to a high fear appeal vs. those exposed to a low fear appeal context. One explanation may be individual difference in terms of response to fear and the link to behavior change, as suggested by previous research (Boss et al. 2015). This may have implications on naming terms and on obtrusiveness in studies involving fear. To better understand PMT, scholars should consider including and comparing findings for a no-fear appeal setting as a third group to better understand the effect of the fear appeal.

7.2 CONTRIBUTIONS TO PRACTICE

With our results we contribute to practice in several ways. *First*, this is the first study to statistically demonstrate how vulnerable email users are to potential privacy loss through email tracking. More than half (51.1 percent) of all 1,555 participants of our study were trackable. We call for governments and email and software providers to help individuals protect their privacy by avoiding email tracking. *Second*, our results indicate that frightening people and giving them easily executable advice on how to protect themselves against email tracking leads to real email tracking protection behavior. *Third*, among participants who say they have disabled automatic image download, about two-third were still trackable. Discounting individuals who manually downloaded the images sent in the second email, it is very likely that individuals overestimate their ability to take the necessary steps to disable automatic image download. Hence, every fear appeal must include clear and complete instructions on how to protect oneself against email tracking.

7.3 LIMITATIONS

Our study is subject to several limitations. 1) There is a risk that participants trust our university and manually allow downloaded images for our email but deny it for other emails. This would distort actual behavior because we asked participants whether they disabled automatic image download. However, given the significant difference in actual behavior after the second email, we do not think that the trust factor distorted our results significantly. 2) Our study was conducted in the context of email tracking in the domain of privacy. Hence, the first part of our contributions is only applicable to the context of email tracking and the second part is only applicable to general privacy research studies. 3) In measuring the actual behavior of participants and whether they are trackable via email, we assumed that not being tracked implies that individuals acted to protect themselves against email tracking. It is possible that our email was deleted unopened or that the email was opened on a client which protects against email tracking but was not opened on a different client which is not protected against email tracking. It could also be that individuals do not protect intentionally against e-mail tracking, however, their provider blocks images in their e-mails by default. These technical limitations might be a potential avenue for future research, by conducting a controlled experiment, where this limitation is overridden. 4) Since this study was not a controlled environment, we cannot know whether participants consulted other sources of information (e.g., friends, IT department or online sources) after reading the fear appeal text and taking the survey. This might weaken the link between the level of fear appeal and explanation of the research model. We do not think that this issue mainly distorts our results since the taken approach is very similar to other already conducted studies. Still, one could overcome this limitation by asking individuals in the survey if they have consulted other sources of information after having read the fear appeal text.

8 CONCLUSION

In this study, we investigate the role of fear appeal in an email tracking context. We applied the full nomology of PMT to investigate what drives individual protection intention and behavior. According to our results, a high fear appeal better explains the research model than a low fear appeal since more hypotheses are supported, the R^2 of the protection intention is higher and the overall model fit is better. With this, this study contributes theoretically, showing that a fear appeal in general is needed and that all core concepts of PMT should be considered when applying PMT in privacy research. This study also has practical contributions for government policy makers and email service providers since this study is among the first ones to show that a majority of individuals does not protect against email tracking.

9 APPENDIX

9.1 ITEMS

Construct	Items	Loading	Author(s)
Perceived threat severity	If emails I receive were tracked, it would be severe.	0.920	Johnston and Warkentin 2010
	If emails I receive were tracked, it would be serious.	0.872	
	If emails I receive were tracked, it would be a real problem for me.	0.852	
Perceived threat vulnerability	E-mails I receive are at risk to be tracked.	0.890	Johnston and Warkentin 2010
	It is likely that emails I receive are tracked.	0.948	
	It is possible that emails I receive are tracked.	0.896	
Fear	My email account has a serious email tracking problem.	0.883	Osman et al. 1994
	My emails might be seriously getting tracked.	0.904	
	The amount of my emails getting tracked is terrifying.	0.915	
Maladaptive rewards	Not disabling the automatic image download on my email account saves me time.	0.843	Boss et al. 2015; Myyry et al. 2017
	Not disabling the automatic image download on my email account saves me money.	0.751	
	Not disabling the automatic image download on my email account keeps me from being confused.	0.898	
Response efficacy	Disabling image download on my email account is effective to protect against email tracking.	0.891	Johnston and Warkentin 2010
	When disabling image download on my email account, my emails are more likely to be protected against email tracking.	0.929	
	Disabling image download on my email account is sensible to protect against email tracking.	0.924	
Self-efficacy	I was able to disable automatic image download on my email account, ...	-	Compeau and Higgins 1995
	... if I could call someone for help if I got stuck.	0.952	
	... if someone else helped me get started.	0.975	
	... if someone showed me how to do it first.	0.970	
Response costs	I would be discouraged from disabling automatic image download because it would take too much time.	0.949	Milne et al. 2002
	Taking the time to disable automatic image download would cause me too many problems.	0.925	
	I would be discouraged from disabling automatic image download because I would feel silly to do so.	0.929	
Privacy Concerns	I am concerned that the information I submit on the Internet could be misused	0.883	Dinev and Hart 2006
	I am concerned that a person can find private information about me on the Internet.	0.888	
	I am concerned about submitting information on the Internet, because of what others might do with it.	0.720	
Intention*	My intentions to disable automatic image download on my email account are high.	0.950	Johnston and Warkentin 2010; Posey et al. 2015
	It is likely that I will disable automatic image download on my email account.	0.975	
	I intend to expend effort to disable automatic image download on my email account.	0.964	
Behavior**	Behavior was measured by sending an email including a tracking pixel to participants. See section on methodology for more details.	-	-
Fear appeal	We gave participants two different texts to read such that they were exposed to a high or low fear appeal context. Participants were assigned to either a high or low fear appeal based on a random basis. See section on methodology and the appendix for more details.	-	-
*Intention: Intention to disable automatic image download **Behavior: Behavior of disabling automatic image download Items were measured on a 7-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree)			

Table 3. Items and Loadings

9.2 CROSS LOADINGS

	Fear	Maladaptive rewards	Intention	Perceived threat severity	Perceived threat vulnerability	Response costs	Response efficacy	Self-efficacy
Fear1	0,883	0,306	0,188	0,298	0,426	0,371	0,112	0,079
Fear2	0,904	0,293	0,154	0,116	0,437	0,249	0,115	0,127
Fear3	0,915	0,228	0,235	0,224	0,438	0,233	0,162	0,146
Maladaptive rewards1	0,202	0,843	-0,178	-0,081	0,264	0,383	0,05	0,036
Maladaptive rewards2	0,3	0,751	-0,111	0,001	0,185	0,539	-0,071	0,077
Maladaptive rewards3	0,283	0,898	-0,21	-0,028	0,197	0,436	0,008	0,098
Intention1	0,181	-0,224	0,95	0,296	0,072	-0,206	0,207	0,189
Intention2	0,207	-0,208	0,975	0,313	0,067	-0,183	0,274	0,22
Intention3	0,233	-0,171	0,964	0,294	0,067	-0,147	0,244	0,247
Perceived threat severity1	0,17	-0,086	0,284	0,92	0,144	-0,058	0,173	0,212
Perceived threat severity2	0,169	-0,098	0,298	0,872	0,171	-0,071	0,171	0,359
Perceived threat severity3	0,288	0,048	0,247	0,852	0,209	0,079	0,14	0,213
Perceived threat vulnerability1	0,422	0,264	0,077	0,233	0,89	0,165	0,086	0,138
Perceived threat vulnerability2	0,49	0,244	0,05	0,171	0,948	0,144	0,014	0,141
Perceived threat vulnerability3	0,398	0,196	0,071	0,143	0,896	0,081	0,053	0,153
Response costs1	0,301	0,535	-0,185	0	0,163	0,949	-0,068	0,014
Response costs2	0,336	0,48	-0,128	0,013	0,133	0,925	-0,138	0,011
Response costs3	0,266	0,445	-0,192	-0,046	0,109	0,929	-0,139	-0,044
Response efficacy1	0,088	0,066	0,202	0,155	0,034	-0,103	0,891	0,114
Response efficacy2	0,161	0,024	0,216	0,145	0,058	-0,058	0,929	0,157
Response efficacy3	0,143	-0,055	0,265	0,193	0,054	-0,159	0,924	0,121
Self-efficacy1	0,152	0,062	0,241	0,272	0,134	-0,034	0,135	0,952
Self-efficacy2	0,112	0,091	0,21	0,287	0,156	-0,001	0,127	0,975
Self-efficacy3	0,11	0,094	0,204	0,301	0,169	0,011	0,15	0,97

Table 4. Cross loadings

9.3 LITERATURE REVIEW

Concepts used from PMT	Concepts missing	Added constructs after having evaluated PMT	Added constructs without evaluating PMT	Process #1	Process #2	Process #3	Process #4	Context of research study	Author(s)
Maladaptive rewards Perceived severity Perceived vulnerability Response efficacy Self-efficacy Perceived threat/vulnerability	Fear Fear appeal Protection behavior Response costs	-	Information privacy concerns	x	Partly	-	-	Social networking sites	Adhikari and Panda 2018
-	Fear Fear appeal Maladaptive rewards Response costs Perceived threat severity Protection behavior	-	Awareness of Big data applications Perceived threat severity Self-disclosure accuracy Trust	Partly	Partly	-	-	Social networking sites	Alashoor et al. 2017
-	Fear Fear appeal Maladaptive rewards Protection behavior Perceived threat severity Response costs Self-efficacy	-	Information stolen Relational conflicts Online privacy concerns Awareness of Online Information Disclosure	-	-	-	-	General context	Chen et al. 2016
Perceived threat severity Perceived threat/vulnerability	Fear Fear appeal Maladaptive rewards Protection behavior Response costs Self-efficacy	-	Herding behavior Social influence	Partly	x	-	-	Identity protection services	Kim 2016
Maladaptive rewards (as intrinsic and extrinsic rewards) Response costs Response efficacy Self-efficacy Perceived threat severity Self-efficacy Perceived threat/vulnerability	Fear Fear appeal Maladaptive rewards Protection behavior Response costs Self-efficacy Fear appeal (only as manipulation check) Fear appeal (only high fear appeal and no low fear appeal) Protection behavior	-	-	x	Partly	-	Partly	Social networking sites	Marett et al. 2011
Response costs Response efficacy Self-efficacy Perceived threat/vulnerability	Fear Fear appeal Maladaptive rewards Protection behavior Response costs Self-efficacy Perceived threat severity	-	Privacy statement Privacy customization Assurance mechanisms	Partly	Partly	-	-	Social networking sites	Mousavizadeh and Kim 2015
-	Fear Fear appeal Maladaptive rewards Protection behavior Perceived threat severity	-	Perceived invasion	Partly	Partly	-	-	Biometric security	Najati and Karimi 2013
Fear Perceived threat severity Perceived threat/vulnerability Response efficacy Self-efficacy	Fear Fear appeal Maladaptive rewards Protection intention Protection behavior Response costs Self-efficacy	-	Mobile banking Internet privacy concerns Interaction management Information management Trusting beliefs	Partly	Partly	-	-	Mobile Banking	Terlizzi et al. 2019
Response efficacy Self-efficacy Perceived threat severity Perceived threat/vulnerability	Fear Fear appeal Maladaptive rewards Protection behavior Response costs Self-efficacy	-	Social needs Information needs Entertainment needs	Partly	Partly	-	-	Social networking sites	Vishwanath et al. 2018
Maladaptive rewards Perceived threat severity Perceived threat/vulnerability	Fear Fear appeal Maladaptive rewards Protection behavior Response costs Self-efficacy	-	-	Partly	-	x	-	General websites	Youn 2005
Privacy self-efficacy Perceived threat/vulnerability Maladaptive rewards	Fear Fear appeal Maladaptive rewards Protection behavior Response costs Response efficacy Self-efficacy	-	Gender Use Persuasion knowledge Privacy knowledge Level of Online Privacy Concerns	Partly	Partly	-	-	General websites	Youn 2009
Fear Fear appeal Maladaptive rewards Protection behavior Perceived threat severity Perceived threat/vulnerability Response costs Response efficacy Self-efficacy	-	-	-	x	x	x	x	Email Tracking	This research

Table 5. Literature review on the protection motivation theory in the domain of privacy

9.4 FEAR APPEALS

9.4.1.1 High fear appeal:

Please read the following information carefully. The subsequent statements to be evaluated also refer to this text. Thank you very much.

Through e-mail tracking you pay more when shopping online!

Email tracking is a relatively unknown, but no less dangerous way to undermine the privacy of users. 99 percent of all sent newsletters and even almost 20 percent of all "normal" e-mails are tracked. Tracking means that the sender of an e-mail can find out a lot of data about the recipient of an e-mail. For example, whether and when he opened the e-mail, whether he forwarded the e-mail, where he was at the time the e-mail was opened, and much more. The recipient is not aware of this and does not have to give any consent at all. The tracking therefore runs unnoticed. Such tracking undermines the privacy of the recipient. As shown in the headline, merchants, for example, use e-mail tracking to categorize their customers and thus offer different prices for their products. Employers can use email tracking to monitor their employees at home. Burglars can use email tracking to check if someone is at home and better plan their break-in.

Technically, the sender of the e-mail inserts a tracking element - usually in the form of an invisible image. As soon as the recipient opens the e-mail and downloads the image, he transmits further information to the sender, who can evaluate it. At the moment, there is only one really effective protective measure: deactivate the automatic download of images in e-mails. This ensures that no more images are downloaded in emails and that all tracking elements are blocked.

Often the automatic download of images is already activated. However, users can disable this in the settings of their e-mail account or e-mail program. Instructions for the most common programs and e-mail accounts are linked here.

Browser-Access:

GoogleMail (Google states that they limit the tracking of e-mail. However, it is only fully restricted when downloading of images is deactivated).

GMX

Web.de

Access via Smartphone:

Android / Gmail

iOs (Apple iPhone or iPad)

MacOS (Mountain Lion)

Access via software on a computer:

Outlook 2016/2013/2010/2007

Thunderbird

9.4.1.2 Low fear appeal:

Please read the following information carefully. The subsequent statements to be evaluated also refer

to this text. Thank you very much.

Being online also means putting your privacy at risk. For example, by entering your data on social networks, banking transactions online or sending e-mails. Even just surfing the Internet can lead to privacy restrictions. Regarding this, on the one hand, for example, users disclose information about themselves to others via so-called web tracking, for example via cookies or tracking elements on websites. Users can protect themselves against this, for example by installing appropriate software. On the other hand, the behavior of users is often tracked by receiving e-mails. Email recipients can protect themselves by disabling the automatic download of images in emails, which also disables possible tracking elements.

10 REFERENCES

- Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), pp. 509–514.
- Adhikari, K., and Panda, R. K. 2018. "Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks," *Journal of Global Marketing* (31:2), pp. 96–110.
- Alashoor, T., Han, S., and Joseph, R. 2017. "Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Social Networking Websites: An APCO Model," *Communications of the Association for Information Systems* (41:1), pp. 62–96.
- Bender, B., Fabian, B., Lessman, S., and Haupt, J. 2016. "E-Mail Tracking: Status Quo and Novel Countermeasures," in *Proceedings of the 37th International Conference on Information Systems*, B. Fitzgerald and J. Mooney (eds.), Dublin, Ireland.
- Bhattacharjee, A., and Sanford, C. 2009. "The intention–behaviour gap in technology usage: the moderating role of attitude strength," *Behaviour & Information Technology* (28:4), pp. 389–401.
- Bonfrer, A., and Drèze, X. 2009. "Real-Time Evaluation of E-mail Campaign Performance," *Marketing Science* (28:2), pp. 251–263.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864.
- Brunet, N. 2017. *OMC Releases State of Email Tracking Report*.
<http://www.prweb.com/releases/2017/06/prweb14427071.htm>. Accessed 6 September 2017.
- Carmines, E. G., and Zeller, R. A. 2008. *Reliability and validity assessment*, Newbury Park, California: Sage Publications.
- Chen, H., Beaudoin, C. E., and Hong, T. 2016. "Protecting Oneself Online," *Journalism & Mass Communication Quarterly* (93:2), pp. 409–429.
- Chin, W. W., Thatcher, J. B., and Wright, R. T. 2012. "Assessing common method bias: Problems with the ULMC technique," *MIS Quarterly* (36:3), pp. 1003–1019.
- Compeau, D. R., and Higgins, C. A. 1995. "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly* (19:2), pp. 189–211.
- Dincelli, E., Goel, S., and Warkentin, M. 2017. "Understanding Nuances of Privacy and Security in the Context of Information Systems," *AMCIS 2017 Proceedings*.
- Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61–80.
- Englehardt, S., Han, J., and Narayanan, A. 2018. "I never signed up for this!: Privacy implications of email tracking," *Proceedings on Privacy Enhancing Technologies* (2018:1).
- Fabian, B., Bender, B., and Weimann, L. 2015. "E-Mail Tracking in Online Marketing - Methods, Detection, and Usage," in *Proceedings of the 12th International Conference on Wirtschaftsinformatik*, O. Thomas and F. Teuteberg (eds.), Osnabrück, Germany, pp. 1100–1114.
- Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A meta-analysis of research on protection motivation theory," *Journal of applied social psychology* (30:2), pp. 407–429.
- Fornell, C., and Larcker, D. F. 1981. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18:1), pp. 39–50.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A primer on partial least squares structural equation modeling (PLS-SEM)*, Los Angeles, London, New Delhi, Singapore,

- Washington DC, Melbourne: Sage.
- Hasounah, A., and Alqeed, M. 2010. "Measuring the Effectiveness of E-mail Direct Marketing in Building Customer Relationship," *International Journal of Marketing Studies* (2:1), pp. 48–64.
- Henseler, J., Hubona, G., and Ray, P. A. 2016. "Using PLS path modeling in new technology research: Updated guidelines," *Industrial Management & Data Systems* (116:1), pp. 2–20.
- Henseler, J., Ringle, C. M., and Sarstedt, M. 2014. "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science* (43:1), pp. 1–21.
- Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., and Dhillon, G. 2014. "A Framework and Guidelines for Context-Specific Theorizing in Information Systems Research," *Information Systems Research* (25:1), pp. 111–136.
- Hu, L.-T., and Bentler, P. M. 1999. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp. 1–55.
- Hulland, J. 1999. "Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies," *Strategic Management Journal* (20:2), pp. 195–204.
- Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly* (34:3), 549-A4.
- Karwatzki, S., Trenz, M., Tuunainen, V. K., and Veit, D. 2017. "Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence," *European Journal of Information Systems* (26:6), pp. 688–715.
- Kim, T.-S. 2016. "Factors influencing the intention to adopt identity theft protection services: Severity vs vulnerability," *PACIS 2016 Proceedings*.
- Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS Quarterly* (31:1), pp. 59–87.
- Marett, K., McNab, A., and Harris, R. 2011. "Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory," *AIS Transactions on Human-Computer Interaction* (3:3), pp. 170–188.
- Merchant, B. 2017. *How email open tracking quietly took over the web*.
<https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/>. Accessed 22 January 2018.
- Milne, S., Orbell, S., and Sheeran, P. 2002. "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions," *British Journal of Health Psychology* (7:2), pp. 163–184.
- Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory," *Journal of applied social psychology* (30:1), pp. 106–143.
- Mohamed, N., and 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), pp. 2366–2375.
- Mohiyeddini, C., Pauli, R., and Bauer, S. 2009. "The role of emotion in bridging the intention–behaviour gap: The case of sports participation," *Psychology of Sport and Exercise* (10:2), pp. 226–234.
- Mousavizadeh, M., and Kim, D. J. 2015. "A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory," in *Proceedings of the Thirty Sixth International Conference on Information Systems*, D. Leidner and J. Ross (eds.), Dallas, TX, USA.
- Myry, L., Siponen, M., Pahnla, S., Vartiainen, T., and Vance, A. 2017. "What levels of moral reasoning and values explain adherence to information security rules?: An empirical study," *European Journal of Information Systems* (18:2), pp. 126–139.
- Ngugi, B., and Kamis, A. 2013. "Modeling the Impact of Biometric Security on Millennials' Protection Motivation," *Journal of Organizational and End User Computing* (25:4), pp. 27–49.
- Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric properties in a community sample," *Journal of Behavioral Medicine* (17:5), pp. 511–522.

- Peng, C.-Y. J., Lee, K. L., and Ingersoll, G. M. 2002. "An Introduction to Logistic Regression Analysis and Reporting," *The Journal of Educational Research* (96:1), pp. 3–14.
- Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179–214.
- Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of psychology* (91:1), pp. 93–114.
- Rogers, R. W., and Prentice-Dunn, S. 1997. "Protection motivation theory," in *Handbook of health behavior research 1: Personal and social determinants*, New York, NY, US: Plenum Press, pp. 113–132.
- Schwarz, A., Rizzuto, T., Carraher-Wolverton, C., Roldan, J. L., and Barrera-Barrera, R. 2017. "Examining the Impact and Detection of the "Urban Legend" of Common Method Bias," *ACM Sigmis Database* (48:1), pp. 93–119.
- Smith, J. H., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 980–1015.
- Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503–529.
- Terlizzi, A. M., Brandimarte, L., Brown, S., and Sanchez, O. P. 2019. "Privacy Concerns and Protection Motivation Theory in the Context of Mobile Banking," in *Proceedings of the 27th European Conference on Information Systems (ECIS)*, Uppsala, Sweden.
- van Eerde, W., and Thierry, H. 1996. "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* (81:5), pp. 575–586.
- Vishwanath, A., Xu, W., and Ngoh, Z. 2018. "How people protect their privacy on facebook: A cost-benefit view," *Journal of the Association for Information Science & Technology* (69:5), pp. 700–709.
- Witte, K. 1992. "Putting the fear back into fear appeals: The extended parallel process model," *Communication Monographs* (59:4), pp. 329–349.
- Xu, H., Hao, S., Sari, A., and Wang, H. 2018. "Privacy Risk Assessment on Email Tracking," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Honolulu, HI.
- Youn, S. 2005. "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *Journal of Broadcasting & Electronic Media* (49:1), pp. 86–110.
- Youn, S. 2009. "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *Journal of Consumer Affairs* (43:3), pp. 389–418.



Appendix

1 PUBLICATIONS

1.1 JOURNAL-ARTIKEL (PEER REVIEWED)

- Maier, C., Laumer, S., Wirth, J., and Weitzel, T. 2019. "Technostress and the hierarchical levels of personality: a two-wave study with multiple data samples," *European Journal of Information Systems* (28:5), pp. 496–522, <http://dx.doi.org/10.1080/0960085X.2019.1614739>
- Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2019. "Perceived information sensitivity and interdependent privacy protection: a quantitative study," *electronic markets* (29:3), pp. 359–378, <http://dx.doi.org/10.1007/s12525-019-00335-0>

1.2 KONFERENZ-ARTIKEL (PEER REVIEWED)

- Wirth, J., and Maier, C. 2019. "Privacy and Speech-Disclosure: An Extension of the Privacy Calculus," in *Proceedings of the 27th European Conference on Information Systems (ECIS)*, P. Johannesson, P. Ågerfalk and R. Helms (eds.), Stockholm & Uppsala, Sweden. (Research in Progress)
- Wirth, J., Maier, C., and Laumer, S. 2019. "Subjective Norm and the Privacy Calculus: Explaining Self-Disclosure on Social Networking Sites," in *Proceedings of the 27th European Conference on Information Systems (ECIS)*, P. Johannesson, P. Ågerfalk and R. Helms (eds.), Stockholm & Uppsala, Sweden.
- Wirth, J., Maier, C., and Laumer, S. 2019. "Justification of Mass Surveillance: A Quantitative Study," in *Proceedings of the 14th International Conference on Wirtschaftsinformatik*, T. Ludwig and V. Pipek (eds.), Siegen, Germany.
- Wirth, J., Maier, C., and Laumer, S. 2018. "The Influence of Resignation on the Privacy Calculus in the Context of Social Networking Sites: an Empirical Analysis," in *Proceedings of the 26th European Conference on Information Systems*, P. Bednar, U. Frank and K. Kautz (eds.), Portsmouth, UK.
- Wirth, J. 2018. "Dependent Variables in the Privacy-Related Field: A Descriptive Literature Review," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, T. Bui (ed.), Waikoloa Village, Hawaii, pp. 3658–3667.
- Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2017. "Understanding Privacy Threat Appraisal and Coping Appraisal through Mindfulness," in *Thirty Eighth International Conference on Information Systems*, Y. J. Kim, R. Agarwal and J. K. Lee (eds.), South Korea, pp. 1–11. (Research in Progress)
- Maier, C., Wirth, J., Laumer, S., and Weitzel, T. 2017. "Personality and Technostress: Theorizing the Influence of IT Mindfulness," in *Thirty Eighth International Conference on Information Systems*, Y. J. Kim, R. Agarwal and J. K. Lee (eds.), South Korea. (Research in Progress)
- Wirth, J. 2017. "Strength of Ties as an Antecedent of Privacy Concerns: A Qualitative Research Study," in *Proceedings of the 23rd Americas Conference on Information Systems*, D. Strong and J. Gogan (eds.), Boston, USA.
- Wirth, J., and Maier, C. 2017. "Why individuals switch to using mobile payment: A migration-theoretic, empirical study," in *Proceedings of the 23rd Americas Conference on Information Systems*, D. Strong and J. Gogan (eds.), Boston, USA.
- Oehlhorn, C., Maier, C., Wirth, J., Laumer, S., and Dürr, S. 2016. "A Temptation to Stalk: The Impact of Curiosity on User Acceptance of Social Networking Sites," in *Proceedings of the 22nd Americas Conference on Information Systems*, B. Shin, R. Nickerson and R. Sharda (eds.), San Diego, California.
- Wirth, J., Maier, C., Laumer, S., and Weitzel, T. 2015. "Drivers and Consequences of Frustration When Using Social Networking Services: A Quantitative Analysis of Facebook Users," in *Proceedings of the 21st Americas Conference on Information Systems*, A. Dennis and S. Paul (eds.), Fajardo, Puerto Rico.

1.3 WORKSHOP-ARTIKEL (PEER REVIEWED)

- Wirth, J., and Maier, C. 2017. "The Influence of Resignation on the Privacy Calculus: A Research

- Approach,” in Pre-ICIS Workshop on Information Security and Privacy, Seoul, South Korea. (Research in Progress)
- Wirth, J. 2017. “Individuals' Beliefs and Actions in Respect to Privacy: A Research Agenda,” in Proceedings of the Doctoral Consortium WI, St. Gallen, CH.
- Wirth, J., Maier, C., and Laumer, S. 2015. “Influence of laziness on data disclosure: an empirical investigation,” in Twentieth DIGIT Workshop, H. Sun, C. Hsu and R. T. Wright (eds.), Fort Worth, TX, USA. (Research in Progress)
- Laumer, S., Maier, C., Wirth, J., and Weitzel, T. 2015. “A work system theory perspective on user satisfaction: Using multiple case studies to propose a work system success model,” in Proceedings of the Special Interest Group on Adoption and Diffusion of Information Technology (DIGIT) (Pre-ICIS Workshop), Fort Worth, TX, USA.
- Wirth, J., Laumer, S., Maier, C., and Weitzel, T. 2014. “Using a work system theory perspective to review 25 years of technology acceptance research: proposing a research agenda,” in Proceedings of the Special Interest Group on Adoption and Diffusion of Information Technology (DIGIT) (Pre-ICIS Workshop), Auckland, New Zealand.

1.4 SONSTIGE

- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020. “Social Recruiting und Active Sourcing - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020. “Generation Z - die Arbeitnehmer von morgen - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020. “Employer Branding - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Weinert, C., Pflügner, K., Oehlhorn, C., Wirth, J., and Laumer, S. 2020. “Digitalisierung und Zukunft der Arbeit - Ausgewählte Ergebnisse der Recruiting Trends 2020 und der Bewerbungspraxis 2020,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019. “Social Recruiting und Active Sourcing - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019. “Employer Branding - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2019. “Digitalisierung und Zukunft der Arbeit - Ausgewählte Ergebnisse der Recruiting Trends 2019 und der Bewerbungspraxis 2019,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018. “Social Recruiting und Active Sourcing, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018. “Mobile Recruiting, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018. “Employer Branding, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Maier, C., Oehlhorn, C., Weinert, C., Wirth, J., and Laumer, S. 2018. “Digitalisierung der Personalgewinnung, Ausgewählte Ergebnisse der Recruiting Trends 2018 und der

- Bewerbungspraxis 2018,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017. “Women in IT - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017. “Employer Branding und Personalmarketing - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017. “Bewerbung der Zukunft - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2017. “Active Sourcing und Social Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2017 und der Bewerbungspraxis 2017,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016. “Techniksprung in der Rekrutierung - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016. “Mobile Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016. “Employer Branding und Personalmarketing - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016. “Bewerbung der Zukunft - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016. “Best Practices und Big Failures - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Laumer, S., Maier, C., Oehlhorn, C., Wirth, J., and Weinert, C. 2016. “Active Sourcing und Social Recruiting - Ausgewählte Ergebnisse der Recruiting Trends 2016 und der Bewerbungspraxis 2016,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Eckhardt, A., Laumer, S., Maier, C., von Stetten, A., Weinert, C., and Wirth, J. 2015. “Recruiting Trends im Mittelstand - Eine empirische Untersuchung mit 1.000 Unternehmen aus dem deutschen Mittelstand,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Eckhardt, A., Laumer, S., Maier, C., von Stetten, A., Weinert, C., and Wirth, J. 2015. “Recruiting Trends 2015 - Eine empirische Untersuchung mit den Top-1.000-Unternehmen aus Deutschland sowie den Top-300-Unternehmen aus den Branchen Finanzdienstleistung, Health Care und IT,” , Research Report, Otto-Friedrich-Universität Bamberg.
- Weitzel, T., Eckhardt, A., Laumer, S., Maier, C., von Stetten, A., Weinert, C., and Wirth, J. 2015. “Bewerbungspraxis 2015 - Eine empirische Studie mit 7.000 Stellensuchenden und Karriereinteressierten im Internet,” , Research Report, Otto-Friedrich-Universität Bamberg.