Social Nudges as Mitigators in Privacy Choice Environments

Klumpe, Johannes

(2020)

Social Nudges as Mitigators in Privacy Choice Environments

Am Fachbereich Rechts- und Wirtschaftswissenschaften
der Technischen Universität Darmstadt

eingereichte

Dissertation

vorgelegt von

Johannes Wilhelm Heribert Klumpe

geboren am 18.10.1988 in Friesoythe

zur Erlangung des akademischen Grades
Doctor rerum politicarum (Dr. rer. pol.)

Erstgutachter: Prof. Dr. Benlian
Zweitgutachter: Prof. Dr. Schiereck

Darmstadt 2020

Klumpe, Johannes: Social Nudges as Mitigators in Privacy Choice Environments
Darmstadt, Technische Universität Darmstadt,
Jahr der Veröffentlichung der Dissertation auf TUprints: 2020
Tag der mündlichen Prüfung: 24.06.2020

Acknowledgements

Firstly, I like to express my gratitude to my advisor Professor Alexander Benlian for his continuous support, encouragement, and guidance, which have been indispensable to the development of this dissertation. My gratitude also goes to Oliver Francis Koch, who encouraged me to start my research, for his friendship, support, and guidance along the way. I also want to thank my co-authors for the fruitful collaborations that have contributed to this dissertation.

Many thanks to Gregor Albrecht and Justus Bender-Hacke and all my other friends for their support in proofreading and the encouraging words during my pursuit of this degree.

Lastly, I also want to thank my parents Hans-Georg and Annette Klumpe, as well as my sister Antonia Klumpe, who have always supported me and pushed me to achieve greater things.

Abstract

In light of prominent data leaks and a surge of civilian surveillance systems, information service providers are confronted with an increased level of skepticism towards their privacy practices. The predicament is that not only do providers rely on users' information to optimize their services, users also risk losing the benefits of increasingly personalized services.

Research on information privacy has paid great attention to explaining and predicting factors of privacy-related outcomes. On a macro level, researchers have come up with a plethora of models that are focused on deliberate and rational decision-making. In contrast, non-rational decision-making within privacy choice environments (i.e., presentation of privacy-related choices to users) has to date only been sparsely investigated. A more holistic approach to privacy-related outcomes is provided by the Person-Technology fit model. This model describes a relationship between an individual and a technology, which, when it is out of equilibrium, causes stress for the individual. Research on technology-induced stress has discovered that it affects both general stress (e.g., psychological strain) and situational stress outcomes (e.g., behavioral reactions). In this regard, research has explicated intrusive technology features (i.e., features that acquire information from and provide information to the user) as the most salient drivers of stress caused by privacy invasions for users of digital services. However, previous contributions have focused on psychological antecedents of privacy invasions, neglecting how firms may design and enhance privacy choice environments to alleviate privacy-related stress. Likewise, existing literature lacks to address how service providers can combine different technology features in the design of their services to reduce privacy-related stress. Hence, digital nudging, which refers to the practice of influencing user behavior in digital choice environments by leveraging the effect of cognitive biases and decision heuristics in user interface design, holds promising potential for service providers to overcome the detrimental effects of privacy-related stress. Specifically, research has found evidence that social nudges, defined as nudges based on social influences (i.e., unwritten social laws), can guide users to better decisions in choice environments. However, social nudging has been ignored in the context of privacy-related decision making.

This thesis draws on four studies that were conducted to investigate how intrusive technology features affect privacy-related outcomes, and how to utilize social nudges as mitigating technology features in privacy choice environments. The first study describes a laboratory experiment and a subsequent field experiment, which investigated how the intrusive effects of unintentional voice activations of smart home assistants drive user strain and interpersonal

conflicts through privacy invasions, while the study demonstrates how anthropomorphic design features alleviate user strain. The second study elaborates upon the intrusive effect of push-based information delivery on users' geographical location information disclosure through privacy concerns, which can be attenuated by signals of social proof in mobile app stores. Finally, for the third study, we cooperated with the German startup Partner der Wissenschaft UG to investigate how low message interactivity affects users' information disclosure in a chatbot conversation, which we enhanced by employing platform self-disclosure nudges.

In sum, this thesis highlights the importance of understanding the technology-stressor-strain causal relationship for information services by providing significant contributions: First, the findings extend previous research on technology-induced stress by illuminating specific design mechanisms for digital services. In this regard, the studies demonstrate how intrusive technology features drive privacy-related stressors and ultimately cause users to disengage with the respective information services. Thereby, we address the calls for particular and context-related intrusive technology features with applicable design recommendations from Ayyagari, Grover, and Purvis (2011) and Speier, Vessey, and Valacich (2003). Second, this thesis expands the Person-Technology model by a new layer of technology features that help to mitigate and overcome users' privacy-related stress. More specifically, this study illuminates how social nudges can be utilized as mitigating strategies for technology-induced stress and hereby effectuate better privacy-related outcomes. In this regard, this thesis addresses the calls for research from Kretzer and Maedche (2018) and Mirsch, Lehrer, and Jung (2017) on specific and context-related digital nudges with applicable design recommendations by putting together a catalog of social nudges for privacy choice environments.

Zusammenfassung

Angesichts von prominenten Datenlecks und der vermehrten Verbreitung von zivilen Überwachungssystemen in den letzten Jahren, sehen sich die Anbieter von Informationsdiensten mit einer verstärkten Kontrolle ihrer Datenschutzpraktiken konfrontiert. Das ist nicht nur deshalb problematisch, weil Anbieter auf die Informationen ihrer Nutzer angewiesen sind, um ihre Dienste kontinuierlich zu verbessern, sondern auch, weil die Nutzer selbst Gefahr laufen, Vorteile von personalisierten Diensten zu verlieren.

Die Privatsphäre-Forschung hat der Erklärung und Vorhersage von Faktoren, die sich auf die Privatsphäre auswirken, große Aufmerksamkeit gewidmet. Auf der Makroebene hat die Forschung eine Fülle von Modellen entwickelt, die auf der Grundlage von bewusster und rationaler Entscheidungsfindung basieren. Im Gegensatz dazu wurde bislang die nicht-rationale Entscheidungsfindung in Privatsphäre-Entscheidungsumgebungen (d.h. Umgebungen, in denen Entscheidungen im Zusammenhang mit dem Datenschutz der Nutzer präsentiert und gestaltet werden) nur wenig untersucht. Ein Modell, das einen ganzheitlichen Ansatz für die Untersuchung von Auswirkungen auf die Privatsphäre bietet, ist das Person-Technologie-Fit-Modell. Das Modell beschreibt die Beziehung zwischen einem Individuum und einer Technologie, die, wenn sie aus dem Gleichgewicht gerät, Stress für das Individuum verursacht. Die Forschung über technologieinduzierten Stress hat enthüllt, dass dieser sowohl allgemeinen Stress (z.B. psychische Belastung) als auch situationsbedingten Stress (z.B. Verhaltensreaktionen) beeinflusst. In dieser Hinsicht hat die Forschung invasive Technologiefunktionen (d.h. Funktionen, die Informationen vom Benutzer akquirieren und Informationen bereitstellen) als die hervorstechendste Ursache für Stress erklärt, der durch Eindringen in die Privatsphäre der Benutzer von digitalen Diensten verursacht wird. Die bisherigen Beiträge in der Forschung haben sich auf die psychologischen Ursachen von Eingriffen in die Privatsphäre konzentriert, so dass eine große Lücke besteht hinsichtlich der Gestaltung und Verbesserung von Privatsphäre-Entscheidungsumgebungen, um Stress im Zusammenhang mit Privatsphäre zu mindern. Ebenso weist die Forschung immer noch eine erhebliche Lücken auf, was die Frage betrifft, wie Dienstleister verschiedene technologische Merkmale bei der Gestaltung ihrer Dienste kombinieren können, um Stress in Verbindung mit Privatsphäre zu verringern. Vor diesem Hintergrund birgt digitales Nudging, also die Beeinflussung des Nutzerverhaltens in digitalen Entscheidungsumgebungen durch Lenkung von kognitiven Verzerrungen und Entscheidungsheuristiken, ein vielversprechendes Potenzial für Dienstanbieter, um die nachteiligen Auswirkungen von Stress im Zusammenhang mit

Privatsphäre zu überwinden. Insbesondere hat die Forschung bewiesen, dass soziale Nudges, also Nudges, welche auf sozialen Einflüssen (d.h. ungeschriebenen sozialen Gesetzen) basieren, die Benutzer zu besseren Entscheidungen in Entscheidungsumgebungen führen. Allerdings wurden soziale Nudges im Zusammenhang mit der Entscheidungsfindung im Bereich der Privatsphäre bislang nicht untersucht.

Diese Arbeit stützt sich auf vier durchgeführte Studien, die untersuchen, wie sich aufdringliche Technologiemerkmale auf die Privatsphäre auswirken, um zu verstehen, wie soziale Nudges als mildernde Technologiefunktionen in Umgebungen mit Privatsphäre Wahlmöglichkeiten eingesetzt werden können. Die erste Studie zeigt in einem Laborexperiment und einem anschließenden bestätigenden Feldexperiment, wie unbeabsichtigte Sprachaktivierungen Benutzer stressen und zwischenmenschliche Konflikte durch das Eindringen in die Privatsphäre erzeugen, die wir durch den Einsatz anthropomorpher Designmerkmale bei Smart Home Assistants mildern konnten. Die zweite Studie zeigt, wie der aufdringliche Effekt von push-basierter Informationsbereitstellung die Freigabe des geografischen Standortes der Benutzer durch gesteigerte Privatsphärebedenken beeinflusst, die, wie wir festgestellt haben, durch Signale von sozialer Akzeptanz in mobilen App-Stores abgeschwächt werden können. Schließlich haben wir für die dritte Studie mit dem deutschen Startup Partner der Wissenschaft UG zusammengearbeitet, um zu untersuchen, wie sich eine geringe Nachrichteninteraktivität auf die Informationspreisgabe der Nutzer in einer Chatbot-Konversation auswirkt, welche wir mithilfe von Plattform Selbstauskünften verbessern.

Zusammenfassend unterstreicht diese Arbeit die Bedeutung eines besseren Verständnisses der Technologie-Stress-Beziehung für Informationsdienste und hat diesbezüglich mehrere wichtige Beiträge: Erstens erweitern diese Ergebnisse die bisherige Forschung über technologieinduzierten Stress, indem sie spezifische Designmechanismen für digitale Dienste beleuchten. In dieser Hinsicht zeigen diese Studien, wie invasive Technologiefunktionen Stressoren für Privatsphäre verstärken und letztlich dazu führen, dass sich die Benutzer von Informationsdiensten abwenden. Diese Arbeit folgt den Aufforderungen von Ayyagari, Grover und Purvis (2011) und Speier, Vessey und Valacich (2003), Designempfehlungen für kontextbezogene und spezifische invasive Technologiefunktionen zu erarbeiten. Zweitens erweitert diese Studie das Person-Technologie-Modell um eine neue Ebene von Technologiefunktionen, die dazu beitragen, den Stress der Benutzer im Zusammenhang mit ihrer Privatsphäre zu mildern und zu überwinden. Genauer gesagt beleuchtet diese Studie, wie soziale Nudges als Milderungsstrategien für technologiebedingten Stress eingesetzt werden

können und dadurch bessere Ergebnisse in Bezug auf Privatsphäre erzielen. In dieser Hinsicht geht diese Arbeit auf die Aufforderungen von Kretzer und Maedche (2018) und Mirsch, Lehrer, und Jung (2017) zu spezifischen und kontextbezogenen digitalen Nudges mit anwendbaren Gestaltungsempfehlungen ein, indem sie einen Katalog sozialer Nudges für Privatsphäre-Entscheidungsumgebungen zusammenstellt.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ANOVA	Analysis of Variance
APCO	Antecedents → Privacy Concerns → Outcomes
AVE	Average Variance Extracted
CFA	Confirmatory Factor Analysis
CI	Confidence Interval
CV	Control Variable
ICT	Information and Communication Technologies
IS	Information Systems
IT	Information Technology
LLCI	Lower Limit of Confidence Interval
M	Mean
P-T	Person-Technology
RQ	Research question(s)
SD	Standard Deviation
SE	Standard Error
SHA	Smart Home Assistants
StD	Standard Deviation
ULCI	Upper Limit of Confidence Interval

Chapter 1: Introduction

1.1 Motivation and Research Questions

Nowadays, digital services focus on adding value for their users through the collection and processing of personal information in order to deliver custom-tailored information services (Barker, 2016). These vast amounts of collected data have substantial economic value. Personal information (e.g., an individual's preferences and interests) is increasingly regarded as a business asset used to enhance service value, to provide targeted advertising, or as information goods for third parties. A multitude of new business models has emerged around personal data such as sharing-economy services (e.g., Airbnb), and crowdsourcing platforms (e.g., TripAdvisor) with benefits for data subjects and data holders alike (Schenk & Guittard, 2011). However, data leaks and privacy scandals have confronted information service providers with ever-increasing scrutiny towards their privacy practices. For example, Facebook's reputation has been severely damaged after millions of private user profiles were analyzed and used for targeted election campaigns in the Cambridge Analytica scandal (Neate, 2018). These concerns for information privacy drove firms such as Apple to position themselves as privacy companies that offer digital services with sophisticated personal data protection (Etherington, 2019). This strategy emphasizes the importance for practitioners to better understand how privacy-related choice environments work and how they can be shaped for digital information services (Barker, 2016).

Previous literature on information privacy can be categorized into two streams. The research, in one stream, has come up with a multitude of models to explain users' deliberate behavioral reactions in information privacy choice environments. In this regard, research has investigated the disclosure of personal information for newsletter sign-ups and website registrations (Keith, Thompson, Hale, Lowry, & Greer, 2013; Y. Li, 2014) as well as the disclosure of location information (Koohikamali, Gerhart, & Mousavizadeh, 2015; H. Xu, Teo, Tan, & Agarwal, 2012). Ultimately this stream of research converged in declaring the construct of concerns for information privacy as the most reliable proxy for privacy-related decision making (Benamati, Ozdemir, & Smith, 2016; Dinev, McConnell, & Smith, 2015; Smith, Dinev, & Xu, 2011a). The second stream of research has focused on psychological stress and has developed macro models to investigate the detrimental effects of privacy invasions on the well-being of individuals in information services (Allen & Shoard, 2005; Y.-K. Lee, Chang, Lin, & Cheng, 2014; Pinsonneault & Heppel, 1997; Weinert, Laumer, Maier, & Weitzel, 2013). In this regard, previous research has predominantly investigated how privacy invasions drive general

psychological stress in workplace environments (Ayyagari, Grover, & Purvis, 2011; Maier, Laumer, Weinert, & Weitzel, 2015). Specifically, literature has highlighted intrusive technology features, which describe characteristics that reflect a technologies' presenteeism (i.e., degree to which a feature enables individuals to be reachable) and anonymity (i.e., degree to which exact use of a feature could be identifiable), as the main drivers of privacy invasions (Ayyagari et al., 2011; Pinsonneault & Heppel, 1997). Nevertheless, only recently has research started to investigate how the digitization of the individual (i.e., exposure to ubiquitous computing) affects users in their personal environment. Ergo, the person-technology fit model aims to investigate how a technology adopted by an individual is aligned with their environmental expectations and how a user's misfit with their environment drives general user strain (i.e., the ultimate form of stress) as well as situational behavioral reactions and usage intentions (Ayyagari et al., 2011; D'Arcy, Gupta, Tarafdar, & Turel, 2014; T. Ragu-Nathan, Tarafdar, Ragu-Nathan, & Tu, 2008; Tarafdar, Pullins, & Ragu-Nathan, 2015; Tarafdar, Tu, Ragu-Nathan, & Ragu-Nathan, 2007; Tarafdar, Tu, & Ragu-Nathan, 2010). Both streams of research have focused on identifying the most crucial technology features and stressors that are connected with privacy-related outcomes, hereby contributing towards explaining and predicting users' behavior in privacy contexts (France Bélanger & Robert E Crossler, 2011; Smith et al., 2011a). Despite these valuable contributions, research has only recently, started to investigate how privacy choice environments can be designed to enhance users' non-rational decision-making. Research has only sparsely investigated how privacy choice environments can be shaped to improve decision-making outcomes and individuals' well-being regarding the ever-increasing amount of privacy invasions through digital information services.

Dual-processing theory describes the distinction between cognitive processes that are fast, automatic, and unconscious (system 1) and those that are slow, deliberate, and conscious (system 2) (Evans, 2008; Gilovich, Griffin, & Kahneman, 2002). Dinev et al. (2015) highlight that previous information privacy research has predominantly been focused on developing macro models to predict how individuals behave under effortful, deliberate information processing in privacy contexts. However, none of the previous macro models consider the nontrivial impact of low-effort thinking and extraneous influence of default heuristic processes and biases within information services. An upcoming stream of research, arising from the findings of the dual-processing theory, has coined the term *nudging* to define the act of guiding an individual's behavior in choice environments by leveraging the underlying heuristic processes and cognitive biases of system 1 to build so-called choice environments (Guthrie, Mancino, & Lin, 2015; Sunstein, 2014). Nudging, which has also been transported to the digital

world (i.e., digital nudging), has been successfully implemented to guide users' decision making in situations of uncertainty and decision-inertia (C. Schneider, Weinmann, & vom Brocke, 2017; Weinmann, Schneider, & Brocke, 2016). According to Mirsch, Lehrer, and Jung (2017), social influences are among the most effective cognitive biases that guide users' within digital choice environments. Even though research has paid great attention towards the implementation of social influences as persuasion tactics in offline and online sales channels (e.g., Monteserin & Amandi, 2015; Zhou & Guo, 2017; Zimmer, Arsal, Al-Marzouq, Moore, & Grover, 2010), there is limited knowledge on the use of social influences as digital nudges that guide users' decision making in privacy choice environments (Gu, Xu, Xu, Zhang, & Ling, 2017; Weinmann et al., 2016). In that matter, Kretzer and Maedche (2018) define social nudges as nudges that (1) steer an individual's choice toward a desired option by exploiting the effects of social influence, and (2) that do not change the range of choices available to the individual. However, contributions on social nudges within privacy choice environments have been sparse, leaving open questions as to how this knowledge may be leveraged to shape better privacy decision-making outcomes. Hence, this thesis aims to resolve these pending issues by addressing the following research questions:

RQ1: How do intrusive technology features drive behavioral outcomes through privacy-related stressors within privacy choice environments?

RQ2: How do social nudges interact with stress induced by intrusive technology features within privacy choice environments?

In order to answer these questions, four empirical studies that illuminate the interaction of intrusive technology features with social nudges in various IS contexts in three articles have been carried out. These studies have been published through three articles in IS outlets and are also included in this thesis. The next section discusses the structure of the thesis in detail.

1.2 Thesis Structure and Synopses

After the introduction in Chapter 1, the overall research context is depicted in Chapter 2, followed by the positioning of the thesis. The three peer-reviewed articles, which comprise the four studies, constitute Chapters 3 to 5 in a slightly modified version to facilitate a consistent appearance throughout the thesis (see Table 1). The first article in chapter 3 deals with the implications of privacy invasions through Smart Home Assistants in private households, and how intrusive technology features and anthropomorphism affect users' strain and interpersonal conflicts. The second article in Chapter 4 deals with the role of pull/push information delivery

and social proof nudges improving location disclosure outcomes. Lastly, the third article examines how platform self-disclosure and message interactivity in user onboarding with chatbots may be used to enhance user self-disclosure outcomes. Chapter 6 concludes the thesis with the main contributions to research and practice.

Study 1 & 2	**Chapter 3** Article 1	**Smart Home Assistants with Intrusive Technology Features and their Interaction with Anthropomorphic Features** Benlian, A., Klumpe, J., & Hinz, O., (2019) "*Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation*" In: Information Systems Journal. **VHB: A**
Study 3	**Chapter 4** Article 2	**Location Based Services with Push Information Delivery Mechanisms and their Interaction with Social Proof** Klumpe, J., Koch, O. F., & Benlian, A., (2018) "*How pull vs. push information delivery and social proof affect information disclosure in location based services*" In: Electronic Markets, Online First. **VHB: B**
Study 4	**Chapter 5** Article 3	**Chatbots with Low Message Interactivity and their Interaction with Platform Self-Disclosure** Adam, M., & Klumpe, J., (2019) "*Onboarding with a Chat – The Effects of Message Interactivity and Platform Self-Disclosure on User Disclosure Propensity*" In: 27th European Conference on Information Systems (ECIS2019), Stockholm-Uppsala, Sweden. **VHB: B**

Table 1: Overview of Articles.

In the following sections, the articles are summarized, and their main contributions are positioned within the context of the overall research question. The summaries of the articles are written in a first-person plural perspective (i.e., we) to reflect that these studies were conducted with co-authors and, therefore, also express their opinions.

Article 1 (Chapter 3):

Mitigating the Intrusive Effects of Smart Home Assistants with Anthropomorphic Features: A Multi-Method Investigation

Digital services increasingly invaded people's private households due to the rapid adoption of Smart Home Assistants (SHAs). However, the effects of this new device category on users' strain and their interpersonal relationships remain unknown. On the one hand, SHAs enable users to access the internet through voice user interfaces that are always available and effortless to use. On the other hand, service providers have been met with increased scrutiny towards their

privacy practices, because SHAs continuously record their environment to capture voice commands. Thus far, it is unclear how these intrusive technology features affect individual users' concerns for privacy or how they might impair social relationships at home. Despite research on the effect of intrusive technology features in workplace environments, little is known about the effects of these technological characteristics in users' private households. Moreover, there is a lack of understanding on how these privacy invasions and their consequences can be mitigated. This study draws on the synergistic properties of an online experiment (N=136) and a follow-up field survey with a representative sample of SHA users (N=214) to show how and why SHAs' intrusive technology features cause individual strain and interpersonal conflicts at home. Additionally, our study shows how anthropomorphic design features can be leveraged to mitigate the effects of privacy invasions caused by intrusive technology features on users' strain.

Article 2 (Chapter 4):

How Pull vs. Push Information Delivery and Social Proof Affect Information Disclosure in Location Based Services

With the boom of the app economy, users' location information has become an increasingly valuable distinctive feature to deliver personalized products and services. Consequently, privacy concerns rise as a result of growing user awareness towards service providers profiting from personal information. Research on location-based services has thus far been focused on conceptual and technical issues that come with geographical information services, yet has neglected design recommendations regarding location disclosure outcomes. While location disclosure is of crucial importance for service providers aiming to add genuine value through location information, there is a great need for them to better understand what causes privacy concerns and how they can be mitigated. In this study, we have drawn on two design mechanisms, namely pull (i.e., services with user-controlled position awareness) and push (i.e., demanding always-on access location tracking) information delivery mechanisms and social proof cues (i.e., signal of popularity and demand), to investigate how they individually and combined affect users' actual location information disclosure. We conducted a randomized online experiment with 143 smartphone users within the context of a fictitious coupon app, to investigate the effect of our manipulations on users' actual location information disclosure decisions. The results reveal that both strategies increase actual location information disclosure via two distinct mediation paths. On the one hand, we found that pull information delivery

mitigates users' privacy concerns. On the other hand, our findings corroborated previous studies that social proof increases users' trusting beliefs. However, more interestingly when both strategies are employed together, we found that social proof overrides the effect of pull information delivery mechanisms and thereby attenuates users' privacy concerns. In conclusion our study contributes to a better understanding of how users' privacy concerns are affected by social influence nudges and how these nudges can be employed to improve users' location disclosure outcomes.

Article 3 (Chapter 5):

Onboarding with a Chat – The Effects of Message Interactivity and Platform Self-Disclosure on User Disclosure Propensity

User onboarding strategies help companies to activate first time visitors to become familiar with the product and understand the value of the service. Hence, user onboarding has become a pivotal factor for the adoption of digital services against the backdrop of fierce competition in the industry. Previous research has focused on the antecedents of information disclosure for visitors that register by sharing personal information to become users (i.e., activation stage), but has barely taken into consideration actionable design recommendations for companies to shape better activation outcomes. Therefore, this study investigates how social influence cues can be leveraged to shape better personal information disclosure outcomes within the user onboarding journey. Drawing on social response, as well as, social exchange theory, our study investigates how disembodied interfaces like chatbots can facilitate the user onboarding journey. We conducted an empirical study in cooperation with a German startup company, and tested 2095 visitors in a randomized field experiment how low vs. high message interactivity (i.e., static vs. conversational presentation of requests) and platform self-disclosure (i.e., a platform providing information about itself) affect user disclosure propensity (i.e., likelihood that a user discloses information). Our results demonstrate that high message interactivity has a significantly positive effect on users' self-disclosure propensity compared to low message interactivity. Users that were exposed to a platform self-disclosure were significantly more likely to self-disclose personal information as opposed to those who were not exposed to one. Furthermore, high message interactivity significantly amplified the effect of the platform self-disclosure on user disclosure propensity in contrast to low message interactivity.

In addition to the publications summarized above, the following articles, which are not part of this dissertation, were also published during my time as a PhD candidate:

Roethke, K., Klumpe, J., Adam, M., & Benlian, A., (2020) "*Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations*"
In: Decision Support Systems, Online First. **VHB: B**

Schneider, D., Klumpe, J., Adam, M., & Benlian, A., (2019) "*Nudging Users into Electronic Identification Adoption: The Case of E-Government Services*"
In: Electronic Markets, Online First. **VHB: B**

Terres, P., Klumpe, J., Jung, D., & Koch, F. O., (2019) "*Digital Nudges for User Onboarding: Turning Visitors Into Users*"
In: 27th European Conference on Information Systems (ECIS2019), Stockholm-Uppsala, Sweden. **VHB: B**

The next chapter will clarify the overall research context that is relevant to this thesis.

Chapter 2: Research Context

This section is an aggregate of literature reviews, starting with a review on information privacy and digital choice environments to frame the context of this study. Subsequently, the theoretical framework is provided, including a literature review on the Person-Technology model and how it integrates into information privacy research. Finally, in order to ground the understanding of social nudges on solid theoretical reasoning, a literature review on digital nudging and social influences is presented.

2.1 Information Privacy Choice Environments

The societal role of information privacy has evolved as information systems have increased companies' ability to process vast amounts of personal information and monetize on personal data. For example, Facebook's data leak in the Cambridge Analytica Scandal caused its stock value to drop by over $16 billion as soon as the public was informed and dramatically affected their brand identity (Neate, 2018; Rodriguez, 2018; Wong, 2019). Users' increased scrutiny towards service providers' privacy practices has led to a shift in the value perception of information privacy for digital services. Hence, companies, such as Apple, are positioning themselves as privacy-as-a-service companies that emphasize privacy as a critical differentiator to competitors (Etherington, 2019).

Against this backdrop, it has become essential to understand how to design privacy choice environments (i.e., environments that confront users with choices that affect their information privacy) to protect users' privacy and add value through processing personal information (Dinev et al., 2015; Richard H. Thaler, Sunstein, & Balz, 2014; Weinmann et al., 2016). As issues surrounding privacy are myriad and of a varied nature, there are many definitions for information privacy, which generally describe information privacy as an individual's interest in controlling, or at least significantly influencing, the handling of data about themselves (France Bélanger & Robert E Crossler, 2011). We define privacy choice environments as the design of different ways in which to present privacy-related choices to users (Jameson et al., 2014; Smith et al., 2011a; Richard H. Thaler et al., 2014). In choice environments, the outcome of any choice is influenced not only by rational deliberations of the available options but also by how the options are presented (E. J. Johnson et al., 2012; Koch & Benlian, 2017; Richard H. Thaler et al., 2014). For example, Netflix gives the option to either disclose information about previously watched movies for personalized movie suggestions, or to skip that option and start viewing without revealing any information, putting users in control over whether or not they want customized movie suggestions. Information systems that raise privacy conflicts encourage

privacy-protective behavior, which comes at a cost for both parties. On the one hand, users who choose to disclose less information do this at the expense of valuable online services, product customization, or tailored advertising and promotions (Chellappa & Sin, 2005). On the other hand, service providers rely on user information to improve their quality of service, train predictive models, and ultimately, yield profits. Hence, understanding these trade-offs and how consumers approach privacy choices is critical. It is challenging for service providers to design privacy choice environments, having to balance information privacy with utility gains from information disclosure (Dinev et al., 2015).

Extant research on information privacy has explored the factors that drive individuals' willingness to disclose information or to engage in commerce (Dinev et al., 2015; Smith et al., 2011a). This has brought up a plethora of macro models such as the privacy calculus (considers the trade-off between risks and benefits during information disclosure) and the APCO macro model (investigates the effect sequence: Antecedents → Privacy Concerns → Outcomes) (Dinev & Hart, 2006b; H. Xu, H.-H. Teo, B. C. Tan, & R. Agarwal, 2009a). In the past years, this stream of research has converged on explicating privacy concerns as the most salient predictor for information disclosure in privacy choice environments (Dinev & Hart, 2004, 2006b; Dinev et al., 2015; Smith et al., 2011a). Despite these valuable insights, the majority of macro models assumes that users make deliberate decisions in privacy choice environments (e.g., Bansal & Zahedi, 2008; Junglas, Johnson, & Spitzmüller, 2008; Phelps, D'Souza, & Nowak, 2001; Van Slyke, Shim, Johnson, & Jiang, 2006; H. Xu, 2007; H. Xu, Dinev, Smith, & Hart, 2008; H. Xu & Gupta, 2009), yet neglects low-effort thinking, the impact of decision heuristics, and biases when a decision is being made (Dinev et al., 2015; Smith et al., 2011a). Hence, this thesis aims to instruct how to shape privacy choice environments to alter users' non-rational and low-effort decision making.

2.2 Person-Technology Fit in Privacy Choice Environments

As mentioned above, each of our presented studies explains the effect of different design mechanisms on behavioral outcomes within different information privacy macro models. This thesis assembles our studies in a greater scheme, by drawing on the Person-Technology (P-T) fit model, which investigates the sequential effects of Technology Characteristics → Stressors → Outcomes (Ayyagari et al., 2011). The P-T model is derived from the well-established Person-Environment fit model and describes an equilibrium relationship between individuals and technology (Cooper, Dewe, & O'Driscoll, 2001; Jeffrey R Edwards, 1991; Jeffrey R Edwards & Cooper, 1988b). When this relationship is out of equilibrium, it results in stress that

manifests as behavioral strain (i.e., the behavioral reaction of an individual to stress) or psychological strain (i.e., individual's psychological response to stress) (Tarafdar et al., 2010). Misfits and gaps in the relationship between individuals and technology manifest as stressors (i.e., conflicts and stimuli in the technological environment) (Tarafdar et al., 2015). Among the stressors of P-T fit, research has unveiled a variety of stimuli that affect stress such as work-home conflicts, work overload, role ambiguity, job insecurity, and privacy-related stressors (Ayyagari et al., 2011; Maier, Laumer, Weinert, et al., 2015).

From a technology characteristics perspective, Ayyagari et al. (2011) explicated a variety of technology characteristics that are driving stressors within the P-T model: First, usability features capture the usefulness, complexity, and reliability of a technology. Second, dynamic features correspond to the pace of change that the specific technology is undergoing. Lastly, intrusive technology features resemble the presenteeism and anonymity of a technology. Amongst these technology characteristics, research has found that intrusive technology features are the sole driver of privacy-related stressors (Ayyagari et al., 2011; Tarafdar et al., 2010). Intrusive technology features are defined as a source of invasion by technology, which lead to increased concern about users' privacy (Best, Krueger, & Ladewig, 2006; McFarlane & Latorella, 2002). Within privacy choice environments, intrusive technology features are used to capture information from the individual (e.g., voice interfaces or input fields) or convey information to the individual (e.g., push notifications). Research has thus far focused on the concept of presenteeism and anonymity as two main indicators for intrusive technology characteristics (Ayyagari et al., 2011). Technology presenteeism, on the one hand, is one of the most widely discussed factors in the practitioner and technostress literature (G. B. Davis, 2002; Kakabadse, Kouzmin, & Kakabadse, 2017; T. Ragu-Nathan et al., 2008; Tarafdar et al., 2007; Tu, Wang, & Shu, 2005). In human-computer literature, presenteeism is seen as a source of interruptions leading to reduced efficiencies and stress (McFarlane & Latorella, 2002). Further, these intrusions enable increased communication flow, which leads to irresolution of work tasks (G. B. Davis, 2002; Kakabadse et al., 2017; T. Ragu-Nathan et al., 2008; Tarafdar et al., 2007; Tu et al., 2005). This kind of fragmentation of tasks is seen as a source of stress and frustration (Straub & Karahanna, 1998). Hence, users are becoming increasingly concerned about their privacy being invaded by computer technologies (Best et al., 2006). On the other hand, technology anonymity is seen as the degree to which technology makes users identifiable and trackable (Ayyagari et al., 2011). Research has demonstrated that users are apprehensive about the possibility of invasive monitoring (e.g., surveillance at the workplace) (Alge, 2001; Best et al., 2006; Zweig & Webster, 2002). The ability of information services to identify people and

their behavior enables monitoring which, if done implicitly or explicitly, invades users' privacy, triggering a concern over loss of privacy (Ayyagari et al., 2011; DeTienne, 1993; Frey, 1993; Jenero & Mapesriordan, 1992; Tarafdar et al., 2015). Technology presenteeism and technology anonymity refers to a range of intrusive technology features. Thus, IS researchers called for research on specific and context-related intrusive technology features with applicable design recommendations (Ayyagari et al., 2011; Cheri Speier, Iris Vessey, & Joseph S Valacich, 2003). In this regard, this study aims to provide a better understanding of actual and timely intrusive technology features, such as voice user interfaces, within information privacy choice environments.

From an outcome perspective, literature differentiates technostress research into two streams. One stream focuses on the general strain-related outcomes of technostress (Brod, 1984; Ennis, 2005; Tarafdar et al., 2007; Weil & Rosen, 1997); while the second stream focuses on the situational and usage-related outcomes of technostress (Maier, Wirth, Laumer, & Weitzel, 2017; Tarafdar et al., 2010; Weinert, Maier, & Laumer, 2014). For the most part, research has considered technostress along the entire transactional process of users encountering technological stimuli and experiencing stress-related outcomes, such as behavioral (e.g., decrease in productivity) and psychological (e.g., dissatisfaction and poorer job performance) strain on an individual's life (Ayyagari et al., 2011; T. Ragu-Nathan et al., 2008). This stream of research has predominantly been focused on the prediction of technology stressors in workplace environments and has explored its impact on organizational settings (Galluch, Grover, & Thatcher, 2015; Maier, Laumer, Eckhardt, & Weitzel, 2015; Srivastava, Chandra, & Shirish, 2015; Tarafdar et al., 2007). Only recently has research started to discover how P-T fit affects users' psychological well-being, as a result of the digitization of the individual and their personal environments (Benlian, 2020; Maier, Laumer, Eckhardt, et al., 2015; Ofir Turel, Cheung, Matt, & Trenz, 2019). In this regard, Benlian (2020) suggests that person-technology misfits can spill-over from work to home environments and cause conflicts with peers and family members. The second and younger stream, has focused on situational and usage-related outcomes, such as behavioral reactions and intentions of service discontinuance (Dinev et al., 2015; Maier, Laumer, Weinert, et al., 2015; Tarafdar et al., 2010). This stream has exposed that stress can impair users' decision making and decrease users' satisfaction with an information service. Further research in this direction has laid focus on user's behavioral intentions (e.g., Y.-K. Lee et al., 2014; Maier, Laumer, Weinert, et al., 2015; Weinert et al., 2014) without investigating actual decision-making outcomes. In this regard, this thesis focuses on the most

salient privacy-related behavioral outcome, namely information disclosure (Dinev et al., 2015; Smith et al., 2011a).

As the theoretical interest of this thesis lies in the design of privacy choice environments, we focus on the effects of intrusive technology features and the effects of privacy-related stressors. This thesis aims to contribute to a better understanding of how intrusive technology characteristics drive stressors in privacy choice environments and how these stressors can be mitigated (see Figure 1).

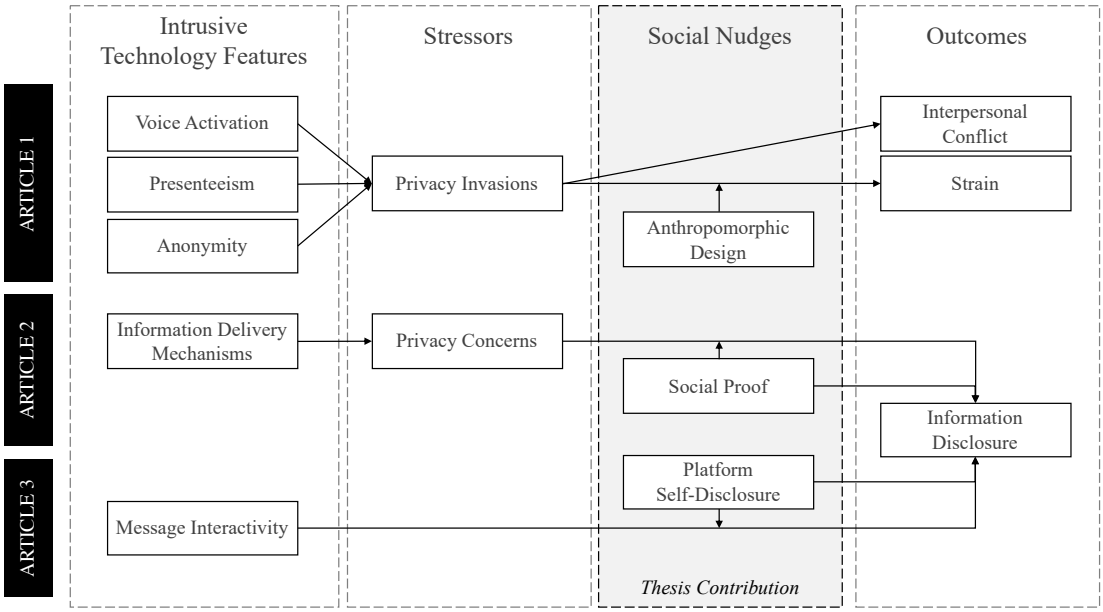


Figure 1: Person-Technology Fit Model and Thesis Contribution.

Ultimately, while previous literature focused on identifying and examining underlying mechanisms and psychological pathways of intrusive technology features and their efficacy on users' strain (Ayyagari et al., 2011; Y.-K. Lee et al., 2014; Srivastava et al., 2015; Tarafdar et al., 2010), there have yet to be studies conducted, with actual design implementations in privacy choice environment. Thus, this study aims to contribute towards a better understanding of the effects of intrusive technology features within privacy choice environments. Although research has investigated the effect of intrusive technology features on privacy invasions (e.g., Ayyagari et al., 2011; Cooper et al., 2001; Eddy, Stone, & Stone-Romero, 1999) it has barely touched upon mitigation measures (e.g., Gu et al., 2017). This research aspires to demonstrate how technology features can be employed to mitigate stressors in privacy choice environments. For this reason, we have added a layer of actionable mitigating technology features to the P-T model to investigate the interplay of intrusive and mitigating technology characteristics, specifically in the information privacy context.

2.3 Social Nudges

The challenge of designing privacy choice environments becomes apparent when one considers the complexities introduced by heterogeneous and intricated choices which are susceptible to nuanced manipulations of decision framing (Mirsch et al., 2017; Weinmann et al., 2016). Research has thus far focused on controlling mechanisms for privacy protection (K. Chen & Rea, 2004; Kagal & Abelson, 2010). It is clear, however, that this may not suffice as choice environments need to be carefully designed, regarding the intricate outcomes of privacy choices (Kagal & Abelson, 2010). Control mechanisms mainly have the effect of reducing users' privacy concerns by providing the opportunity to restrict the collection and use of their personal information while, in practice, actually implementing policies that result in users continuing to disclose broad, and potentially harmful, information to firms (Adjerid, Acquisti, & Loewenstein, 2018).

Social nudging offers a promising avenue to design and investigate technology features that are less intrusive and might also mitigate the detrimental effects of privacy invasions. Nudging refers to deliberate design decisions within choice environments that encourage or discourage the use of heuristics to influence peoples' behavior (Richard H Thaler & Sunstein, 2008). Nudging is based on the premise that individuals' decision making is irrational due to cognitive limitations and is influenced by the presentation of options within a choice environment (C. Schneider et al., 2017; Sunstein, 2014; Weinmann et al., 2016). The reliance on heuristics and the influence of psychological effects such as cognitive biases (e.g., loss aversion) and social influences (e.g., herding effects) leads individuals to making predictable mistakes and often to making decisions to their disadvantage (Fleischmann, Amirpur, Benlian, & Hess, 2014; Gilovich et al., 2002). Taking the latter into consideration, nudging aims to deliberately design choice environments to affect human behavior while respecting individual freedom of choice (Kahneman, Knetsch, & Thaler, 1991; Richard H Thaler & Sunstein, 2008). This concept has been recently translated into digital choice environments where digital nudging aims to shape user-interface design elements to guide users' decision-making predictably without forbidding any options or significantly changing their economic incentives (Adam, Wessel, & Benlian, 2019; Alexander Benlian, 2015; Fleischmann, Amirpur, Grupp, Benlian, & Hess, 2016; Wessel, Adam, & Benlian, 2019).

Social nudges are defined as nudges specifically based on the effect of social influences to promote desirable choices (Kretzer & Maedche, 2018). According to Mirsch et al. (2017), social influences are one of the most important psychological mechanisms that can be utilized for

digital nudging. Social influence refers to the way individuals change behavior in direct response to unwritten social laws (Cialdini & Goldstein, 2004). These social influences can be categorized by the influence motivation type and by the influence's process of change: The type of influence motivation, can be distinguished into informational and normative, whereby the former is based on the desire to form an accurate interpretation of reality and behave correctly, and the latter is based on the goal of obtaining social approval from others (Cialdini & Goldstein, 2004). Normative influences are most effective when the decision making is exposed to others. Research has proven three distinct paths through which social influences change a person's behavior or cognitions (i.e., opinions, thoughts, and feelings), namely identification, compliance, and internalization (Cialdini & Garde, 1987; Cialdini & Goldstein, 2004; Kelman, 1958). Identification refers to the changing of attitudes or behaviors due to the influence of someone who is admired. Compliance refers to the act of responding favorably to an explicit or implicit request offered by others which leads to changes in behavior but not necessarily in cognition (Freedman & Fraser, 1966; Kelman, 1958). Lastly, internalization refers to the act of accepting an influence because it is intrinsically rewarding (i.e., in accordance with a person's value system) and thus changes an individual's behavior and cognition (Cialdini & Goldstein, 2004). Scholars have leveraged the effectiveness of normative and informational social influences in various digital contexts (e.g., Chu & Kim, 2017; Hogg & Lerman, 2014; J. Lu, Yao, & Yu, 2005). In this regard, previous research has demonstrated that computer agents can act as social actors, and therefore social influences even apply with internet-anonymity (Cialdini & Goldstein, 2004; Guadagno & Cialdini, 2005; Maedche et al., 2019; Nass, Steuer, & Tauber, 1994). However, research has predominantely focused on the antecedents of social influences and how they alter decision processes (Cialdini & Goldstein, 2004; Kelman, 1958; J. Lu et al., 2005; Todri & Adamopoulos, 2014; Venkatesh & Morris, 2000), and less on how social influences can be utilized to design digital nudges for choice environments (Kretzer & Maedche, 2018). Therefore, this research follows Kretzer and Maedche (2018), and Mirsch et al. (2017) by refining and designing concrete social nudges and by demonstrating and testing their effects for privacy-related decision making. Thus, this research demonstrates how social nudges can be integrated into privacy choice environments as mitigating technology features.

2.4 Thesis Positioning

In order to answer the overarching research questions, we draw on three articles. The first research question aims to demonstrate how intrusive technology features affect critical outcomes through privacy-related stressors. The second research question aims to assess how social nudges can moderate the effect of intrusive technology features on privacy-related

outcomes as mitigating technology features. This thesis is structured as follows: an introductory chapter, a chapter that establishes the theoretical foundation, three chapters that present the published articles as shown in Table 1, and a final chapter that concludes with theoretical and practical contributions. As depicted in Figure 2, the following three chapters represent each of the articles.

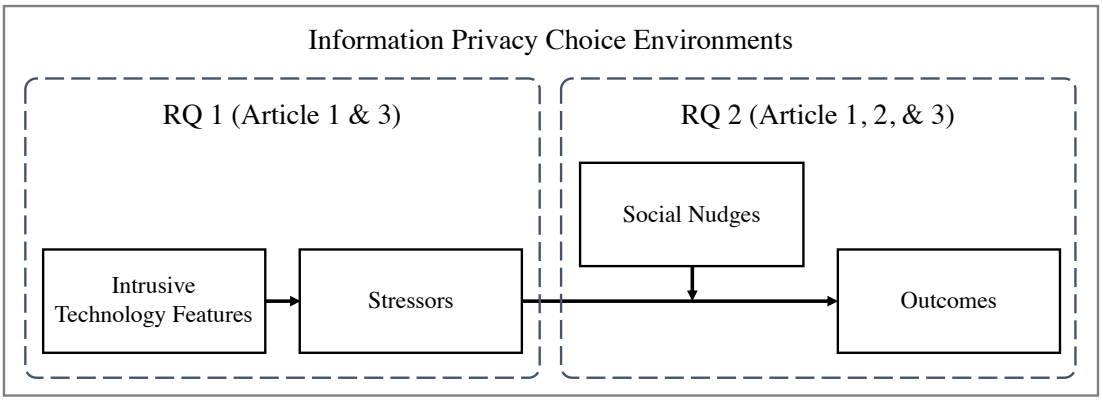


Figure 2: Overarching Article Contributions.

Chapter 3: Smart Home Assistants with Intrusive Technology Features and their Interaction with Anthropomorphic Features

Title: Mitigating the Intrusive Effects of Smart Home Assistants with Anthropomorphic Features: A Multi-Method Investigation

Authors: Alexander Benlian, Technische Universität Darmstadt, Germany
Johannes Klumpe, Technische Universität Darmstadt, Germany
Oliver Hinz, Goethe Universität Frankfurt, Germany

Published in: Information Systems Journal, forthcoming.

Abstract

With the growing proliferation of Smart Home Assistants (SHAs), digital services are increasingly pervading people's private households. Through their intrusive features, SHAs threaten to not only increase individual users' strain but also impair social relationships at home. However, while previous research has predominantly focused on technology features' detrimental effects on employee strain at work, there is still a lack of understanding of the adverse effects of digital devices on individuals and their social relations at home. In addition, we know little about how these deleterious effects can be mitigated by using IT artifact-based design features. Drawing on the person-technology fit model, self-regulation theory and the literature on anthropomorphism, we used the synergistic properties of an online experiment (N=136) and a follow-up field survey with a representative sample of SHA users (N=214) to show how and why SHAs' intrusive technology features cause strain and interpersonal conflicts at home. Moreover, we demonstrate how SHAs' anthropomorphic design features can attenuate the harmful effects of intrusive technology features on strain by shaping users' feelings of privacy invasion. More broadly, our study sheds light on the largely under-investigated psychological and social consequences of the digitization of the individual at home.

Keywords: smart home assistants, intrusive features, anthropomorphism, privacy invasion, technostress, interpersonal conflict, digitization of the individual, person-technology fit, self-regulation theory, multi-method approach

3.1 Introduction

Smart Home Assistants (SHAs) such as Amazon Echo or Google Home, which typically come in the form of voice command devices with an integrated virtual assistant, have increasingly penetrated consumer households in recent years because of their interactive and easy-to-use digital services. Users interact with SHAs primarily via a voice user interface that acquires information via microphones and provides information through audio speakers. Typical uses for SHAs are playing music, ordering products, controlling connected smart home devices (e.g., kitchen appliances, heating, lighting, security alarms), and acquiring weather, traffic and other real-time information. In addition, SHA service providers integrate third-party services such as ridesharing (e.g., Uber) and audio books or music (e.g., Audible, Spotify) to add value for users. Over 40 million US Americans have already adopted SHAs: this means that roughly one in every six homes in the US has an SHA, with an expected growth rate of 129% in 2017 alone (Perez, 2018; Richter, 2017). IDC projects worldwide SHA sales to increase from $4.4 bn to $17.4 bn by 2022 (Kinsella, 2018), indicating that the digitization of individuals and their homes is inexorably on the rise. Despite their merits, SHAs are met with consumer skepticism regarding the amount of information that is collected and processed by their voice user interfaces. As a recent example, SHAs have attracted considerable attention when a police murder investigation had to draw on information collected by an SHA that was listening during the incident (Buhr, 2016). Thus, the voice processing abilities of SHAs have become rather infamous, thus confronting service providers with a challenging trade-off between protecting users' information privacy and personalizing information (Hatmake, 2017). As providers strive to personalize their services, they acquire and process vast amounts of data to improve the intelligence of their virtual assistants and thus their digital services. Potential negative consequences for consumers, such as the invasion of privacy, are often left out of the equation by SHA and third-party service providers, begging the question of how SHAs' intrusive technology features—manifested in technology presenteeism (i.e., the degree to which individuals are reachable and accessible) and technology anonymity (i.e., the degree to which individuals' technology use is identifiable)—can be attenuated to reduce the individual strain that often goes along with privacy infringements (Ayyagari et al., 2011).

Despite the pervasiveness and severity of such intrusive technology features, previous IS research has mainly focused its investigations of technology stress on the work domain by examining how and why technostressors—a concept defined as stress experienced by end users in organizations as a result of their use of and greater dependence on information and communication technologies (ICT)—affect work outcomes and how the counterproductive

effects of those technologies can be mitigated in organizations (e.g., T. S. Ragu-Nathan, Tarafdar, Ragu-Nathan, & Qiang, 2008; Tarafdar et al., 2007). Although these insights are valuable because they shed light on the effects of technostress in our working lives and how we can cope with the dark side of ICT at work, our understanding of how specific technology characteristics create stress at home and how these detrimental effects can be mitigated is still far from complete (Tarafdar, Cooper, & Stich, 2019). This knowledge gap comes as a surprise, given that IS scholars have not only provided initial findings that (abstinence from) non-work technology use (e.g., social media use) in the home environment can significantly affect stress and well-being (Krasnova, Widjaja, Buxmann, Wenninger, & Benbasat, 2015; Ofir Turel, Cavagnaro, & Meshi, 2018). They have also pointed to the importance of examining specific technology characteristics and their stress-inducing effects in the home domain (Ayyagari et al., 2011) and extending research on the adverse effects of the digitization of individuals in their private lives (O. Turel, Cheung, Matt, & Trenz, 2018).

Furthermore, while the majority of previous technostress studies have placed the focus squarely on individual, within-person outcomes such as strain, performance, or satisfaction (e.g., Ayyagari et al., 2011; T. S. Ragu-Nathan et al., 2008; Tarafdar et al., 2010), minimal attention has been paid to outcomes that go beyond individuals to include their social relationships at home. Given the strong and far-reaching consequences of intrusive technology features, it seems critical to seriously consider the wider social implications of digital devices at home and how their potentially harmful effects could be counterbalanced.

In light of these research gaps, the objective of this paper is to shed light on how SHAs' intrusive technology features affect strain (i.e., the ultimate form of psychological stress) and interpersonal conflicts (i.e., social impairments) at home by heightening feelings of privacy invasion. Given that previous research and practitioner-based studies have repeatedly indicated that technological artifacts can trigger and increase feelings of privacy invasion because they are considered artificial and impersonal machines (e.g., Hauk & Padberg, 2016; Qiu & Benbasat, 2009b), our study also focuses on the anthropomorphic features of SHAs (i.e., features that imbue nonhuman agents with humanlike capabilities to create trust) that may serve as potential buffers against the adverse effects of intrusive technology features. SHAs usually come in a cylindrical or cubistic shape to blend into households like ordinary speakers (e.g., Apple's Homepod). However, companies have more recently started to adopt anthropomorphized characteristics (e.g., smiling face, curved body shape, human speech synthesizing) to facilitate more humanlike virtual assistant experiences (e.g., Jibo. Applying

anthropomorphic design features to SHAs' voice interfaces and body shapes creates the theoretically intriguing possibility that SHAs will be perceived as pals rather than as perpetrators, enabling them to establish more trusting relationships with their SHA users (Mourey, Olson, & Yoon, 2017). Despite their theoretical and practical relevance, however, previous IS research has so far neglected the role of such anthropomorphic design features as potential moderators of privacy invasion, thus leaving a gap in the literature that is both important and interesting to address. In light of the abovementioned gaps and calls for future research, we ask the following two research questions:

RQ1: What is the impact of SHAs' intrusive technology features on individuals' strain and interpersonal conflicts at home?

RQ2: How do anthropomorphic design features influence the potential relationship between SHAs' intrusive technology features and individual strain?

To examine our research questions, we used a multi-method approach with two studies, including a vignette-based online experiment (N=136) and a follow-up field survey (N=214). In doing so, we were able to improve the validity of our research by countering the limitations and trade-offs inherent in each method. Drawing on the person-technology fit model, self-regulation theory and literature on anthropomorphism, we investigated whether and how SHAs' intrusive technology features produce strain and interpersonal conflict at home and why anthropomorphic design features may attenuate the detrimental effects of intrusive technology features on strain by shaping users' perceptions of privacy invasion. The complementary features of an online experiment and a field survey allowed us to show that SHAs' intrusive technology features (i.e., unintentional voice activation, low user anonymity, and high presenteeism) can increase feelings of privacy invasion, which in turn may heighten individual strain and interpersonal conflicts at home. At the same time, we found converging empirical evidence across our two studies, lending credence to the robustness of our overall findings that anthropomorphic design features can cancel out the negative effect of privacy invasion on user strain.

Our study contributes to research on technology stress and the digitization of the individual in several important ways. First, we extend previous research on technology-induced stress from the work to the home domain and broaden the focus of this stream of research to include individual and social consequences at home. While previous research on technology characteristics and technology-induced stress has largely focused on consequences for

employees in work settings (Srivastava et al., 2015; Tarafdar et al., 2015), the more far-reaching effects on individuals and their social environment at home have received only scant attention so far. Second, by investigating the role of anthropomorphic design features in mitigating the intrusive effects of SHAs, we integrate the person-technology fit model and the literature on anthropomorphism to show that technology characteristics not only induce stressors (i.e., privacy invasion) but also serve as resources for coping with such stressors. Third, more broadly, by looking at the privacy invasion of the digitized individual and factors that modulate the adverse influence of digitization on individuals, we answer Turel et al.'s (2018) call for research into the largely unaddressed psychological and social consequences of digital technologies for individuals and their relationships at home.

3.2 Theoretical Background

3.2.1 Person-Technology-Fit Model and Intrusive Technology Features

We draw on the person-technology (P-T) fit model advanced by Ayyagari et al. (2011) as a theoretical foundation on which to examine the effects of SHAs on strain and interpersonal conflicts with other household members. The P-T fit model is derived from the broader, well-established person-environment fit theory (Jeffrey R Edwards, 1991; Jeffrey R. Edwards, 1996) and integrates the sequence of "(Individual perceptions of) technology characteristics → stressors → strain (and other outcomes)" into its foundational nomological network. A key premise of the P-T model is that individuals live in an equilibrium relationship with their technological environment (e.g., individuals in a digitized household). If this relationship is out of equilibrium, the imbalance or misfit causes stress outcomes such as strain, which refers to individuals' psychological and behavioral responses to stress, including dissatisfaction, anxiety, and withdrawal (Ayyagari et al., 2011; Jeffrey R Edwards, Cable, Williamson, Lambert, & Shipp, 2006). More specifically, individuals' evaluation of the extent of gap or misfit (also called perceived misfit) between the characteristics of the person and the technology can lead to unmet individual needs or desires that typically manifest in stressors (i.e., demands encountered by individuals), eventually leading to strain or other adverse outcomes (Cooper et al., 2001).

With the aim of developing a comprehensive P-T fit model, Ayyagari et al. (2011) integrated a diverse set of technology characteristics (i.e., usability, intrusive, and dynamic features) and stressors (i.e., work-home conflict, invasion of privacy, work overload, role ambiguity, and job insecurity) into the model. In the current study, given that our main theoretical interest lies in the intrusive effects of SHAs on individual users and their relationships in the home context,

we focus on intrusive technology features of the P-T fit model, which are the most pertinent technology characteristics to the phenomenon under study (Ayyagari et al., 2011). Previous research has shown that in light of their increasing ubiquity in work and home environments, intrusive technology features are particularly critical if we want to gain a better understanding of the consequences of technology use (Maier, Laumer, Eckhardt, et al., 2015). According to Ayyagari et al. (2011), intrusive technology features reflect information technologies' invasiveness and include technology presenteeism (i.e., the degree to which technologies enable individuals to be reachable) and technology anonymity (i.e., the degree to which technology makes users trackable and identifiable) as two main indicators of invasiveness. While presenteeism and anonymity refer to broad intrusive technology features, IS scholars have pointed to the need for future research into specific and context-related intrusive technology features (Ayyagari et al., 2011; C. Speier, I. Vessey, & J. S. Valacich, 2003). Responding to this call, in addition to presenteeism and anonymity, we include SHAs' voice user interface as a specific source and driver of technology intrusiveness and specifically examine the role of unintentional voice activation in affecting individual strain. Unlike other potential intrusive technology features (e.g., unsolicited targeted ads, unprompted recommendations of third-party skills, default configurations to connect to SHA providers' other services), unintentional voice activation of SHAs is not only perceived as one of the most privacy-invasive and consequential phenomena in practice, as reported in a series of highly publicized cases about SHAs' privacy infringements in households worldwide (Lau, Zimmerman, & Schaub, 2018; Morley, 2017; Warren, 2018). It also strikes at the core of privacy concerns and the question of whether users feel that SHA providers encroach upon users' private lives in a distressing way, which is a key theoretical focus of this study.

Furthermore, due to our focus on intrusive technology features and their invasive effects in users' homes, we are particularly interested in investigating the invasion of users' privacy at home as a stressor of the P-T fit model (Ayyagari et al., 2011). Invasion of privacy refers to individuals' perception that their privacy has been compromised, making it theoretically the most adequate stressor to capture fit or misfit between the demands of intrusive technology features and the privacy needs of users (Alge, 2001; Ayyagari et al., 2011). Previous literature has highlighted the invasion of privacy as one of the most important theoretical mechanisms explaining stress outcomes at work and at home (Jeffrey R Edwards, 1991; Jeffrey R Edwards & Cooper, 1988a). Given that the privacy-invading effects of digital technologies do not stop at the user but often spillover to other members of the household, the social environment of technology users is also affected by privacy invasion and underlying technology characteristics,

leading to a blending of external and home demands (Hammer, Bauer, & Grandey, 2003; Hawk, Keijsers, Hale III, & Meeus, 2009). Thus, the social environment of technology users is arguably just as important to study as technology users themselves, but it has received much less attention in research on the dark side of information technology (D'Arcy, Gupta, Tarafdar, & Turel, 2014; Tarafdar et al., 2019). Indeed, although technostress research to date has mostly focused on individual strain as an outcome, perceived misfits or imbalances have also been linked to the impairment of social relationships via the resource-depleting effects of stressors and corresponding self-control failures (Luchies, Finkel, & Fitzsimons, 2011).

3.2.2 Self-Regulation Theory and Interpersonal Conflict

While studies of outcomes of P-T misfit and resulting stressors have largely focused on individual strain, previous research has also considered a broader range of outcomes because individuals are embedded in social networks and their roles are tied to others through various relationships (e.g., marital relationships, coworker ties) that exist in each domain (Takac, Hinz, & Spann, 2011). In this regard, stressors that individuals experience in their work or home domains lead not only to intrapersonal strain (i.e., strain within the person) but also to interpersonal strain or conflict that may have adverse effects on an individual's social relationships with other people in those domains (Hong Deng, Coyle-Shapiro, & Yang, 2018; Pseekos, Bullock-Yowell, & Dahlen, 2011). The main reasoning behind these potentially negative effects on social relationships is that stressors resulting from P-T misfit carry self-regulatory consequences (H. Deng, Wu, Leung, & Guan, 2016).

Self-regulation theory suggests that individuals have a limited pool of resources available (e.g., energy, time) that they need to sustain attention and block out distracting information in order to perform properly in the roles they assume in work and private life (Muraven & Baumeister, 2000). In this regard, role performance refers to how well one fulfills the general demands and responsibilities associated with a particular role, which is a function of the amount of resources devoted to that role (Frone, Yardley, & Markel, 1997). When individuals experience a stressor in their environment, they are more likely to suffer from resource depletion (just as a muscle becomes fatigued from exertion) because coping with a stressor involves cognitive rumination and emotion regulation, all of which consume resources (Baumeister, Vohs, & Tice, 2007). According to this "muscle model" (also called the strength model) of self-control (Baumeister et al., 2007), resource drain decreases individuals' self-control, which refers to the capacity to alter or override dominant response tendencies and to regulate behavior, thoughts, and emotions (R. E. Johnson, Lin, & Lee, 2018). Individuals exert self-control when they, for example, resist

impulses to check social media repeatedly or strive to remain focused on work tasks despite interruptions from technology. Another more recent theoretical account of self-control failure is the "process model" (Brevers et al., 2018; Inzlicht & Schmeichel, 2012), according to which people constantly switch between interest in "have-to" work (i.e., tasks that are often demanding and performed out of a sense of duty) and cognitive "want-to" leisure (i.e., tasks that are enjoyable and easy to perform). In line with this explanation, resource depletion stems from the individual tendency to rotate between mentally demanding tasks and more rewarding (or less effortful) activities, a rotation that can have important implications for individuals' attentional and motivational resources. Taken together, both the "muscle model" and "process model" of self-regulation failure provide valuable theoretical underpinnings for a resource depletion effect.

Self-regulation theory goes on to suggest that as a result of resource depletion, people strive to protect their resources by engaging in avoidance and withdrawal behaviors to protect themselves from further damage and loss (Halbesleben, 2006). This resource protection tendency in turn increases the likelihood of individuals subtracting time and effort from behaviors associated with adequate interpersonal functioning, such as catering to the needs of partners and family members (de Ridder, Lensvelt-Mulders, Finkenauer, Stok, & Baumeister, 2012). Indeed, several empirical studies have shown that depleted self-regulatory resources have adverse consequences for relationship functioning. For example, compared to their non-depleted counterparts, depleted individuals tend to respond to partner requests less constructively, exhibit more aggressive behaviors, and take credit for success but deny responsibility for failure, all of which increase the likelihood of interpersonal conflict (DeWall, Baumeister, Stillman, & Gailliot, 2007; Finkel, DeWall, Slotter, Oaten, & Foshee, 2009; Luchies et al., 2011). The detrimental effects of resource-depleting stressors on social relationships are also supported by literature on work-family conflict (Amstad, Meier, Fasel, Elfering, & Semmer, 2011; Byron, 2005), which is defined as a "form of interrole conflict in which the role pressures from the work and family domains are mutually incompatible in some respects" (Greenhaus & Beutell, 1985), p. 77). Work-family conflict usually occurs when one's efforts to meet the demands of one's work role interfere with one's efforts to fulfill family demands, and vice versa. Recent research has suggested that work-home conflict can be translated into other interrole conflicts, such as that between the ICT user role and the family role (Piszczek, Pichler, Turel, & Greenhaus, 2016). According to this view, stressors or strain generated in the ICT user role can spill over into the family role, affecting the latter role in an adverse way by diminishing role performance and increasing interpersonal conflict (Barber,

Taylor, Burton, & Bailey, 2017). Taken together, self-regulation theory and the corresponding literature on work-family conflict serve as appropriate theoretical lenses through which to depict privacy invasion as a resource-depleting stressor that can be transmitted from the ICT user role to the family role to create conflict.

While one of our research objectives is to expand the criterion space of the P-T fit model to include interpersonal outcomes at home, we also aim to extend previous technostress research by incorporating moderating mechanisms that are likely to mitigate the harmful effects of privacy invasion on strain. Previous research drawing on the P-T fit model has primarily focused on establishing the main and mediation effects among technology characteristics, stressors and strain (Maier, Laumer, Eckhardt, et al., 2015). However, that research has largely neglected to study potential moderating effects, even though Ayyagari et al. (2011) have called for explicitly examining the coping mechanisms that moderate an individual's reactions to stressors. In the current research, we suggest anthropomorphic technology features as potential coping mechanisms, to which we turn next.

3.2.3 Anthropomorphic Technology Features

Anthropomorphism is the attribution of human-like physical or non-physical features, behaviors, emotions, and characteristics to a non-human agent or to an inanimate object (Pankaj Aggarwal & McGill, 2012; Pfeuffer, Benlian, Gimpel, & Hinz, 2019). Humans have integrated anthropomorphic features into products since behavioral modernity (50,000-10,000 BC; (Trinkaus, 2005). For example, paintings from approximately 30,000 years ago depict animals with a human-like appearance, which is the first known expression of anthropomorphism in art (Dalton, 2004). This usage of anthropomorphism to facilitate understanding and personification with a non-human agent is still an established measure in literature and art in modern times, especially in children's literature and movies (Lanier, Rader, & Fowler, 2013). Because humans are accustomed to attributing human-like characteristics and emotions to non-human agents from early childhood, it is no surprise that consumer research has discovered anthropomorphism as a design pattern for products and has started to study the psychological consequences of engaging with anthropomorphic products (Wen, Peng, & Jin, 2017). Anthropomorphic versions of consumer products have, for example, been shown to elicit greater moral care from consumers and greater trust in non-human technological products such as polygraph tests and autonomous vehicles (Waytz, Heafner, & Epley, 2014). Additionally, the literature has revealed that consumers develop greater trust in anthropomorphized products by establishing an emotional relationship to non-human agents (Mourey et al., 2017; Touré-

Tillery & McGill, 2015). Scholars have also explicated that anthropomorphism is rooted in sociality motivation, which describes humans' fundamental need for social approval, social connectedness, and social contact with other humans and with non-human agents (Pankaj Aggarwal & McGill, 2007; Epley, Waytz, & Cacioppo, 2007).

Anthropomorphism in humanoid, hardware- and/or software-based agents has also been the subject of investigation in robotics and human-robot interaction for some time. In this regard, a fundamental theory that synthesizes much of what has been examined is the uncanny valley model and its extensions (Mathur & Reichling, 2016; Mori, 1970; Mori, MacDorman, & Kageki, 2012). This model hypothesizes that a person's response to a humanlike robot will abruptly shift from empathy and acceptance to revulsion as the robot approaches, but does not quite replicate, a high level of human likeness. The valley thereby denotes a dip in the person's affinity for and positive emotional reactions to the robot, a reaction that otherwise increases at low to medium and at very high levels of the robot's human likeness (Burleigh, Schoenherr, & L. Lacroix, 2013). While the uncanny valley has become increasingly relevant in the past few years because robots that actually look and move like humans are starting to become a reality, previous research largely focused on industrial robots that were examined in rather artificial lab experiments. Research scholars thus have yet to fully embrace whether and how anthropomorphic features in new digital devices and services (e.g., SHAs or chatbots) harm or help individuals in their private lives at home (Ciechanowski, Przegalinska, Magnuski, & Gloor, 2019).

Anthropomorphism at the human-computer interface is typically triggered by anthropomorphic features that are embedded in the design of the hardware (e.g., human body shape of a smartphone) or software (e.g., display of a smile or the sound of a human voice) of the IT artifact and are usually transmitted via visible or auditory cues (Qiu & Benbasat, 2009b). Previous IS research has largely focused its investigations of anthropomorphism on facilitating the interaction between users and a software system by designing virtual agents' appearance and behavior, such as avatar dimensionality, communication modalities, and facial expressions (e.g., Nunamaker, Derrick, Elkins, Burgoon, & Patton, 2011; Qiu & Benbasat, 2009b; Riedl, Mohr, Kenning, Davis, & Heekeren, 2014). These designs have been examined in various application fields, such as e-commerce, e-learning, and security (e.g., Al-Natour, Benbasat, & Cenfetelli, 2006; Chae, Lee, & Seo, 2016; Pickard, Burgoon, & Derrick, 2014). While the majority of this body of research has supported the view that avatar-based communication increases perceived interpersonal trust, the IS literature has been silent about how

anthropomorphic design features affect users' privacy concerns in the face of intrusive technology features.

When considered together with intrusive technology features, the relatively separate literature on user privacy and anthropomorphism suggests an interesting interplay between technology-driven invasion of privacy and the potential coping capacities offered by anthropomorphic design features. More specifically, what has been missing in the literature is the degree to which privacy invasion and anthropomorphic design features interact such that the latter could potentially interfere with the harmful effects that typically follow experiences of the former. In this study, we propose that the intrusive features of SHAs will create individual strain through privacy invasion unless users have the opportunity to engage with an SHA that has anthropomorphic design features. Our underlying rationale is that anthropomorphic design features can mitigate the adverse effects of the invasion of individuals' privacy, created through SHAs' intrusive features, on individual strain.

It is important to note here that according to Ayyagari et al. (2011)'s P-T fit model, the term technology characteristics refers to individuals' perceptions or assessment of attributes or features of a particular ICT rather than what the ICTs are objectively composed of, as it is primarily individuals' perceptions of technology features that trigger stressors and their downstream consequences (A. Benlian, 2015). To remain consistent with this conceptualization, when referring in this paper to intrusive technology features (i.e., unintentional voice activation, high presenteeism, low anonymity) and anthropomorphic design features, we are referring to individuals' perceptions and assessment of these features.

3.3 Hypotheses Development

Drawing upon the P-T fit model as a theoretical foundation that builds on the sequence "(individual perceptions of) technology characteristics → stressors → strain and other outcomes" (Ayyagari et al., 2011), we develop a research model that first sheds light on the effects of intrusive technology features of SHAs (i.e., unintentional voice activation, high presenteeism, low user anonymity) on potentially detrimental outcomes at home (i.e., strain and interpersonal conflicts), with privacy invasion being the central theoretical mechanism (i.e., stressor) underlying these intrusive effects. We then continue by theorizing the moderating influence of anthropomorphic design features on the indirect effect of intrusive technology

features on strain[1] via privacy invasion. We expound upon each of the posited relationships[2] depicted in our proposed research model in Figure 3 in the following sections.

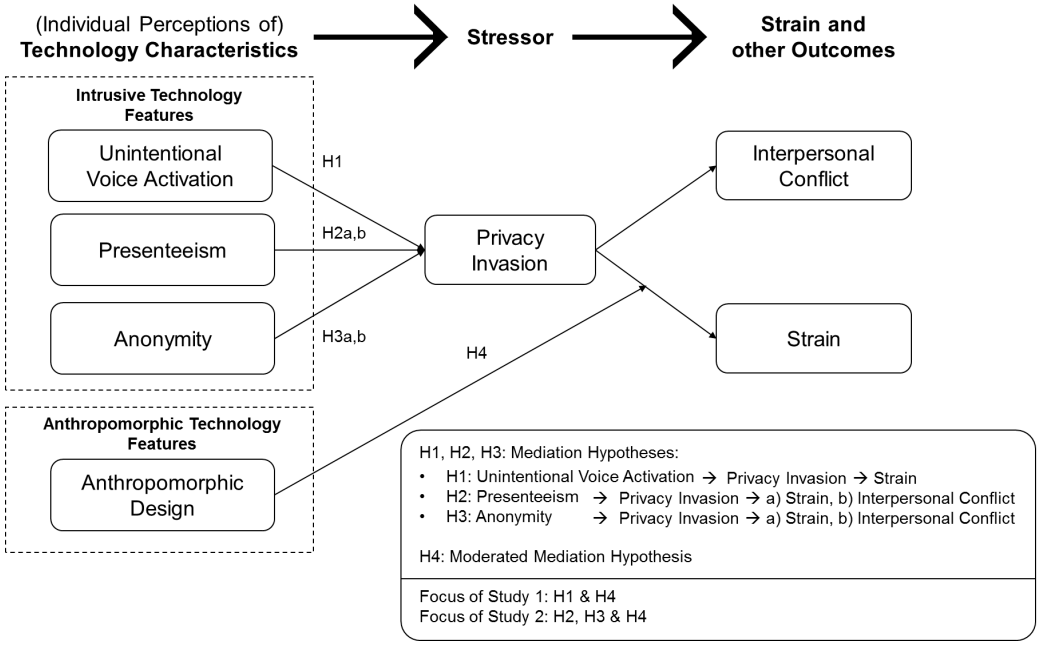


Figure 3: Proposed Research Model.

3.3.1 The Intrusive Effects of Unintentional Voice Activation Through Privacy Invasion

SHAs usually employ sophisticated voice processing interfaces that are triggered or activated by a vocal wake-up keyword (e.g., "Alexa" or "Hey Google") to acquire information from and provide information to users. The intrusiveness of SHAs' voice processing interfaces can be considered potentially high, as they not only have to constantly listen to users' personal environment in order to be activated but also can make mistakes in the form of unintentional activations, which can be a major source of disturbances and privacy concerns at home (Wueest, 2017). That is, although the recognition of a trigger keyword relies on a sophisticated training model (usually based on machine-/deep-learning methods), SHAs are still prone to so-called false-positives (i.e., the false identification of a keyword), which cause unintentional voice

[1] We did not hypothesize potential moderating effects of anthropomorphic design on the privacy invasion–interpersonal conflict relationship because anthropomorphic design features at the user interface mainly affect the SHA user directly and are less likely to affect interpersonal conflicts with other home members indirectly.

[2] It is important to note here that in our multi-method approach with two studies, the focus of study 1 was to establish the causal baseline relationship between one single intrusive technology feature, using unintentional voice activation as an SHA-specific instance, and strain via privacy invasion, and the moderating effect of anthropomorphic design on the privacy invasion-strain relationship. To broaden the scope of these baseline insights, we used study 2 to investigate more general and established intrusive technology features (i.e., presenteeism, anonymity) and their impact on a relationship-related outcome (i.e., interpersonal conflict) above and beyond individual strain. Given this approach, we did not hypothesize and examine the effect of unintentional voice activation on interpersonal conflict (via privacy invasion) in our two studies.

activations. These unintentional voice activations have been found to increase feelings of privacy invasion because they imply that SHA providers might collect information about users and their behaviors in an inconspicuous manner in order to create detailed user profiles that they might share with third-party service providers and advertising companies (Watkins Allen, Coopman, Hart, & Walker, 2007; Wueest, 2017).

Such potential privacy violations after unintentional voice activations are likely to be at odds with users' privacy needs and values, creating a misfit between technology demands and individual needs, which in turn increases the likelihood of higher individual strain (Ayyagari et al., 2011). More specifically, the underlying rationale for the potentially harmful effects of unintentional voice activation on strain is that accidental activation of a voice user interface obfuscates the amount of personal information disclosed to service providers. This, in turn, negatively affects users' perceived control over their information and heightens privacy concerns (Dinev, Xu, Smith, & Hart, 2013; Klumpe, Koch, & Benlian, 2019b). In this regard, previous literature has also shown that when a user has no control over the information that is disclosed to a service provider, they feel invaded in their privacy, are less likely to use the service, and perceive higher strain (Ayyagari et al., 2011; H. Xu & Gupta, 2009). According to the previous arguments and empirical findings, we thus hypothesize the following:

H1: *Unintentional (vs. intentional) voice activation has a positive indirect effect on SHA users' strain through privacy invasion.*

3.3.2 The Intrusive Effects of High Presenteeism Through Privacy Invasion

Technology presenteeism (hereafter 'presenteeism' for simplicity) has been defined as the degree to which a technology makes users reachable (Ayyagari et al., 2011). The premise is that through varying degrees of connectivity of technological devices, users are more or less accessible to the "anytime and anywhere" demands of the digital world. Studies have found that high presenteeism exacerbates users' inability to disengage from information technology (T. S. Ragu-Nathan et al., 2008; Tarafdar et al., 2007) and have shown that employees who are constantly reachable by their employer are more prone to burnout (McGee, 1996). Information technology is also considered a source of interruptions, leading to reduced efficiencies and higher stress (Tams, Thatcher, & Grover, 2018).

In our study, we contend that perceptions of high presenteeism induce strain through privacy invasion. With their always-on microphones, cameras and sensors, SHAs typically entail constant connectivity and reachability such that users may be accessible to SHA and service

providers anytime when they are at home (Mazmanian, 2013). Despite being sensitive to potential privacy violations, users most often, for convenience reasons, do not switch off their SHAs or their recording features, a situation often referred to in the literature as the privacy paradox (Corey M. Angst & Ritu Agarwal, 2009; Naveen Farag Awad & M. S. Krishnan, 2006). Thus, SHAs can be seen as gateways into users' intimate space, which is often in conflict with users' need for privacy in their households. To the extent that individuals acknowledge this discrepancy between their privacy needs and the omnipresence of technologies in their homes, and thus feel their privacy is being invaded, they are likely to feel higher strain. Empirical evidence corroborates this finding: presenteeism has been linked to perceptions of increased privacy invasion, which, in turn, has been found to be positively associated with strain (Ayyagari et al., 2011). In line with this reasoning and prior empirical evidence, we propose that SHA users' perception of technology presenteeism is positively related to individual strain because of heightened feelings of privacy invasion. The following hypothesis captures our theorizing:

H2a: *High (vs. low) presenteeism has a positive indirect effect on SHA users' strain through privacy invasion.*

Extrapolating from self-regulation theory as presented above, we expect that users interacting with their SHAs at home are also more likely to have interpersonal conflicts with other household members because of privacy invasion concerns that result from a misfit between users' preferences for presenteeism (i.e., reachability, accessibility) and their SHA's presenteeism demands. To obtain a tighter grip on user preferences and behaviors, SHAs increasingly penetrate users' homes with additional features (e.g., third-party apps such as Alexa's 'skills') and growing connections to network devices such as security, utility and entertainment systems (Crist & Gebhart, 2018). This expanding accessibility to external demands may, consciously or subconsciously, unsettle users about where they want to draw the boundary between technology presence and absence. Dealing with the feelings of privacy invasion that result from such an ongoing struggle between immersion into and detachment from the interaction with the SHA at home is likely to tax users' resources and drain their energy (A. Chen & Karahanna, 2018). Previous research has also shown that the interruptive nature of ICT and the constant attentional pull it exerts may go against users' privacy needs and produce inner conflicts that likely occupy users' mental capacity and deplete their resources (Tams et al., 2018). Being increasingly drawn into pervasive and interruptive ICT may, however, come at the cost of time and attention spent on nurturing social relationships and thus is likely to

increase social frictions with other household members (Roberts & David, 2016). The reduced attention and time invested in social bonding may lead to family members being offended by SHA users' absent-mindedness and to impaired communication quality, leading to greater interpersonal conflicts.

In addition, the constant rotation between what SHA users are preoccupied with in their ICT user role (i.e., finding the right balance of accessibility in their SHA use) and what they have to take care of in their family role (e.g., catering to family needs) may create interrole conflicts (Brevers et al., 2018; Piszczek et al., 2016). These conflicts may not only imply that users' time and attention are siphoned away from social behaviors at home that drive interpersonal satisfaction, such as fulfilling home responsibilities or spending time together. They may also imply that the feelings of privacy invasion that result from interaction with the SHA create strain that spills over to impair SHA users' relationships with other family members via increased aggressive impulses and interpersonal conflicts (Bakker & Demerouti, 2013). Because of the reasons and empirical findings mentioned above, we thus propose the following:

H2b: *High (vs. low) presenteeism has a positive indirect effect on SHA users' interpersonal conflict with other home members through privacy invasion.*

3.3.3 The Intrusive Effects of Low Anonymity Through Privacy Invasion

Technology anonymity (hereafter 'anonymity' for simplicity) denotes the degree to which an individual perceives that the use of information technology is not identifiable or cannot be tracked (Ayyagari et al., 2011). If, for example, an SHA user feels that the use of the SHA can be monitored, it represents low anonymity. Individuals are basically concerned about the possibility of invasive monitoring by organizations (e.g., Best et al., 2006). However, the pervasiveness of information technologies and previous major incidents have made individuals even more sensitive to potential privacy infringements in recent years (Dinev, McConnell, & Smith, 2016). Perusal of the literature on electronic monitoring and ubiquitous surveillance also shows that monitoring is stressful for employees and individuals (McNall & Roch, 2007; Posey, Bennett, Roberts, & Lowry, 2011). The underlying logic is that the capability of technologies to collect personal information about individuals and their behavior enables monitoring—which may be inconsistent with and violate individuals' values increasing their concerns over loss of privacy. This P-T misfit in turn increases individual strain.

Consistent with these arguments, we suggest that SHA users' perception of anonymity is essential for control over their personal information and the sanctity of their privacy. When

SHA users feel that it is becoming increasingly difficult to escape the data collection, storage, and processing performed by artificially intelligent SHAs (i.e., potentially enabling service providers to monitor their private lives and eavesdrop on them), they are more likely to feel greater strain because of a higher invasion of their privacy (and a greater misfit between technology demands and their need for privacy). Previous research has also found users to be more concerned about their privacy when they lose control over the timing of information disclosure and the amount of information they disclose (Dinev et al., 2013; Smith et al., 2011a). Based on this logic and in light of previous empirical evidence, we thus propose that SHA users' perception of anonymity is negatively related to individual strain because of lower feelings of privacy invasion.

H3a: *High (vs. low) anonymity has a negative indirect effect on SHA users' strain through privacy invasion.*

Similar to the theoretical arguments developed above, we suggest that concerns about privacy invasion resulting from a misfit between the anonymity needed by a user and the anonymity provided by the SHA will deplete users' personal resources (Ayyagari et al., 2011). This depletion may in turn undermine their interpersonal functioning and social behaviors at home (Trougakos, Beal, Cheng, Hideg, & Zweig, 2015). SHAs are equipped with increasingly sophisticated sensors, microphones, and artificial intelligence, all of which enhance SHAs' monitoring and processing capabilities (Lau et al., 2018). This enhanced transparency into users' private lives is likely to cause user distress about what data are collected and how they are processed, potentially leaked, or exposed to other third parties. Being preoccupied with potential anonymity breaches may however tap into SHA users' finite pool of resources and thus foster resource depletion, implying that time and attention are more likely "stolen" from the cultivation of social relationships with other home members. In other words, when SHA users suffer from depletion, their role performance may suffer at home. Consequently, they are more prone to violate relationship norms and expectations such that their social functioning is compromised, increasing the likelihood of interpersonal conflicts (Feeney, 2002). Indeed, previous research on electronic monitoring and surveillance has found that invasive monitoring can increase anxiety, antisocial behaviors, and social conflicts because of nagging privacy concerns (McNall & Roch, 2007; Oulasvirta et al., 2012).

Furthermore, constantly oscillating between the challenges posed by SHAs' potential anonymity violations and the demands of meeting home responsibilities may increase resource depletion and the likelihood of interpersonal conflicts (Brevers et al., 2018). More specifically,

dealing with potential anonymity breaches in the ICT user role may create strain that is carried over to the family role, where it is likely to translate into interpersonal strain with other family members (Sanz-Vergel, Rodríguez-Muñoz, & Nielsen, 2015). In light of these arguments and earlier empirical findings, we thus suggest that low anonymity through SHAs leads to users feeling a sense of heightened privacy invasion, which in turn increases interpersonal conflicts between SHA users and other household members. Conversely, high anonymity should result in lower interpersonal conflicts through diminished concerns about privacy invasion. We thus propose the following:

H3b: *High (vs. low) anonymity has a negative indirect effect on SHA users' interpersonal conflict with other home members through privacy invasion.*

3.3.4 The Moderating Effect of Anthropomorphic Design Features

As mentioned earlier, anthropomorphism is defined as imbuing non-human agents with human-like attributes (Eyssel, Hegel, Horstmann, & Wagner, 2010). Previous literature on the effects of anthropomorphic features in non-human agents has consistently found that anthropomorphic designs—especially when they do not resemble humans too closely (Mori et al., 2012)—give humans a familiar feeling because they can establish a natural and personal connection with the non-human agent (Burgoon et al., 2000; Epley et al., 2007). Qui & Benbasat (2009b), for example, found in a laboratory experiment that using humanoid embodiments of product recommendation agents increases users' perceptions of social presence, which in turn enhances users' trusting beliefs towards the agents.

Applying this logic to the context of SHAs, we argue that anthropomorphic design features of SHAs are likely to attenuate SHAs' intrusive effects on individual strain via privacy invasion. While one may hold that anthropomorphic design features amplify the adverse effect of privacy invasion on strain because they can heighten users' concerns about SHAs acting as indiscreet perpetual listeners, we propose the opposite. Previous research has predominantly found that anthropomorphic design features increase users' perceptions of social presence such that SHAs are likely to be perceived as pals rather than as perpetrators (Mourey et al., 2017; Qiu & Benbasat, 2009b). The underlying reasoning is that the feelings of familiarity and personal connection created through anthropomorphic design features may override potential sources of anxiety and distrust towards the SHA. Therefore, perceptions of higher social presence are likely to increase trust in the SHA such that anthropomorphic design features should attenuate the negative effects of privacy invasion on individual strain.

Previous literature has demonstrated how positive anthropomorphic schemas can enhance trust and consumers' liking of a product (Pankaj Aggarwal & McGill, 2007; Waytz et al., 2014). For example, scholars have provided evidence for how a human-like face on a non-human agent may improve the human-agent relationship. Landwehr et al. (2011) found that the anthropomorphic shape of a car's grille, perceived as a smile, positively influenced perceptions of the car's friendliness, indicating that thoughtful design of key elements of a product could lead consumers to project human-like mental states and characteristics on the product, increasing its likeability and trustworthiness. Moreover, S. Kim and McGill (2011) have shown that users feel more powerful in the presence of anthropomorphized machines and thus believe that they have more control over them, reducing behavioral uncertainty and concerns vis-à-vis machines. In previous research on the "computers-as-social actors" paradigm, Nass, Fogg, and Moon (1996) also found that users apply social heuristics in interactions with computers that are imbued with human or social cues, leading users to display more socially appropriate manners and better cope with potential privacy concerns.

Considering the mediation hypotheses 1, 2a and 3a related to strain, along with prior mediated moderation studies (Jeffrey R Edwards & Lambert, 2007), we thus propose a mediated moderation model. Given the above arguments and empirical evidence, our model suggests that anthropomorphic design features attenuate the effects of privacy invasion—created through the intrusive effects of SHAs—on strain. That is:

H4: *The indirect effect of SHAs' intrusive technology features on strain through privacy invasion is moderated such that anthropomorphic design features attenuate the negative effect of privacy invasion on strain.*

3.4 Research Studies and Results

3.4.1 Rationale for Multi-Method Approach

We employed a multi-method approach including two independent studies to examine the hypotheses in our proposed research model (see Figure 3). The first was an experimental vignette study (Study 1) with a convenience sample of experienced and predominantly German SHA users; we used this study to establish the causal baseline effect of a specific intrusive technology feature of SHAs (i.e., unintentional voice activation) on strain via perceived privacy invasion and to examine how this adverse effect can be mitigated with anthropomorphic design features. We then conducted a follow-up field survey study (Study 2) with a representative

sample of SHA users from the U.S. to test the robustness and generalizability of our findings and to extend the theoretical scope of our model.

More specifically, our research design aimed to fulfill three purposes of multi-method research: corroboration, expansion, and compensation (Mingers, 2001; Venkatesh, Brown, & Bala, 2013). First, we used the two studies to triangulate how our findings regarding the core theoretical relationships (i.e., the 'intrusive technology features → stressor → strain' chain of relationships and the moderating effect of anthropomorphic design) converge (or diverge) across different methods and samples (Jick, 1979). Replication across independent studies using different methods and sampling procedures also reduces the likelihood that the observed relationships are spurious and increases the reliability of conclusions (Hinz, Spann, & Hann, 2015). Second, the field survey study expanded the experimental study by examining more general intrusive technology features (i.e., presenteeism, anonymity) and adding social outcomes (i.e., interpersonal conflict) to the model. Third, our design leveraged the strengths and compensated for the limitations of each approach. In this regard, the experimental study demonstrated high internal validity, while the field study ensured high realism and external validity (Goldbach, Benlian, & Buxmann, 2018; Shadish, Cook, & Campbell, 2002).

3.4.2 Study 1: Methods

3.4.2.1 Experimental Design and Treatments

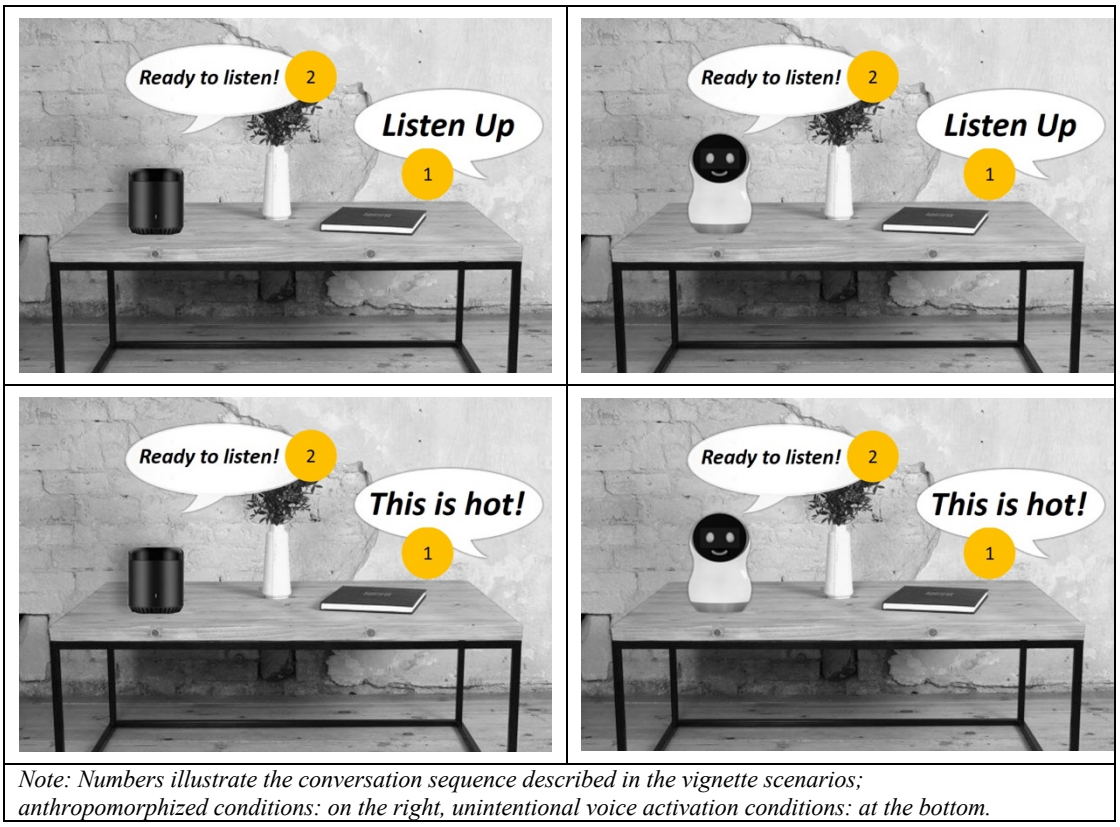
Consistent with previous research (Benlian & Hess, 2011), participants were recruited from online forums and discussion groups for actual SHA owners (e.g., alefo.de, smarthomeassistent.de). Subjects were motivated to participate in a raffle, where they were able to win one out of three Amazon gift cards worth 50€ each. Using this approach, we recruited a pool of 1,976 potential subjects, mostly from Germany.

To test our hypotheses, we employed a 2 (voice activation: unintentional vs. intentional) x 2 (anthropomorphic design: absent vs. present) full factorial design with between-subject treatments. The treatments were manipulated based on vignettes depicted on a website embedded in an online survey. The vignette methodology was chosen for our experiment to control users' experience and avoid social desirability bias (Aguinis & Bradley, 2014). Similar to lab experiments, vignette methodology comes with downsides such as artificial simplifications and hypothetical linear usage scenarios; however, it enables precisely employing manipulations, accurately examining the effects on dependent variables, and identifying hypothesized causal relationships. This technique has also been demonstrated to be

valid and effective in assessing individuals' perceptions of and reactions to specific information privacy- and security-related conditions (P. Lowry, Moody, & Chatterjee, 2017; Warkentin, Goel, & Menard, 2017). Our fictional vignettes described a discussion among family members at dinner in the presence of an SHA called Ingenium; the discussion concerned an upcoming holiday trip. We used this background scenario as context for our manipulations because such SHA usage scenarios were frequently reported in the online forums from which we recruited our participants. In so doing, we followed recommendations in the methodological literature that suggest improving realism in the stimulus presentation by increasing the level of immersion and similarity between the experimental and natural settings (Aguinis & Bradley, 2014). Accordingly, users who are more familiar with a specific usage scenario should usually be able to better immerse themselves into it.

Our experiment proceeded in four major steps. First, participants received the instruction to participate in an assessment of an SHA usage scenario that required their subjective opinion. Second, they were then randomly assigned to one of four experimental conditions, implemented in vignette scenarios, in which they were instructed to step into the shoes of the protagonist Alex, who recently acquired a new SHA for his family home. A textual description of the SHA features was accompanied by a visual depiction of the device to introduce our anthropomorphic stimuli. In conditions with anthropomorphic design cues, the SHA featured visual human attributes (i.e., a smiling face and human-like, curved shape), whereas it had no human resemblance in conditions without anthropomorphic design. In all textual vignettes, we also gave participants the background information that the voice user interface is usually activated with the wake-words "Listen up!". Third, the vignette scenario then continued with the description of a concrete situation in which Alex's family discussed their next holiday trip (i.e., the expected weather in Las Vegas for next week) while having a family dinner. In the unintentional voice activation condition (i.e., "false-positive" condition), while talking to his family about the next holiday trip, Alex unintentionally activated the SHA by stating "This it hot!", which sounds phonetically similar to "Listen up!" In the intentional voice activation condition, Alex addressed the SHA with the correct trigger keywords "Listen up!". The textual description of the scenario was supported by a visual depiction of the conversation with the SHA (see Figure 4, including the manipulations of the respective condition (i.e., absent vs. present anthropomorphized design x unintentional vs. intentional voice activation). In this way, and as recommended for experimental vignette methodology studies (Aguinis & Bradley, 2014), participants were able to understand the design of and interaction with the SHA via textual and graphical manipulations. The response of the SHA ("Ready to listen!") and the

ending of the vignettes were again identical across the four experimental conditions (see Table 5 - Table 8 for the construction of the textual scenarios/vignettes). Fourth, after confirming that participants had understood all information in the respective vignette scenarios, participants were forwarded to a survey in which they completed a post-experimental questionnaire that captured manipulation checks (i.e., perceived intrusiveness, perceived anthropomorphic design), the mediation variable privacy invasion, the dependent variable strain, and several controls.



Note: Numbers illustrate the conversation sequence described in the vignette scenarios; anthropomorphized conditions: on the right, unintentional voice activation conditions: at the bottom.

Figure 4: Displays of the Four Experimental Conditions.

To ensure ecological validity, the depiction of the fictional (non-)anthropomorphized SHA used in the vignettes was based on real-world SHAs (e.g., Jibo. However, we deliberately did not choose popular SHA brands (e.g., Amazon Echo, Google Home) to avoid confounding effects. We also conducted a pretest involving 36 participants (M_{age} = 33.25; 47% male) to develop and fine-tune our stimuli for the main study. Specifically, participants of this pre-test confirmed that unintentional voice activation was perceived as intrusive and that a smiling face and curved body shape (i.e., humanoid embodiment) in an SHA were perceived to convey anthropomorphic features.

3.4.2.2 Variables Measured

Consistent with previous research, we measured our core dependent variable, individual strain, as psychological strain with four items adapted from Moore (2000). Privacy invasion was assessed with three items adapted from Ayyagari et al. (2011). We averaged the items of these constructs for our statistical analysis, as they displayed high internal consistency as well as convergent and discriminant validity (Fornell & Larcker, 1981); see Appendix A Table 9 for a list of items of the principal study variables).

In terms of our manipulation check questions, we drew on a single item for perceived intrusiveness ("*The SHA exhibits intrusive features*", 7-point Likert scale) adapted from Li et al. (2002). To check our manipulation of anthropomorphic design, we used three items measuring perceived anthropomorphic design based on a 5-point semantic differential rating scale ranging from (1) product-oriented, machine-like, artificial to (5) person-oriented, human-like, life-like, prefaced with the stem "*Please rate how you generally perceive the design of your SHA*" (Bartneck, Kulić, Croft, & Zoghbi, 2009; Mourey et al., 2017).

We included age, gender, nationality, perceived ease of use, personal innovativeness, product involvement, and perceived preference fit as controls to account for potential alternative explanations. We adopted three items for measuring perceived ease of use of the SHA from Gefen, Karahanna, and Straub (2003). One item adopted from D. H. McKnight, V. Choudhury, and C. Kacmar (2002) was used to assess participants' personal innovativeness. Furthermore, we measured participants' product involvement with a single item based on Zaichkowsky (1985) as well as perceived preference fit by adapting an item from Alexander Benlian (2015). All control variables were measured on a 7-point Likert scale ranging from 1 = strongly disagree to 7 = strongly agree.[3] The main language in the survey was German, but participants could also choose to answer all questions in an English version of the online questionnaire. The German questionnaire was translated (and back-translated) from the original English version by a professional translation services firm (Brislin, 1990).

3.4.2.3 Sample Descriptives and Manipulation Checks

Of the 1,976 individuals in our subject pool, 197 responded to our invitation. Nineteen subjects failed to complete the questionnaire, and 14 subjects were removed because they provided incorrect answers to attention filter questions. Finally, 28 subjects were removed from the sample because they did not own an SHA at the time of the study. Hence, we used a sample of

[3] The items for the control variables can be obtained from the authors upon request.

136 subjects (effective response rate of 7%) for our statistical analysis. Of the 136 subjects, 35 were females and 101 were males. Their average age was 29 years. The majority of participants were German (72.1% Germans, 19.9% US citizens, and 8% from other nationalities). On average, the subjects had been using SHAs for 2.30 years and spent 2.33 hours using the SHA on average per day. Table 10 in Appendix A reports descriptive statistics, correlations, and reliabilities of the variables in our model.

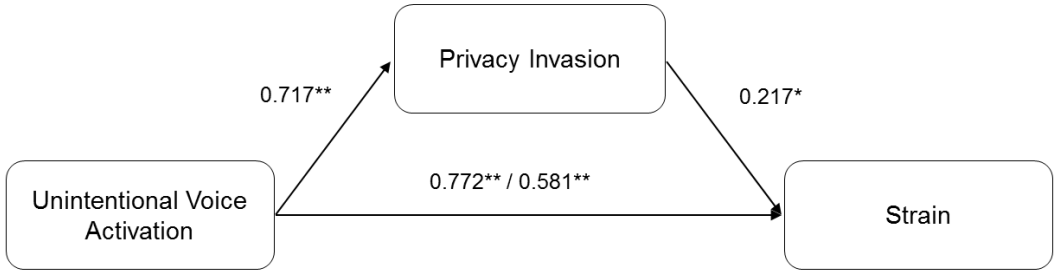
To confirm the successful randomized assignment of participants to our experimental conditions, we conducted several one-way ANOVAs. There were no significant differences in perceived usefulness $F = 0.41$; $p > 0.05$), perceived ease of use $F = 0.05$; $p > 0.05$), perceived preference fit $F = 0.13$; $p > 0.05$), product involvement $F = 0.75$; $p > 0.05$), personal innovativeness $F = 0.40$; $p > 0.05$), age $F = 2.91$; $p > 0.05$), gender $F = 0.46$; $p > 0.05$), or nationality $F = 0.81$; $p > 0.05$) among the experimental conditions. Thus, our results indicate that these factors were not the cause for differences in users' strain.

To check our manipulation of voice activation as an intrusive technology feature, a one-way ANOVA showed that participants in the unintentional voice activation condition $M = 5.65$, $SD = 1.87$) perceived the SHA to be more intrusive than did those in the intentional voice activation condition $M = 3.35$, $SD = 1.87$; $F = 43.94$, $p < .001$). We first averaged responses to the three items to form a perceived anthropomorphic design manipulation check score $r = .83$). A one-way ANOVA showed that subjects in the anthropomorphic design condition $M = 4.01$, $SD = 1.01$) perceived the SHA to be more humanized than did those in the non-anthropomorphic design condition $M = 2.05$, $SD = 0.93$; $F = 36.87$, $p < .001$). Taken together, these results indicate that the treatments were successfully executed.

3.4.3 Study 1: Results

H1 suggested that the effect of unintentional (vs. intentional) voice activation on individual strain is mediated by privacy invasion. We performed a mediation analysis using the bootstrapping mediation technique with a 95% bias-corrected confidence interval and 10,000 samples based on PROCESS model 4 of A. F. Hayes (2018). We entered privacy invasion as a potential mediator, unintentional voice activation as an independent variable and strain as a dependent variable in our mediation model, along with our control variables as covariates. As depicted in Figure 5 and in support of H1, our results confirmed a statistically significant mediation effect of unintentional voice activation on strain via privacy invasion *indirect effect* = 0.195; *standard error* = 0.097; *bias-corrected confidence interval* = [0.051, 0.442]). Specifically, we found that unintentional voice activation significantly increased privacy

invasion $b = 0.717$; $p < 0.01$), while privacy invasion significantly increased strain $b = 0.217$; $p < 0.05$). In sum, our results show that unintentional voice activation has a positive indirect effect on strain via privacy invasion.



Note: The first coefficient on a given path represents the direct effect without the mediator in the model; the second represents the direct effect when the mediator is included in the model. Coefficients were computed using bootstrapping 10,000 samples and a 95% bias-corrected confidence interval (Hayes 2018).
** p < 0.05; ** p < 0.01*

Figure 5: Mediation Results.

In H4, we further suggested that the indirect effect of unintentional voice activation on strain through privacy invasion is moderated by anthropomorphic design, also called a conditional indirect effect, which is equivalent to moderated mediation (A. F. Hayes, 2018). We first analyzed two separate multiple regression models (see Table 2). The first model (Model 1) included unintentional voice activation and all controls as independent variables and privacy invasion as the dependent variable. The analysis confirmed a positive and statistically significant effect of unintentional voice activation on privacy invasion $b = 0.73$; $p < 0.01$). In the second model (Model 2), as the moderating effect of anthropomorphic design is theorized between privacy invasion (i.e., the mediator) and strain, we additionally entered privacy invasion, anthropomorphic design, and the interaction term between unintentional voice activation and anthropomorphic design to predict individual strain. The model revealed a negative and statistically significant interaction between anthropomorphic design and privacy invasion $b = -0.48$; $p < 0.01$) on strain, demonstrating that anthropomorphic design cues interact with privacy invasion such that the effect of privacy invasion on strain is attenuated in the presence of anthropomorphic design cues. Taking the results from Models 1 and 2 into account, we thus find initial evidence for a conditional indirect effect.

	Model 1		**Model 2**	
Outcome	Privacy Invasion		Strain	
	β	*SE*	*β*	*SE*
Intercept	4.21***	.70	.61	.96
Mediator				
Privacy Invasion			.59***	.14
Manipulations & Interaction				
Voice Activation (Intentional vs. Unintentional)	.73***	.23	.67**	.24
Anthropomorphic Design (Non-anthropomorphic vs. Anthropomorphic)			1.47	.86
Privacy Invasion × Anthropomorphic Design			-.48**	.18
Controls				
Age	-.02	.01	-.02	.01
Gender (male)	.38	.26	.02	.26
Nationality (German)	.12	.08	.00	.08
Perceived Ease of Use	-.02	.10	-.12	.11
Perceived Preference Fit	-.08	.08	-.07	.05
Product Involvement	-.02	.07	-.03	.08
Personal Innovativeness	.03	.09	.02	.03
R^2	.12		.25	
F	2.61*		4.06**	
*Note: * p < .05; ** p < .01; *** p < .001; N= 136; SE = Standard Error*				

Table 2: Direct Effect of Unintentional Voice Activation on Strain.

As a more direct and rigorous test of H4, we computed the conditional indirect effect using bootstrapping analysis with 10,000 samples and a 95%-biased corrected confidence interval (CI) based on PROCESS model 14 of A. F. Hayes (2018). The results in Table 3 show that the conditional indirect effect of unintentional voice activation on strain via privacy invasion is significant in the absence of anthropomorphic design but not in its presence, supporting our theorizing in H4 that anthropomorphic design buffers or even cancels out the intrusive effects of SHAs on strain through privacy invasion.

Anthropomorphic Design	Coefficient for Conditional Indirect Effect	Boot SE	Lower Limit CI	Upper Limit CI
absent	0.425	0.178	0.153	0.873
present	0.080	0.083	-0.053	0.282
Note: Coefficients were computed based on moderated mediation analysis incl. all controls and using bootstrapping with 10,000 samples and a 95% bias-corrected confidence interval (A. F. Hayes, 2018)				

Table 3: Conditional Indirect Effect of Unintentional Voice Activation on Strain.

As mentioned above, study 1 was constrained to a rather artificial scenario with limited ecological validity and a relatively small sample of SHA aficionados. In addition, the first study's research setting used only one single and specific instance of an intrusive technology feature (unintentional voice activation) and focused solely on individual strain as outcome. Study 2 aimed to address these limitations, corroborating the high internal validity of study 1's experimental design within a more generalizable context, using a larger and representative sample and more general (and classical) measures for intrusive technology features (i.e., presenteeism and anonymity). Moreover, in study 2, we were able to account for an extended reach of the consequences of SHAs' intrusive features beyond individual strain to include interpersonal conflict at home and thus the relational and social consequences of SHAs' intrusive technology features.

3.4.4 Study 2: Methods

3.4.4.1 Data Collection and Sample Description

In our follow-up field study, we cooperated with a market research firm that maintained a research panel to obtain a random sample of SHA users. The subject pool consisted of U.S. citizens with representative demographics for SHA owners. In line with previous research, we motivated our subjects to participate in exchange for a payment of $6 e.g., (P. B. Lowry, Moody, Galletta, & Vance, 2013). The welcome page of the online questionnaire outlined the purpose of the survey. It also stated that the confidentiality and anonymity of the responses were ensured. Consistent with previous studies on anthropomorphized products (Mourey et al., 2017), participants were instructed to complete the questions in the presence of their SHA to ensure that they were able to look at and touch the SHA, thus ensuring high engagement.

The market research firm sent invitations to 1,500 potential SHA owners in their panel who were directed to our online survey questionnaire. We received responses from 243 SHA owners who passed several screening questions of the panel provider, resulting in an initial response

rate of 16%. Additionally, we filtered out another 29 subjects based on attention filter questions and because subjects indicated that they did not have their SHA on hand while completing the survey. Hence, the final sample size used for our statistical analysis included 214 subjects for a final response rate of 14%. The average age of participants was 41, ranging from 18 to 65. A total of 129 of the 214 subjects were female. On average, the subjects had owned SHAs for 1.79 years and indicated that they spent an average of 1.26 hours per day using the SHA. Nonresponse bias was assessed by verifying that early and late respondents were not significantly different (J. S. Armstrong & T. S. Overton, 1977). We compared both samples based on their socio-demographics. t-tests between the means of the early (first 50) and late (last 50) respondents showed no significant differences $p > 0.05$), indicating that nonresponse bias was unlikely to have affected the results.

3.4.4.2 Variables Measured and Measurement Model Assessment

Consistent with our first study, strain was measured as perceived strain, adapting four items from Moore (2000). Four items from Stanley, Markman, and Whitton (2002) were used to measure interpersonal conflict to fit the purpose of this study (i.e., to capture potential interpersonal conflicts between the SHA users and other household members). We again measured privacy invasion based on three items from Ayyagari et al. (2011). In terms of the intrusive technology characteristics, we assessed presenteeism based on three items from Ayyagari et al. (2011) and anonymity based on three items from Pinsonneault and Heppel (1997). All the preceding scales were measured using 7-point Likert scales ranging from (1) strongly disagree to (7) strongly agree. Consistent with study 1 and previous research studies, we measured anthropomorphic design as perceived anthropomorphic design based on three items on a 5-point semantic differential rating scale, prefaced with the stem "*Please rate how you generally perceive the design of your SHA*" and ranging from (1) product-oriented, machine-like, artificial to (5) person-oriented, human-like, life-like (Bartneck et al., 2009; Mourey et al., 2017). Table 11 in Appendix B provides an overview of items for the principal study constructs.

To account for alternative explanations, we additionally included the following control variables: age, gender, education, prior privacy experiences, dispositional privacy concern, positive/negative affectivity, trust in SHA provider, perceived usefulness, perceived ease of use, type of SHA owned, duration of SHA ownership, and intensity/frequency of SHA usage (F. D. Davis, 1989; Dinev & Hart, 2006a; Dinev et al., 2016; Watkins Allen et al., 2007). The patterns of results remained qualitatively unchanged when including these control variables in

our models. Accordingly, we will omit the controls when reporting our statistical results in subsequent sections.[4]

We assessed the psychometric properties of the measurement model results by examining internal consistency, convergent validity, and discriminant validity (see Table 12 in Appendix B). The loadings of the measurement items on their respective latent variables were above the threshold value of 0.70 (Hair, Hult, Ringle, & Sarstedt, 2016) and were all significant $p < 0.05$). Furthermore, measurement items did not have cross-loadings above 0.40 on the unintended constructs, and the square roots of AVE were consistently larger than relevant interconstruct correlation coefficients, suggesting discriminant validity (Hair, Black, Anderson, & Babin, 2018). The internal consistency of all constructs clearly exceeded the threshold of 0.70, implying acceptable reliability (Fornell & Larcker, 1981). Hence, the constructs in our second study represent theoretically and empirically distinguishable concepts.

Given that all of our items were measured with the same method, we tested for common method variance using Harman's one factor test (Podsakoff, Mackenzie, Lee, & Podsakoff, 2003). We performed an exploratory factor analysis on all the variables, but no single factor was observed, and no single factor accounted for a majority of the covariance in the variables. Furthermore, we used a correlational marker technique where the highest variable from the factor analysis was entered as an additional independent variable (Richardson, Simmering, & Sturman, 2009). This variable did not create a significant change in the variance explained in the dependent variables. Both tests suggest that common method bias is unlikely to have significantly affected our results.

3.4.5 Study 2: Results

To test our research model, we used partial least squares structural equation modeling (PLS-SEM), which is widely used in IS research and was implemented in our study with the software package SmartPLS3 (Ringle, Wende, & Becker, 2015). Hair et al. (2016) and Rigdon, Sarstedt, and Ringle (2017) have emphasized that the use of PLS-SEM, compared to covariance-based SEM, is particularly suited for research that tends to be exploratory. As our study extends a novel theory in an under-researched context, PLS-SEM fits our purposes well.[5] We computed

[4] The items for the control variables and our statistical results including the control variables can be obtained from the authors upon request.

[5] We also repeated our statistical analysis with hierarchical moderated regression models, and we tested our mediation and moderated mediation hypotheses with conditional indirect effect analyses (A. F. Hayes, 2018), leading to substantively similar findings.

all relationships in our models using a bootstrapping procedure with no sign changes, mean replacement algorithm, and 10.000 resamples.

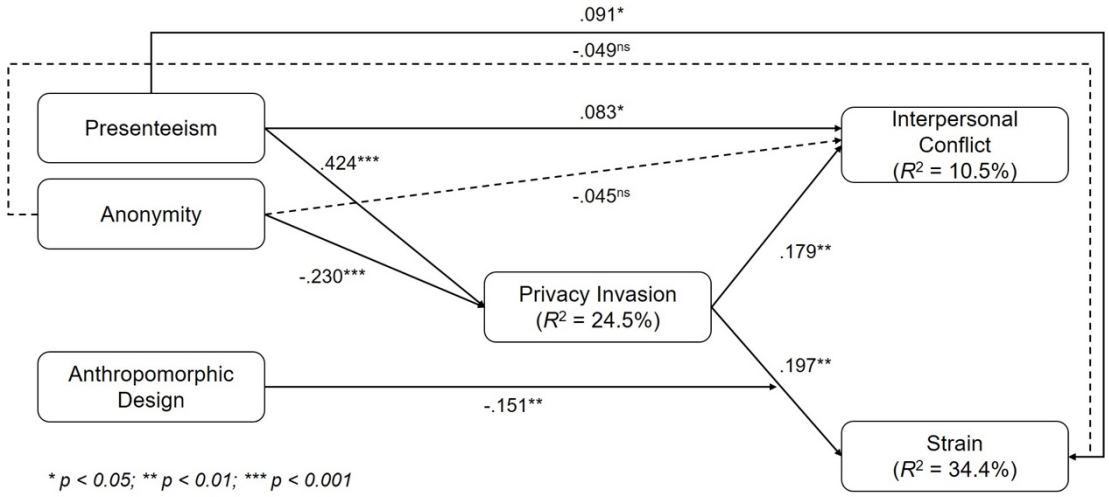
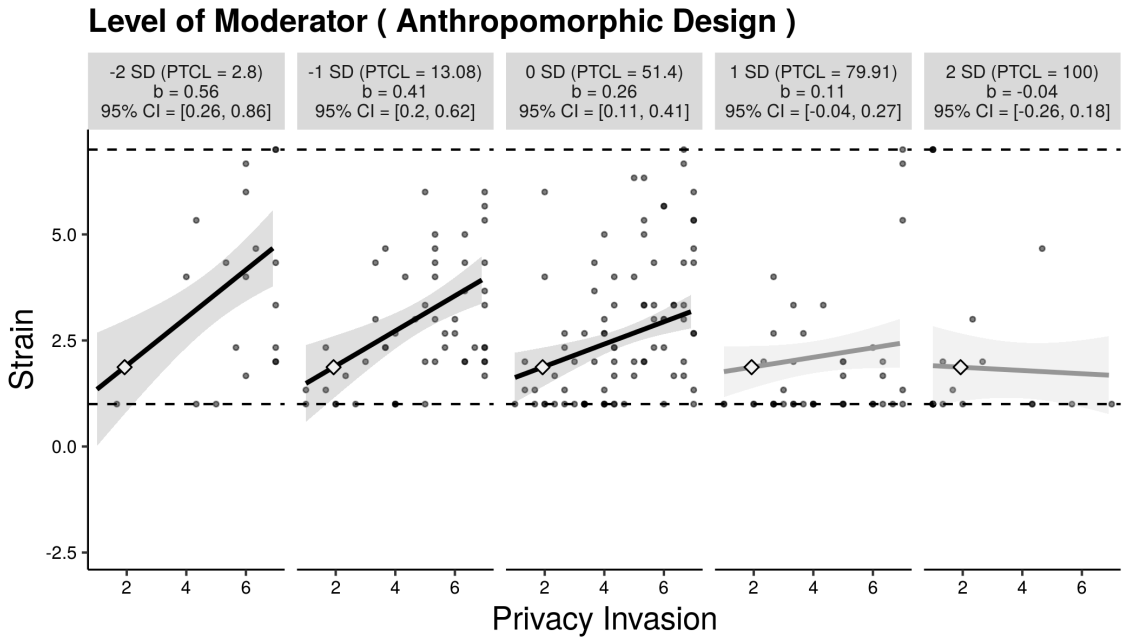


Figure 6: Results of PLS-SEM Analysis.

The results of our PLS-SEM analysis (see Figure 6) supported all of our mediation hypotheses. In support of H2a, we found a positive indirect effect of presenteeism on strain through privacy invasion (indirect effect = .091; standard error = .049; bias-corrected confidence interval = [.007, .202]), while we found a negative indirect effect of anonymity on strain through privacy invasion (indirect effect = -.049; standard error = .028; bias-corrected confidence interval = [-.124, -.007]), supporting H3a. More interestingly, the indirect effects of intrusive technology features via privacy invasion also extended to interpersonal conflicts between SHA users and their household members. In support of H2b, presenteeism exhibited a positive indirect effect on interpersonal conflict through privacy invasion (indirect effect = .083; standard error = .041; bias-corrected confidence interval = [.014, .176]). In contrast, anonymity had a negative indirect effect on interpersonal conflict through privacy invasion (indirect effect = -.045; standard error = .024; bias-corrected confidence interval = [-.107, -.009]), supporting H3b. Taken together, our results demonstrate that SHAs' intrusive technology features (i.e., presenteeism and anonymity) have detrimental effects not only on individual strain but also on individuals' social relationships at home through privacy invasion.

In addition to the mediation results, our PLS-SEM analysis revealed a negative interaction effect between anthropomorphic design and privacy invasion on strain $\beta = -.151$; $p < 0.01$). To shed further light on this moderating effect, we conducted simple slope tests (Aiken & West, 1991; McCabe, Kim, & King, 2018). Figure 7 depicts the simple slopes of the moderator (anthropomorphic design) at 2 SD and 1 SD below the mean, at the mean, and at 1 SD and 2

SD above the mean. Consistent with our findings in study 1, the simple slope analysis revealed that anthropomorphic design moderates the effect of privacy invasion on strain such that the more humanlike the SHA design was perceived to be, the weaker the effect of privacy invasion on strain.



Note: Each graphic shows the computed 95% confidence region (shaded area), the observed data (gray circles), the maximum and minimum values of the outcome (dashed horizontal lines), and the crossover point (diamond). The x-axes represent the full range of the focal predictor. CI = confidence interval; PTCL = percentile, SD = standard deviation.

Figure 7: Simple Slope Analysis.

As a more robust assessment of our moderated mediation hypothesis in H4, we conducted two moderated mediation analyses for the conditional indirect effects of presenteeism and anonymity on strain through privacy invasion. We again computed the conditional indirect effects using bootstrapping with 10,000 samples and a 95% bias-corrected CI based on PROCESS model 14 (A. F. Hayes, 2018). The results in Table 4 show that the conditional indirect effects of presenteeism and anonymity on strain via privacy invasion are significant at low levels (i.e., 1 SD below the mean) of anthropomorphic design but not significant at high levels (i.e., 1 SD above the mean) of anthropomorphic design. Hypothesis H4 was thus fully supported.

Intrusive Technology Feature	Anthropomorphic Design	Coefficient for Conditional Indirect Effect	Boot SE	Lower Limit CI	Upper Limit CI
Presenteeism	- 1SD	0.267	0.052	0.171	0.374
	+ 1SD	0.032	0.027	-0.020	0.086
Anonymity	- 1SD	-0.131	0.062	-0.261	-0.030
	+ 1SD	-0.034	0.021	-0.084	0.011
Note: Coefficients were computed based on moderated mediation analysis using bootstrapping with 10,000 samples and a 95% bias-corrected confidence interval (A. F. Hayes, 2018)					

Table 4: Conditional Indirect Effects of Presenteeism and Anonymity on Strain.

3.5 Discussion

This paper aimed to shed light on the broader consequences of SHAs' intrusive effects on individual users' strain and their social relations at home. We also sought to advance our understanding of how anthropomorphic design features might mitigate these adverse effects.

The results from two independent studies that leveraged the synergistic properties of experimental and field survey research and helped replicate our core findings support the premise that intrusive technology features of SHAs increase strain and interpersonal conflicts through privacy invasion. Specifically, we show that unintentional voice activation, high presenteeism, and low user anonymity drive privacy invasion, which in turn heightens individual strain and interpersonal conflicts at home. The core rationale behind these relationships is that intrusive technology features create a misfit between the demands of a digitized environment and users' need for privacy, and that misfit may unsettle users and even impair social relationships. In addition, we found robust empirical evidence that anthropomorphic design features can attenuate and even offset the detrimental effect of privacy invasion on user strain. We argue this is the case because anthropomorphic features address a fundamental social need of individuals, namely to socialize and build trust with another party. When SHAs can meet such needs with more human-like qualities, users may be more willing and able to cope with privacy invasion through SHAs' intrusive technology features. Overall, these findings make important theoretical and practical contributions, and suggest avenues for future research.

3.5.1 Theoretical Contributions

First, we add to research on technology-induced stress by empirically validating a critical causal pathway of the P-T fit model in the home domain; we do this by linking intrusive SHA features

to individual strain via privacy invasion. Above and beyond this contribution, we extend the P-T fit model with self-regulatory theory by showing how the detrimental effects of intrusive SHA features can even impair users' social relationships at home via resource depletion and, as such, expand the criterion space in this stream of research to include individual *and* social outcomes at home. While previous technostress research has predominantly looked at consequences for individual employees in work settings, the far-reaching effects of digital technologies on individuals and their interpersonal relationships at home have received only minimal attention so far. Our findings also highlight privacy invasion as a central explanation of why intrusive technology features influence third parties not directly involved in the person-technology relationship, suggesting that technology-induced privacy invasion has a potentially wider reach than previously assumed. Our work therefore provides insights into making the transition from an individual-centric technostress model to a model that is able to explain outcomes for third parties (e.g., friends, significant others, children) beyond the individual.

Second, this research advances our understanding of how technology features of the same underlying IT artifact not only have stress-inducing effects but also serve as resources that enable users to cope with such stress. Specifically, we integrate the person-technology fit model with the literature on anthropomorphism to show that anthropomorphic SHA features can help mitigate and even neutralize the intrusive effects of SHAs. Our reasoning is that anthropomorphic features seem to compensate for a lack of trust, increase perceived control and thus help users better deal with privacy invasions. These findings provide a more nuanced understanding of the conditions under which the negative effects of intrusive technology features are likely to occur and thus extend the P-T fit model by introducing a novel, IT artifact-based moderating effect in the technology-stressor-strain causal chain of relationships. In a similar vein, our study contributes to previous research on anthropomorphism across various disciplines (e.g., robotics, human-computer interaction) by showing in field investigations that anthropomorphic features in new digital devices and services (i.e., SHAs) can help, rather than harm, individuals in their private lives at home.

Finally, and more broadly, by looking at the effects of digitization on individuals' strain and interpersonal relationships and at factors that modulate the adverse influence of digitization, we answer Turel et al.'s (2018) call for research into the largely unaddressed psychological and relational consequences of digital technologies for individuals and their social environments at home. Given that research on the digitization of individuals is still in its embryonic stages, it is

both important and useful for scholars to explore new technology-based coping strategies that help users address privacy invasion and technostress.

3.5.2 Practical Contributions

Our results also have important implications for practice. For SHA and third-party service providers who are attempting to attract new users and convince existing users to use their devices and services on an ongoing basis, it is imperative to understand that intrusive technology features may not only enhance user strain through privacy invasion but also impair social relations between users and other household members. SHA and third-party service providers might benefit from our study by carefully testing and monitoring the intrusive features of their devices and services with the goal of reducing individual strain and interpersonal conflicts. As evidenced in our study, increasing anonymity on the one hand and reducing presenteeism and unintentional voice activation on the other may be proactive approaches to achieving this goal.

As much as SHA and third-party service providers would like to take the above steps, they may find it difficult or even counterproductive to keep their intrusive technology features to a minimum, as they would probably miss out on user learning opportunities and future improvements of their solutions. Our study findings show that in such cases, complementary technology features, such as anthropomorphic features, may serve as a buffer to attenuate the potentially harmful effects of intrusive technology features. If SHA and third-party service providers choose to embed anthropomorphic features into their solutions, they are well advised to carefully examine and test which specific anthropomorphic features (e.g., body, voice, virtual assistant) they use and combine to effectively achieve these buffering effects.

In light of the abovementioned practical implications, our research also sends a cautionary message to SHA users at home. Because our study has shown that anthropomorphic technology features can mitigate SHAs' intrusive effects, users should be cautious about whether such and similar technology features are misused as a red herring to push the boundary of privacy infringements for commercial purposes. Our study may therefore benefit SHA users by helping them better understand the intricate (and often delicate) interplay between different technology features and by encouraging them to reflect on the potentially hidden agendas of service providers.

3.5.3 Limitations, Future Research and Conclusion

Despite the aforementioned theoretical and practical contributions of this research, our study has three major limitations, which may open up a series of interesting research directions. The first limitation relates to our use of self-reports to assess the constructs in our model, in particular in study 2. However, we believe that the use of self-reports is adequate for several reasons. First, variables such as privacy invasion or interpersonal conflict reflect individuals' psychological experience and thus may be best evaluated by the focal person. Second, common method bias (CMB) concerns may be minimized not only due to the statistical procedures we employed but also because we could validate our core hypotheses across two independent studies with different research methods and sampling procedures (Hofmann & Gavin, 1998). Furthermore, CMB is not of concern when testing interaction effects; in fact, it can even make interactions more difficult to detect, which would make our results conservative (Siemsen, Roth, & Oliveira, 2010).

Second, one of the key purposes of the multi-method approach was to expand the scope of the research model across our two studies in some aspects, particularly in terms of intrusive technology features and outcome variables, while triangulating on the core theoretical relationships (i.e., the mediation and moderated mediation relationships). However, we did not replicate the effects of SHA-specific (i.e., unintentional voice activation) or more general intrusive technology features (i.e., technology presenteesim and anonymity) across our two samples. Accordingly, future research may further cross-validate our current findings on the effects of SHA-specific and more general intrusive technology features on different outcome variables including strain and interpersonal outcomes. Moreover, our studies were conducted in countries with relatively similar cultural backgrounds. However, technology users' needs for anonymity and presenteesim and their reactions to information privacy breaches may differ across cultures. For example, Eastern cultures may differ significantly from Western cultures in their reactions to privacy infringements through intrusive technology features e.g., (France Bélanger & Robert E. Crossler, 2011) and thus provide an interesting avenue for future inquiry.

Third, even though we applied a multi-method approach to triangulate users' experiences with and reactions to their SHAs, our study designs—relying on scenario-based, hypothetical and cross-sectional observations—did not allow us to investigate users while they were actually using their SHAs over a longer period of time. To further strengthen the ecological validity of our findings, we invite future research to conduct longitudinal field experiments (Gneezy, 2017) or experience-sampling studies (C. D. Fisher & To, 2012) to examine continuous use over a

longer duration and capture users' reactions to SHAs' technology features in the moments when they are being used. This approach would also allow researchers to observe study participants in their interactions with SHAs in a more realistic setting via modalities that go beyond text-based or visual cues to include voice recognition. In this way, the manipulation of anthropomorphic features would be more multi-faceted and real.

Despite these limitations, our study provides several fruitful directions for future research. First, our research focused on privacy invasion as a stressor and mediating mechanism. This focus was driven by theoretical considerations regarding its centrality to capture the adverse effects of SHAs' intrusive technology features. Future research may examine other explanatory mechanisms, such as role ambiguity or negative affectivity, which provide alternative or complementary accounts (Ayyagari et al., 2011). In the same vein, although we theorized the relationship of SHAs' intrusive characteristics with interpersonal conflicts via privacy invasion and drew on resource depletion arguments to bolster this link, we did not directly measure resource depletion as another potential mediator. Future research is needed to dig deeper into the self-regulatory processes by which technology-induced stressors such as privacy invasion translate into interpersonal conflicts at home.

Second, we chose to focus on anthropomorphic design features that were particularly tangible and relevant in mitigating potential privacy concerns vis-à-vis impersonal machines. Future research may also examine other anthropomorphic features, such as the voice of the virtual assistant or the expression of emotions via multimodal sensory signals (e.g., body posture, eye gaze shift and voice pitch). By extension, other moderators may also be of interest to future researchers. For example, it would be interesting to examine how usability features affect the relationship of SHAs' intrusive features with strain (Ayyagari et al., 2011). Individual differences between users (e.g., regulatory focus) or context variables (e.g., factors related to the quality of the home environment such as family climate) may also be taken into account to gain a more holistic understanding of the factors that serve as regulators moderating the translation of technology-driven stressors into (intra-/interpersonal) strain at home (Higgins, 1998; Moos, 1990; Ofir Turel & Gaudioso, 2018). Moreover, future research may particularly look into moderators that attenuate SHAs' intrusive effects on interpersonal conflicts but that we did not consider for the sake of parsimony.

Third, future research may also further investigate the interaction of anthropomorphic features of SHAs with users' feelings of privacy invasion when varying the degree of human likeness of the anthropomorphic features in line with the uncanny valley model (Mori et al., 2012). This

approach would allow examining the theoretically intriguing question of whether the mitigating effect of anthropomorphic design features on the positive relationship between privacy invasion and strain would turn into an exacerbating effect when anthropomorphic design features approach high levels of human likeness. Finally, important home outcome variables other than strain or interpersonal conflicts could be investigated in future research studies. Such outcomes may, for example, include individuals' social behaviors (e.g., helping or spending time with other household members) or more specific indicators of well-being (e.g., sleep quality, depression). Scholars may also wish to extend our study by focusing on how the intrusive effects of SHAs on users cross over to affect the well-being of their partners and other family members (C.-q. Lu, Lu, Du, & Brough, 2016).

With the growing penetration of our homes by SHAs comes the risk of privacy infringements through SHAs' intrusive technology features that, more often than not, put increased strain on users. Integrating the P-T fit model with self-regulation theory, we show that SHAs' intrusive effects can extend to users' social environment and increase interpersonal conflicts at home. And by applying anthropomorphic design features to SHAs, we also demonstrate that those intrusive effects can be mitigated and even cancelled out, thus proposing a novel, IT artifact-based coping mechanism in the context of digital technologies. We hope that our study will provide a foundation for further research on the effects of digitization on the individual in private life, enabling researchers to uncover creative and viable design solutions for smart home devices to effectively reduce privacy infringements and increase well-being.

3.6 Appendix A: Study 1

Scenario Construction

Page 1 of scenario:

In the following scenario, please put yourself into the shoes of Alex who just came to read the following advertisement in the Internet:
[Randomized display of anthropomorphic design manipulation]
After thoroughly reading through this ad, Alex decided to buy the displayed Smart Home Assistant (SHA) called Ingenium for his family home. After receiving the SHA, Alex places it on a table in the living room where it is set up properly and has reliable access to the Wi-Fi network.

Table 5: First Scenario Page.

Anthropomorphic design manipulations

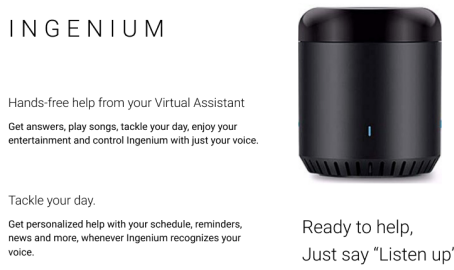
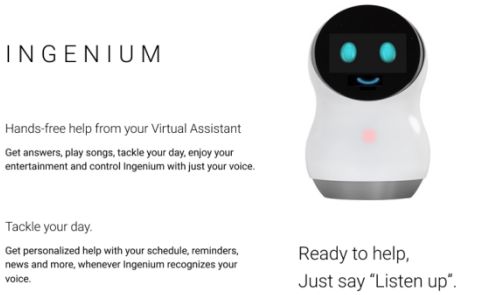
	
Anthropomorphic design absent	**Anthropomorphic design present**

Table 6: Measurement Items of Focal Study Constructs (Study 1).

Page 2 of scenario:

Please remember to assess the following scenario from Alex's perspective:

Alex, his sister and parents are having dinner in the living room and they are chatting about their upcoming family vacation in Las Vegas next week. *Alex asks his family for Las Vegas' next week weather forecast. While no one is absolutely sure, his sister says that the weather is expected to be very hot with a high of 40°C (104°F).*
[Randomized display of voice activation manipulation]
In response to Alex' exclamation, the Smart Home Assistant Ingenium is activated and responds with "Ready to listen!" *After dealing with Ingenium, the holiday conversation among Alex and his family moves on to travel and accommodation arrangements.*
End of usage scenario and transition to survey questions.

Table 7: Second Scenario Page.

Voice activation manipulations

Intentional voice activation:	*Alex wants to play it safe and know exactly how the weather is going to be in Las Vegas next week. He addresses Ingenium with the trigger words: "Listen Up!"*
Unintentional voice activation:	*Alex is excited about such hot temperatures and responds to his sister by exclaiming: "This is hot!"*

Table 8: Voice Activation Manipulations.

Each usage scenario on page 2 was supported by a visual depiction of the conversation with the SHA Ingenium (see Figure 4), including the manipulations of the respective condition (i.e., absent vs. present anthropomorphized design x unintentional vs. intentional voice activation).

Measurement Items, Descriptive Statistics, and Correlations

Construct	Items
Strain Moore (2000) 7-point Likert scale	Alex must feel drained from interactions with Ingenium.
	Alex must feel tired from his Ingenium use.
	Working all day with Ingenium is a strain for Alex.
	Alex must feel burned out from his Ingenium interactions.
Privacy Invasion Ayyagari et al. (2011) 7-point Likert scale	Alex feels his privacy can be compromised because activities using Ingenium can be traced.
	Alex feels that the use of Ingenium makes it easier to invade his privacy.
	Alex feels uncomfortable that the use of Ingenium can be easily monitored.

Table 9: Measurement Items of Focal Study Constructs (Study 1).

	Constructs	Mean	StD	α	1	2	3	4	5	6	7	8
1	Age	28.91	5.83	-	-							
2	Gender male)	.74	.43	-	-.09	-						
3	Privacy Invasion	4.67	1.29	.82	-.08	.16*	**.71**					
4	Perceived Ease of Use	5.64	1.07	.81	-.09	-.01	.07	**.86**				
5	Perceived Preference Fit	4.94	1.58	-	.04	.06	-.14	.26**	-			
6	Product Involvement	4.68	1.98	-	.25**	.24**	-.02	.11	.35**	-		
7	Personal Innovativeness	5.06	1.67	-	.27**	.23**	.03	.10	.28**	.68**	-	
8	Strain	2.99	1.38	.88	-.20**	.00	.15	-.23**	-.09	-.01	-.02	**.76**

*N = 136; *p < .05; **p < .01; α = Cronbach Alpha; Square root of AVE (bolded cells)*

Table 10: Descriptive Statistics, Internal Consistency, Discriminant Validity, and Construct Correlations (Study 1).

3.7 Appendix B: Study 2

Construct	Items
Interpersonal Conflict Stanley et al. (2002) 7-point Likert scale	Interacting with my SHA impairs the quality of communication I have with other home members.
	My interactions with other home members are negatively affected, when I use my SHA.
	It is more likely that I have a dispute with other home members, when I interact with my SHA.
	When I use my SHA, conflicts with other home members are more likely.
Strain Moore (2000) 7-point Likert scale	I often feel tired from interacting with my SHA.
	Having my SHA around me all day is a strain for me.
	I often feel drained from activities that involve using my SHA.
Privacy Invasion Ayyagari et al. (2011) 7-point Likert scale	I feel uncomfortable that my use of my SHA can be easily monitored.
	I feel my provider could violate my privacy by tracking my activities using my SHA.
	I feel that my use of my SHA makes it easier to invade my privacy.
Presenteeism Ayyagari et al. (2011) 7-point Likert scale	The use of my SHA enables the service provider to have access to me.
	My SHA makes me accessible to the service provider.
	My SHA enables me to be in touch with the service provider.
Anonymity Pinsonneault and Heppel (1997) 7-point Likert scale	I feel that the service provider cannot trace back how I use my SHA.
	I feel anonymous when using my SHA.
	I do not feel like my service provider identifies my use of voice commands.
(Perceived) Anthropomorphic Design Bartneck et al. (2009); Mourey et al. (2017) 5-point semantic differential rating scale, ranging from (1) product-oriented, machine-like, artificial to (5) person-oriented, human-like, life-like	Please rate how you generally perceive the design of your SHA: (1) product-oriented – (5) person-oriented (1) machine-like – (5) human-like (1) artificial – (5) life-like

Table 11: Measurement Items of Focal Study Constructs (Study 2).

	Construct	*Mean*	*StD*	*α*	1	2	3	4	5	6	7	8	9
1	Age (years)	40.60	13.02	-	-								
2	Gender (male)	.40	.49	-	-.01	-							
3	Education†	1.77	.82	-	-.01	.20**	-						
4	Presenteeism	4.86	1.49	.84	-.01	.01	-.03	**.75**					
5	Anonymity	3.30	1.56	.86	-.10	.10	-.08	-.06	**.71**				
6	Anthropomorphic Design	4.45	1.49	.83	.01	-.17*	-.09	.13	-.02	**.84**			
7	Privacy Invasion	4.51	1.91	.92	-.11	.09	.09	.33**	-.26**	-.39**	**.80**		
8	Strain	2.66	1.74	.93	-.20**	.13	.10	.30**	.10	-.28**	.37**	**.82**	
9	Interpersonal Conflict	2.96	1.63	.91	-.24**	.08	-.02	.35**	.15*	-.19**	.34**	.65**	**.77**

*N = 214; *p < .05; **p < .01; α = Cronbach Alpha; Square root of AVE (bolded cells); † ranging from (1) high school or equivalent to (4) doctoral degree*

Table 12: Descriptive Statistics, Internal Consistency, Discriminant Validity, and Construct Correlations (Study 2).

Chapter 4: Location Based Services with Push Information Delivery Mechanisms and their Interaction with Social Proof

Title: How Pull vs. Push Information Delivery and Social Proof Affect Information Disclosure in Location Based Services

Authors: Johannes Klumpe, Technische Universität Darmstadt, Germany
Oliver Francis Koch, Technische Universität Darmstadt, Germany
Alexander Benlian, Technische Universität Darmstadt, Germany

Published in: Electronic Markets (2019), pp.1-18.

Abstract

With the boom of the app economy, users' location information has become an increasingly valuable differentiator to deliver personalized products and services, yet continues to raise severe privacy concerns. While research on information privacy has paid great attention on explaining and predicting factors of information disclosure decisions, there is still a significant gap in terms of how app providers can combine different mechanisms in the design of their apps to effectuate better disclosure outcomes. Drawing on a randomized online experiment with 143 smartphone users, we analyze how pull (i.e., services with user-controlled position awareness) and push (i.e., demanding always-on access location tracking) information delivery and social proof cues separately and jointly affect users' actual location information disclosure. The results reveal that both strategies increase actual location information disclosure via two distinct mediation paths. While pull information delivery mitigates users' privacy concerns, social proof increases their trusting beliefs. However, when both strategies are employed together, we found that social proof overrides the effect of pull information delivery mechanisms.

Keywords: Location based services, pull information delivery, social proof, location disclosure, privacy concerns, trust

4.1 Introduction

Smartphone adoption, which is expected to reach 2.53 billion users by 2018 alone, has underpinned the rise of the app economy and the success of marketplaces such as Apple's App Store and Google's Play Store (eMarketer, 2016). However, the dramatic increase in the collection and monetization of users' personal information has brought scrutiny towards the privacy practices of app providers. For example, whereas consumers may understand why Google Maps requires location information in order to provide personalized recommendations, it is less obvious why Facebook requires uploading contact lists to their servers (J. Lin et al., 2012). The consequences are rising privacy concerns which represent a big challenge for new apps that require personal user information to deliver on their value propositions (Alexander Benlian, 2015; Mulligan, 2014).

Information privacy research, which relates to the extent to which consumers can control how their personal information is acquired and used (Smith et al., 2011a), has thus far come up with multiple models and theories trying to explain what affects information privacy-related decision making. Among these theories more recently, the personalization-privacy paradox as well as the Antecedents → Privacy Concerns → Outcomes (APCO) model have been at the center of research attention (Naveen Farag Awad & Mayuram S Krishnan, 2006; Smith et al., 2011a). While the personalization-privacy paradox describes how users are willing to trade off their privacy when they obtain personalization of products and services in return (Naveen Farag Awad & Mayuram S Krishnan, 2006), the APCO framework places privacy concerns, as a measurable proxy for information privacy, at the center of a core nomological network being surrounded by several antecedent and outcome variables (Smith et al., 2011a). From an outcome perspective, aside from investigations on regulatory (Culnan & Armstrong, 1999; Elahi, 2009) and attitudinal outcomes (Smith et al., 2011a; Yun, Lee, & Kim, 2014), research has thus far primarily focused on information disclosure decisions in the context of user authentication on websites at the neglect of more timely and ubiquitous disclosure decisions based on user location information (H. Xu & Gupta, 2009). Compared to other personal information (e.g., email address), location information bears unforeseeable threats and consequences due to its dynamic character. While disclosing the current location seems unproblematic, live-tracking of users imposes threats like the collection of location-related information such as customer movement and trajectory patterns or potential real-world consequences such as unwanted encounters (Barkhuus, 2004; Junglas et al., 2008; Junglas & Watson, 2008). From an antecedent perspective, while research has mostly focused on explaining and predicting individual differences in and attitudes towards information disclosure such as prior privacy experience and

privacy concern types (Culnan & Armstrong, 1999; Phelps et al., 2001; Smith, Milberg, & Burke, 1996), it has paid relatively little attention towards examining important design factors at the IT artifact level, even though previous research has called for looking into the interplay of theoretically interesting and practically relevant design factors affecting privacy-related decision-making (France Bélanger & Robert E Crossler, 2011; Chellappa & Sin, 2005; D. J. Kim, Ferrin, & Rao, 2008; Smith et al., 2011a).

Our research intends to address this gap by examining both the distinct and combined effects of information delivery mechanisms (i.e., methods via which information is acquired from (pull option) or conveyed to (push option) mobile users) as well as social proof cues (i.e., signals of popularity and demand) on mobile users' information disclosure decisions. These mechanisms are widely employed together in practice and their combination is particularly interesting from a theoretical perspective. Given that information delivery mechanisms may impact users' control over their data and thus reduce mobile users' privacy concerns on the one hand (D. J. Kim et al., 2008; H. Xu & Gupta, 2009) and given that social proof cues may increase trust by signaling high popularity on the other hand (Kendall & Kendall, 1999; H. Xu et al., 2008), their combination promises to increase users' actual information disclosure via two distinct theoretical paths. Furthermore, both mechanisms may interact in theoretically interesting ways, as these cues might unfold complementary or substitutive effects on users' information disclosure behavior. While it is conceivable that social proof cues mitigate the negative effects of users' privacy concerns on information disclosure (and thus add to the positive effect of information delivery mechanism), it can also be argued that social proof cues supersede information delivery mechanisms, as mobile users' privacy concerns are sufficiently mitigated by social proofs alone. Against this background, the objective of our study is to address the following research questions:

RQ1: What is the distinct effect of information delivery mechanisms (pull vs. push) on mobile users' location information disclosure?

RQ2: What is the distinct effect of social proof cues (present vs. absent) on mobile users' location information disclosure?

RQ3: How do information delivery mechanisms and social proof cues interact in affecting mobile users' location information disclosure?

This study contributes to IS literature in several important ways. First, we seek to shed light on the potential of two hitherto under-researched design tactics in influencing mobile users' location information disclosure outcomes in the context of mobile applications. More specifically, through a randomized online experiment in the context of a self-developed location-based coupon app called CouponMe, we analyze the effectiveness of pull vs. push information delivery mechanisms and social proof cues in increasing mobile users' actual location information disclosure. Second, we illuminate the causal pathways through which information delivery mechanisms and social proof affect location information disclosure decisions and in doing so expand the investigation of psychological processes in the privacy literature. Third, we investigate the interaction between information delivery mechanisms and social proof cues and thus illuminate whether both strategies complement or substitute one another in their impact on users' privacy-related decision making.

4.2 Theoretical Background

4.2.1 Information Privacy in Location Based Services

Information privacy is defined as the ability to control the terms under which personal information is acquired and used (France Bélanger & Robert E Crossler, 2011; Smith et al., 2011a). The tendency of firms to amass and process large amounts of users' personal data has made consumers concerned about their digital footprint and the unforeseeable consequences of their virtual consume (e.g., unveiling confidential information). Thus, companies are struggling with rising privacy concerns. In particular, providers of location-based services (LBS) (i.e., services that utilize the geographic position of users to increase effectiveness and efficiency of information provision) are struggling with privacy concerns, as consumers are becoming increasingly aware of the threats that sharing their whereabouts involves; that is, the revelation of movement patterns.

Previous research on LBS is mostly conceptual and focused on technical issues (Barkhuus, 2004; Ghosh & Swaminatha, 2001; Rodden, Friday, Muller, & Dix, 2002). Design recommendations regarding location disclosure outcomes on the other hand (i.e., share geographical position with a service provider in order to retrieve information with a higher localizability) have received only minimal research attention so far. On a high level, LBS can be differentiated in position-aware (i.e., using a devices location for a designated feature) and location tracking services (i.e., tracking users' location continuously) (Junglas & Watson, 2008). In terms of privacy concerns related to geographical information, scholars have observed that consumers are more concerned about location tracking services than about position-aware

services (Barkhuus & Dey, 2003). The reason for this is that people are more concerned when others can track their location compared to when they can disclose information at their will (Barkhuus & Dey, 2003; Junglas et al., 2008; H. Xu & Gupta, 2009). Furthermore, scholars have unveiled that users perceive stronger privacy concerns when they have to decide for the first time to disclose their location information and that these initial concerns decline after actual service usage (Barkhuus, 2004; Junglas et al., 2008; Junglas & Watson, 2008). The specific downside to sharing location information is that it bears the threat that users can be identified by their movement patterns, potentially disclosing further personal information unintentionally. Moreover, location information holds potential real-world threats such as unwanted encounters (e.g., stalking) (Bruner & Kumar, 2007; H. Xu & Gupta, 2009). Against this backdrop, it is surprising that there have been only sparse contributions towards how app providers can overcome mobile users' privacy concerns. For example, Naveen Farag Awad and Mayuram S Krishnan (2006) unveiled that despite their privacy concerns, users are willing to disclose personal information in return for personalized services. This personalization-privacy paradox encourages providers to disregard their users' privacy concerns in favor of a more personalized service. In this respect, Sutanto, Palme, Tan, and Phang (2013) picked up the personalization-privacy paradox and investigated the effect of personalization on user gratifications (i.e., consumers' gratification for the experience of the process itself or for the content it delivers) in the context of mobile applications. Their findings suggest, that information privacy and personalization need to be carefully balanced to improve users' gratifications from mobile applications. Although their research provides a first step in the direction of better understanding how the personalization–privacy paradox can be addressed effectively through technology, they do not address how technology can decimate privacy concerns. A more recent study by Gu et al. (2017) investigated how social proof and permission requests affect users' intention to download a mobile application. The study therefore is among the first to identify social proof as a potential tactic to mitigate users' privacy concerns when making technology adoption decisions. Despite this valuable contribution, there are two significant gaps that remain to be examined. First, the interplay of different permission request forms (i.e., information delivery mechanisms) with social proof. Second, the underlying psychological pathway that qualifies social proof as a strategy to mitigate privacy concerns. In sum, research thus far has focused on how app providers can predict privacy concerns and on how to balance personalization with information privacy (France Bélanger & Robert E Crossler, 2011) while more only recent studies have addressed the need for action research with an eye towards actual implementation.

In the following sections, we will focus on two key constructs of information privacy research, namely privacy concerns and trusting beliefs, which have been highlighted as important antecedents of disclosure decision making. Moreover, we will introduce two crucial design factors, information delivery mechanisms and social proof, which have the potential to alleviate privacy concerns and augment trusting beliefs.

4.2.2 Privacy Concerns

In IS research, privacy concerns have emerged as core construct of research surrounding privacy-related decision making. Privacy concerns is a global measure for four data-related dimensions, namely collection (i.e., concern that extensive amounts of personally identifiable data are being collected and stored in databases), errors (i.e., concern that protections against deliberate and accidental errors in personal data are inadequate), secondary use (i.e., concern that information is collected for one purpose but is used for another), and unauthorized access to information (i.e., concern that data about users are readily available to people not properly authorized to view or work with this data) (Smith et al., 1996). These dimensions are highly recognized among researchers (Malhotra, Kim, & Agarwal, 2004; Smith et al., 2011a) and thus made privacy concerns the most reliable scale for measuring users' concerns towards providers' privacy practices. In this regard, Smith et al. (2011a) suggested the APCO (Antecedents → Privacy Concerns → Outcomes) model, which describes privacy concerns as independent variable for privacy-related outcomes and as a dependent variable of privacy-related antecedents.

Regarding the antecedents of privacy concerns, the majority of research has investigated how individual factors such as privacy experiences (e.g., users have been victims of personal information abuse), privacy awareness (e.g., how much an individual is informed about a firm's privacy practices), personality differences (e.g., personality traits like introverts vs. extroverts), demographic differences (e.g., age, gender, and education), and culture/climate (e.g., perceptions and beliefs at societal levels) affect privacy concerns (France Bélanger & Robert E Crossler, 2011; Dinev & Hart, 2004; Smith et al., 2011a; H. Xu et al., 2008; Yun et al., 2014).

From an outcome perspective, previous literature has highlighted regulatory (e.g., privacy laws or sanctions issued by governmental bodies), attitudinal (e.g., user satisfaction or perceived risks), as well as behavioral outcomes (e.g., willingness to provide personal information or to transact) alongside moderators (e.g., trust for the exchange partner). In this respect, while privacy concerns have been identified as a prevalent cause for users to not disclose information, trusting beliefs have been highlighted as driver of information disclosure among other important

factors (e.g., satisfaction and usefulness) (Bansal & Zahedi, 2008; Culnan & Armstrong, 1999; Dwyer, Hiltz, & Passerini, 2007; Elahi, 2009; T. Li, Pavlou, & Santos, 2013; Malhotra et al., 2004; Smith et al., 2011a; Yun et al., 2014).

In sum, despite all these valuable contributions to privacy research, it comes as a surprise that only little attention has been paid towards how extant research can be leveraged to shape better location information disclosure outcomes. In line with Smith et al. (2011)'s call for research on more actionable recommendations in this regard, we intend to address this gap by examining the effects of information delivery mechanisms and social proof cues on location disclosure decisions. Our focus lies on these specific tactics, as they are intricately linked to privacy concerns and trusting beliefs – two factors that research has identified to be critical in influencing information disclosure outcomes. Moreover, both tactics promise to have distinct and joint effects on users' information disclosure decisions that are not only practically relevant but also theoretically interesting.

4.2.3 Trusting Beliefs

Trusting beliefs, which are defined as a sentiment or expectation of users about an exchange partner's dependability in protecting users' personal information (Schlosser, White, & Lloyd, 2006; W. Wang & Benbasat, 2016), are very important for information disclosure decisions and should be considered alongside users' privacy concerns (Belanger, Hiller, & Smith, 2002; Dwyer et al., 2007; Malhotra et al., 2004; Schlosser et al., 2006; Smith et al., 2011a). Extant research has identified ability, benevolence and integrity beliefs as the three key trusting beliefs (H. D. McKnight, V. Choudhury, & C. Kacmar, 2002; W. Wang & Benbasat, 2016). Ability beliefs reflect the degree to which a user is confident that a company has the skills to perform the job; benevolence beliefs reflect users confidence that a company acts in the consumer's interest; and integrity beliefs describe users' confidence that a company adheres to a set of moral principles and professional standards (Mayer, Davis, & Schoorman, 1995). Although, these beliefs are acknowledged as conceptually distinct, they are often combined into a global measure of trusting beliefs to measure an exchange partner's overall trustworthiness (Kumar, Scheer, & Steenkamp, 1995; Morgan & Hunt, 1994). Previous research has shown how trusting beliefs are able to reduce users' risk perceptions (Naveen Farag Awad & Mayuram S Krishnan, 2006; Maier, Laumer, Weinert, et al., 2015) and thereby increase their likelihood to disclose personal information (Bansal & Gefen, 2010; Junglas et al., 2008; Malhotra et al., 2004; Smith et al., 2011a). Additionally, Junglas et al. (2008) have found that individuals who are more likely to trust their social environment express fewer privacy concerns about LBS, as they

assume service providers are inclined to maintain a trust-based relationship and are therefore more likely to disclose location information.

While a great body of research has examined the influence of trusting beliefs on users' behavioral intentions (Bansal, Zahedi, & Gefen, 2016; D. J. Kim et al., 2008; Porter & Donthu, 2008), research has yet paid only minimal attention to how trusting beliefs affect actual information disclosure (Grabner-Kräuter & Kaluscha, 2003). We intend to address this gap by examining the effect of trusting beliefs on actual location information disclosure. More specifically, we examine how social proof cues, which research has explicated as an effective design cue to help users' make decisions in situations of high uncertainty (Amblee & Bui, 2011), affect actual location information disclosure through trusting beliefs. In line with Beldad, De Jong, and Steehouder (2010)'s call for research to investigate the effectiveness of trust-creating cues in diverse contexts, we aim to illuminate how the effect of social proof on actual location information disclosure is mediated through trusting beliefs in the underexplored context of LBS.

4.2.4 Information Delivery Mechanisms: Push vs. Pull

Information delivery mechanisms describe the method via which users can control how information is conveyed to and acquired from them (Kendall & Kendall, 1999). Conceptually, one can differentiate between pull- and push-based methods (H. Xu & Gupta, 2009). While pull-based delivery mechanisms are triggered via specific actions conducted by the user enabling them to direct the information flow (e.g., checking their e-mail and the inbox refreshing at that point in time), push-based mechanisms are triggered once users have agreed, at the providers' discretion and based on external events (e.g., when an incoming e-mail or a batch of e-mails have arrived) (Cheverst & Smith, 2001; Kendall & Kendall, 1999). Information delivery mechanisms have also become a critical component in software design, especially with regards to retrieving information from the user. While the default here has always been to obtain all seemingly necessary information upfront, (i.e., push-based retrieval strategies), there is a trend towards inquiring information only when it is necessary to perform user-induced actions (i.e., pull-based strategies) (Mulligan, 2014).

Among research on how information delivery mechanisms affect users' privacy related decision making, H. Xu, H.-H. Teo, B. C. Y. Tan, and R. Agarwal (2009b) are among the first who showed how information delivery mechanisms moderate privacy related decision making. That aside, previous research has been mainly focused on how information delivery mechanisms affect online marketing and advertising outcomes (Truong & Simmons, 2010; Unni & Harmon,

2007). Against this backdrop, our study aims to illuminate how pull vs. push information delivery mechanisms affect location information disclosure. Moreover, we want to investigate how users' privacy concerns mediate between information delivery mechanisms and actual location information disclosure, while previous research has highlighted privacy concerns as a salient factor of disclosure decision making (Smith et al., 2011a).

4.2.5 Social Proof

Social proof cues are signals that indicate product demand and popularity (Amblee & Bui, 2011; Cialdini, 2007; A. Lee, 2011). Firms often draw on social proof to leverage the fact that people follow each other's behavior under situations of uncertainty (Amblee & Bui, 2011; Cialdini, 2007; Cialdini & Goldstein, 2004). There are two distinct types of social proof: on the one hand, implicit social proof cues that are implemented by featuring positive messages from the media about the product or offer (e.g., Airbnb showing the press logos of the media outlets they were featured in), and on the other hand, explicit social proof cues that demonstrate quantitative figures of real customer interactions (e.g., the app store showing how often an app has been downloaded) (Amblee & Bui, 2011; Koch & Benlian, 2015). While mobile apps are digital experience goods (i.e., app usefulness and quality is difficult to assess in advance, but can be ascertained by usage), app stores implement explicit social proof cues (which are more credible than implicit cues as they reflect real consumer behavior) to help app providers build a trustworthy reputation and overcome users' uncertainty (Cialdini & Garde, 1987; Cialdini & Goldstein, 2004).

Although social proof is an established promotional cue that has been examined extensively in the online and offline world (Cialdini, 2001, 2007; Koch & Benlian, 2015), to the best of our knowledge, it has yet not been analyzed in the context of privacy decision making. Therefore, our study aims to illuminate the effect of social proof on location information disclosure as prior research provides evidence that social proof affects users' trusting beliefs, a critical driver of privacy related decision making (Amblee & Bui, 2011; Bansal et al., 2016).

4.3 Research Model and Hypotheses Development

Our research model depicted in Figure 8 shows the main and direct effects of information delivery mechanisms (pull vs. push) and social proof cues on location information disclosure (H1/H3), and the role of privacy concerns and trusting beliefs in mediating these effects (H2/H4). Lastly, it shows the joint effect of social proof and information delivery mechanisms (via privacy concerns) on actual location information disclosure (H5).

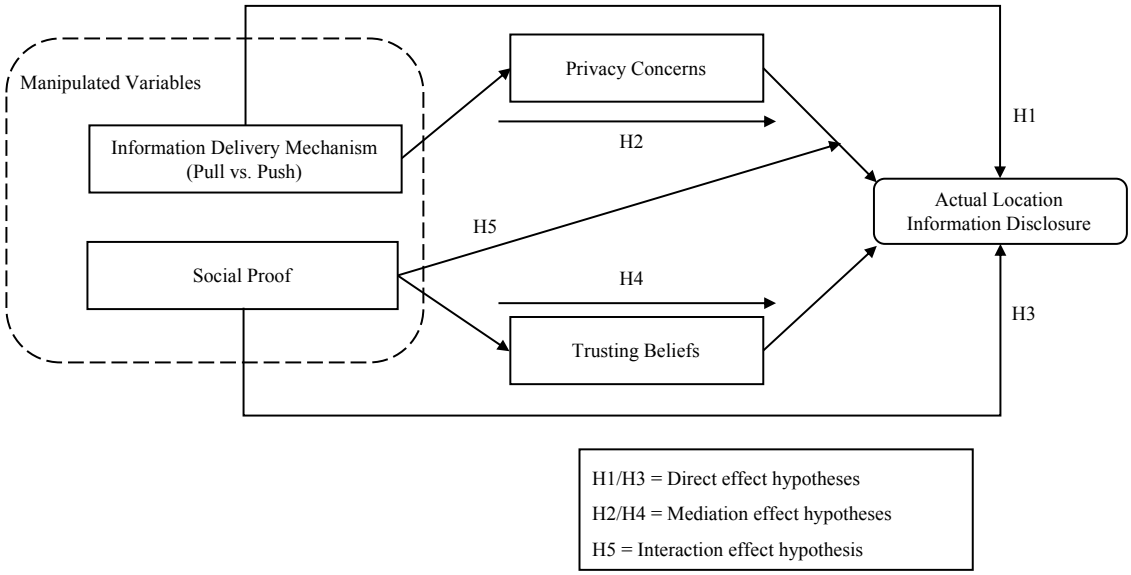


Figure 8: Research Model.

4.3.1 The Effect of Pull vs. Push Information Delivery on Location Information Disclosure

Previous research has demonstrated how pull-based information delivery mechanisms enable users to decide whether and when information exchange activities are triggered (Unni & Harmon, 2007; H. Xu et al., 2009b). Conversely, H. Xu and Gupta (2009) found that users who were asked to disclose information during app installation (push-based scenario) feel uncertain about the amount of information they are disclosing to the app provider. This is because complying with information disclosure during the installation grants providers the permission to access the information at any time in the future without the user necessarily being aware of it (e.g., camera sensor). This is especially critical in the context of location-based mobile applications where users fear that the continuous tracking of their location allows firms to make inferences regarding movement patterns, therefore revealing information which many people would like to rather keep private (Barkhuus, 2004; Barkhuus & Dey, 2003; Junglas et al., 2008). In pull-based scenarios on the other hand, users are aware of when information is being accessed, as it is inquired at the time the user triggers an action (e.g., sharing a camera photo). The contextual link (i.e., user-triggered action) to the disclosure inquiry in pull scenarios helps users understand what benefits and risks are involved in their decision and ultimately lets them decide over the amount of information they are sharing with the provider. Hence, the strong connection to the user's action also provides the ability to better assess the involved risks and benefits of their location disclosure decision (Phelps et al., 2001; H. Xu, 2007; H. Xu & Gupta, 2009). We therefore assert that pull-based (vs. push-based) information delivery mechanisms will increase users' location information disclosure.

Research has shown that information delivery mechanisms enable users to acquire and provide data on demand which in turn affects users' privacy concerns (H. Xu et al., 2009b). This is because users have lower privacy concerns when they can autonomously decide over when their information is disclosed to other entities (Foxman & Kilcoyne, 1993; Nowak & Phelps, 1997; Phelps et al., 2001). Moreover, privacy concerns have been widely acknowledged as crucial predictor of behavioral privacy outcomes like information disclosure decisions (Smith et al., 2011a). According to extant literature, lower privacy concerns lead to more desirable disclosure outcomes for the firm, be it in the form of registrations or content sharing (H. Xu & Gupta, 2009). Taken together, we suggest that the effect of pull-based information delivery on consumer location disclosure decisions is mediated by privacy concerns because pull-based information delivery decreases privacy concerns by enabling users to decide whether and when information exchange activities are triggered. These lower privacy concerns, then, lead to a higher likelihood of users complying with the initiated location information disclosure inquiry. Based on the aforementioned arguments and previous empirical findings, we derive the following hypotheses:

H1: *Users will be more likely to disclose location information in mobile apps when pull-based compared to push-based information delivery mechanisms are in place.*

H2: *Privacy concerns will mediate the effect of pull-based information delivery on location information disclosure.*

4.3.2 The Effect of Social Proof Cues on Location Disclosure

Research on social proof goes back to Cialdini and Garde (1987) who claim that under situations of uncertainty people assume the actions of others in an attempt to reflect correct behavior for a given situation. Social proof may positively affect consumer purchase intentions as it acts as social validation mechanism which signals social appropriateness, good quality and high product value (Bearden & Rose, 1990; Kardes, Posavac, & Cronley, 2004; Thies, Wessel, & Benlian, 2016). According to previous literature (Van Herpen, Pieters, & Zeelenberg, 2009), bandwagon effects explain the phenomenon that consumers have an urge to possess goods that have been purchased by others. The underlying cause is they feel that others' choices reveal superior opportunities that they do not want to miss out on. In addition, social proof also acts as collective signal of reputation that ultimately builds trust towards the provider and thus is able to drive more desirable outcomes for the firm (Amblee & Bui, 2011; Cialdini & Goldstein, 2004; Gu et al., 2017; Thies et al., 2016). That is why app store providers implement explicit social proof cues (e.g., number of app downloads or signups for a waiting list) in app description

pages to provide consumers with insights about the popularity of an application. It is important to highlight that explicit social proof cues have proven to be far more effective than implicit cues (e.g., as seen in media banners) in terms of building trust as they are perceived to be more credible (Amblee & Bui, 2011). This is because explicit social proof cues provide evidence of real customer behaviors and are typically presented by a third party (e.g., the app store). On the other hand, implicit cues, which are typically presented by the providers themselves (e.g., on their website), often raise doubts about the credibility of such information, especially when consumers are unfamiliar with the media the product is claimed to have been featured in. Based on these arguments, we focus on explicit social proof cues in our study and suggest that the presence (vs. absence) of such cues will improve consumers' likelihood of disclosing their location information.

The main reason for this effect is, we argue, that explicit social proof creates and nurtures trusting beliefs towards the provider. Research has demonstrated that social signals exercise a significant effect on trusting beliefs by helping users to better assess a provider's ability, integrity, benevolence and thus overall trustworthiness. The underlying rationale is that users who perceive high popularity create higher trusting beliefs based on a good reputation (Amblee & Bui, 2011; Gefen et al., 2003; Pan & Chiou, 2011; W. Wang & Benbasat, 2007). At the same time, trusting beliefs have also been identified as one of the most salient factors affecting information disclosure decisions (Dwyer et al., 2007; Malhotra et al., 2004; W. Wang & Benbasat, 2007). This is especially true in the context of experience goods (e.g., mobile applications) where users have no knowledge whether a product meets their expectations or is of good quality ex-ante. Pavlou (2003) for example demonstrated that higher levels of trust towards the provider enhance the probability of personal information disclosure and thus website registrations. Hence, users are more likely to disclose personal information (e.g., credit card details) to firms that they believe to be trustworthy (Malhotra et al., 2004; Moorman, Deshpande, & Zaltman, 1993). Based on the arguments and empirical findings presented above, we propose that the effect of explicit social proof cues (vs. no social proof cues) on users' location information disclosure is mediated by trusting beliefs towards the app provider.

H3: *Users will be more likely to disclose location information to an app provider when explicit social proof cues are present compared to when they are absent.*

H4: *Users' trusting beliefs towards the app provider will mediate the effect of explicit social proof cues on their location information disclosure.*

4.3.3 Moderated Mediation Effects of Social Proof Cues

According to H1 and H3, both pull information delivery and social proof cues have the ability to positively affect actual location disclosure. On the one hand, pull information delivery helps users putting them into the driver's seat when they have to disclose personal information (H. Xu & Gupta, 2009). Moreover, it enables consumers to better assess involved benefits and risks of an information disclosure trade-off, which ultimately decreases consumers' privacy concerns and, in turn, increases location information disclosure, as proposed in H2 (H. Xu, 2007). Social proof cues, on the other hand, serve as social validation mechanism which leads consumers to assume that a product is of high value and good quality (Bearden & Rose, 1990; Kardes et al., 2004; Worchel, Lee, & Adewole, 1975). Further, by suggesting high popularity and a good reputation, social proof drives consumers to belief app providers are trustworthy. Trust, which has been identified as a key construct in privacy-related decision-making (D. J. Kim et al., 2008) should in turn increase the likelihood of users to disclose their location information.

While we expect both design tactics, when employed separately, to have a positive influence on location information disclosure, we argue that, when employed together, the effect of pull-based information delivery mechanisms will be overridden by the effects of social proof cues. The basic rationale behind this is that both tactics are interconnected in affecting actual location disclosure behavior such that one effect may offset the other. As mentioned above, social proof cues are a collective signal of reputation which is not only very salient in app stores but has also been found to alter users' privacy concerns (Amblee & Bui, 2011; Cialdini, 2007; Kazai & Milic-Frayling, 2008; D. J. Kim et al., 2008; Koch & Benlian, 2015). Consistent with previous research (Gu et al., 2017; Koch & Benlian, 2015), we argue that social proof cues may moderate the effect of privacy concerns on actual information disclosure such that the effect is stronger when social proof cues are absent compared to when they are present (Schoenbachler & Gordon, 2002). The underlying logic is that the presence and saliency of explicit social proof cues are likely to ease users' privacy concerns and render them less important. Thus, given the high visibility and social validation qualities of explicit social proof cues in mobile app environments, it stands to reason that social proof cues are likely to attenuate or even cancel out the effect of pull-based information delivery on users' information disclosure via their privacy concerns. In sum, when social proof cues are present, we posit that they override (i.e., cancel out) the effect of pull-based information delivery on actual location information disclosure. We therefore propose the following hypothesis:

H5: Social proof will moderate the relationship between privacy concerns and location information disclosure such that it will attenuate or even cancel out the indirect effect of pull information delivery on location information disclosure via privacy concerns.

4.4 Research Method

4.4.1 Experimental Design and Treatments

We conducted a randomized online experiment in the context of a self-developed, fictitious mobile app called CouponMe to test our hypotheses. We chose to mimic a coupon app based on previous research (Liang, Chen, & Turban, 2009; H. Xu & Gupta, 2009) which has shown that the benefits of coupon apps are well understood among a vast majority of consumers. By using a randomized experimental design, we also assured that the app's utility and usability, by letting all users use the same app holding design and functionality constant across all experimental conditions, were unlikely to influence our results. We ensured that all subjects participated with a smart phone internet browser (by informing users that they could only participate with a mobile device) where the app was displayed in full screen mode. To increase the realism of our experiment, we drew on internet browsers' actual geolocation disclosure features to emulate the disclosure of location-based information on a smartphone. In doing so, participants were placed into a real information disclosure situation within a hypothetical scenario that was composed of an Android Playstore, an installation process of the application as well as CouponMe itself.

In line with previous research (Ho, Bodoff, & Tam, 2011; P. B. Lowry et al., 2013), we recruited participants via email from a representative subject pool maintained by a large university in Germany. The subject pool was compiled from various media channels (e.g., facebook, flyers, and online advertisement) to ensure a heterogeneous sample of smartphone users and minimize potential selection biases (MacKenzie, Podsakoff, & Podsakoff, 2011). Thus, aside from students of various majors and different semesters, it contained local residents and employees from the university site. Subjects were motivated to participate in the study in exchange for a fee of 1€. We employed a 2 (pull-based vs. push-based information delivery mechanisms) x 2 (social proof: absent vs. present) between-subjects, full-factorial design. We also conducted a power analysis using G*Power 3.1 (Faul, Erdfelder, Buchner, & Lang, 2009) with the following parameter specifications: four groups (2x2 full-factorial design), a moderate effect size ($f = 0.25$), an α-level of 0.05, and a desired power level of 0.80. The results indicated that a minimum sample size of 128 should be sufficiently powerful to detect significant effects (Baroudi & Orlikowski, 1989; J. Cohen, 1992).

The app store details page illustrated a logo, the providers name as well as a description of the application (see Figure 9) listing various benefits for consumers. Furthermore, a bar with badges provided an indicator of whether downloads for the app have surpassed a threshold (as depicted in Figure 9 and Figure 10, our manipulation of social proof which either was absent or indicated the app has reached 50 million downloads). Besides this information, the details page also contained an install button in all conditions. In the push condition, the button triggered a dialogue during installation that requested users to share their location (see Figure 11). In the pull condition, this dialogue did not surface at the time of installation, but only after the installation was completed and when users actively attempted to use the location filter functionality in the app's coupon search interface (see Figure 12).

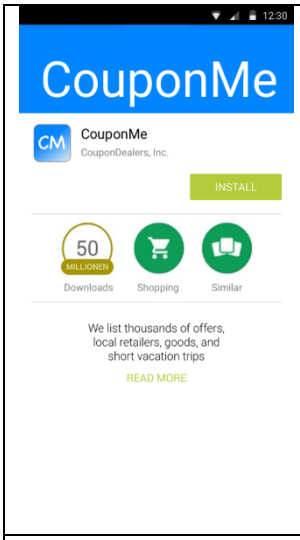


Figure 9: CouponMe App Store Page (Social Proof: Present).

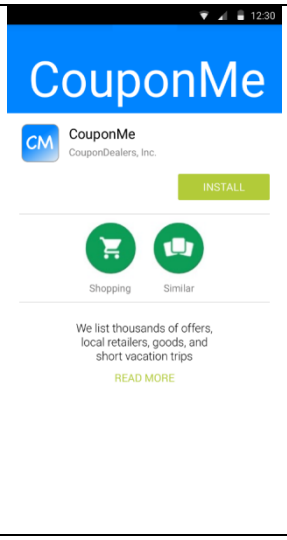


Figure 10: CouponMe App Store Page (Social Proof: Absent).

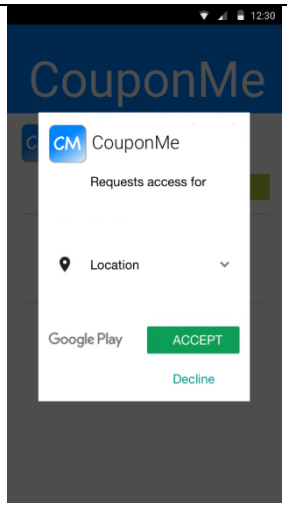


Figure 11: CouponMe Location Information Disclosure Prompt.

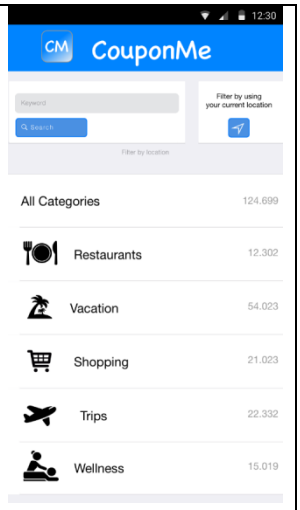


Figure 12: CouponMe Search Interface (Pull Information Delivery Mechanism).

The experiment proceeded as follows: First, participants received instructions which included detailed background information and an explanation that they were providing very early feedback for a new mobile application. They then started by pushing a continue button which lead them to the mobile app and randomly assigned them to either the social proof present or absent condition. Second, on the app store details page of "CouponMe", all participants were instructed to push the installation button which assigned them to either the pull-based or push-based information delivery condition. Pushing the installation button in the push-based information delivery condition triggered a location disclosure prompt in which they could accept or decline to disclose their location information (see Figure 11) followed by the

geolocation disclosure prompt from the respective browser. In the pull condition, pushing the install button resulted in participants being routed to an interface within the app where they were able to filter offers by their location. The location disclosure prompt was displayed only when they interacted with the location search filter, after which they were prompted to disclose their browsers' geolocation information. A post-experimental survey captured the mediation and manipulation check variables as well as several covariates. At the end of the survey, the participants were debriefed and thanked for their participation.

4.4.2 Variables Measured and Measurement Validation

Based on procedures widely used in practice, our pull vs. push information delivery manipulations were implemented by prompting the user for information disclosure at different stages of an app's lifecycle (Mulligan, 2014). In the push conditions, location information was enquired right after the app installation, while in the pull conditions the information disclosure dialogue was only initiated when users were actively looking for specific coupons and thus actually used the location filter feature in the app's coupon search interface. Explicit social proof was implemented by displaying a badge that indicated the app had reached 50 million downloads (Duan, Gu, & Whinston, 2009; Gu et al., 2017; Thies et al., 2016) (see Figure 9). In conditions where social proof was absent, we simply did not display the badge, as is common practice in the Google Playstore (see Figure 10).

To develop the stimuli for this study and evaluate the realism of our coupon app, we conducted a pretest involving 50 participants (M_{age} = 24.94; 46% male). The manipulation check of information delivery mechanisms (push vs. pull) confirmed that participants perceived greater control in pull-based M = 5.71; SD = 1.27) than in push-based M = 4.15; SD = 2.48; $F(1,48)$ = 7.61; $p < 0.01$) scenarios. Furthermore, the manipulation check for social proof confirmed that the perceived popularity of the app was higher when social proof was present M = 4.93; SD = 1.27) compared to when it was absent M = 4.18; SD = 1.22; $F(1,48) = 6.87$; $p < 0.05$) . These results confirmed our expectations that users would perceive greater control over their data for pull-based apps and that the perceived popularity of an application can be effectively influenced by displaying explicit social proof cues.

In line with previous research (Koch & Benlian, 2015; Moe & Fader, 2004; D. Schneider, 2017), we operationalized our dependent variable *actual location information disclosure* via the following point estimator:

$$P_{disclosure}(Group\ Z) = \frac{\sum_{k=1}^{n} x_k}{n}$$

where Group *Z* refers to one of the four treatments, *n* represents the total number of participants, and x_k denotes a dichotomous variable that represents the participants' actual disclosure decision, which equals 1 when a participant actually disclosed his/her location information and 0 if not. Disclosure behavior was captured via clickstream data (i.e., every user event was recorded within the experiment) that we collected during the experiment. Our mediating constructs, privacy concerns and trusting beliefs, were each measured on a 7-point Likert scale ranging from (1) strongly disagree to (7) strongly agree using three items based on Sutanto et al. (2013) and Malhotra et al. (2004) (see Appendix Table 15). Although trusting beliefs reflect multiple beliefs about a provider (i.e., integrity, benevolence, and ability beliefs), they are often combined into a global measure of trusting beliefs to measure an exchange partner's overall trustworthiness (Kumar et al., 1995; Morgan & Hunt, 1994). Following this practice, we measured trusting beliefs based on an app providers' overall trustworthiness.

We further measured the following information disclosure drivers as controls for our experiment. First, in line with H. Xu and Gupta (2009), three items were collected for previous privacy experience which reflects whether users have been victims of personal information abuse which in turn is likely to lead to greater sensitivity in terms of privacy concerns in the future. Second, we also adopted three items for prior experience in using mobile applications from H. Xu and Gupta (2009), as it is associated with a higher likelihood of users conducting a cost-benefit trade-off when making privacy-related decisions (i.e., when the benefits outweigh the costs users are more likely to disclose personal information). Third, privacy concern type, which was measured with three distinct items as well (Van Slyke et al., 2006), describes how individuals feel about information collection and usage by organizations in general (literature differentiates privacy fundamentalists, pragmatists, and unconcerned types). All aforementioned items were measured using a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7). Lastly, as previous studies have demonstrated how various demographic characteristics affect privacy concerns (K. Chen & Rea, 2004; Culnan & Armstrong, 1999; Sheehan, 1999; Sheehan & Hoy, 2000), along with gender and age, we recorded education based on Malhotra et al. (2004), with an ordinal item that ranged from (1) some school/ no degree to (6) master's degree.

As all variables showed adequate internal consistency, we averaged the items of each construct to form composite scores for further statistical analysis (see Appendix Table 16). Convergent validity was confirmed via confirmatory factor analysis (CFA) (Naveen Farag Awad & Mayuram S Krishnan, 2006). Furthermore, each scale's average variance extracted (AVE) surpassed multiple squared correlations, indicating that all discriminant validity requirements were met (Fornell & Larcker, 1981).

4.5 Results

4.5.1 Sample Description, Control and Manipulation Checks

Of the 576 individuals invited from the subject pool, 163 participated in the online experiment (response rate 28.3%). Eight participants did not complete the survey and twelve subjects were removed due to failing the attention filter questions. Thus, the final sample used for our analysis included 143 subjects – a sample size that our power analysis (see the Research Methodology section) and previous studies have shown to be sufficient for a 2x2 full factorial design (e.g. (Koch & Benlian, 2015) and (Goldbach, Kemper, & Benlian, 2014).

The average age of participants was 25 years, ranging from 18 to 31 years, while the split between males and females was 68 to 75 (see Appendix Table 16). In order to check for a non-response bias, we compared both late and early-respondents (J Scott Armstrong & Terry S Overton, 1977). The t-Tests performed on socio-demographics between the first and last 50 participants showed no statistical significance $p > 0.05$) making it unlikely that non-response bias affected the results. In addition, we conducted several one-way ANOVAs to confirm that randomization to the four experimental conditions was successful. Additionally, consistent with previous research (Koch & Benlian, 2015; N. Wang, Zhang, Liu, & Jin, 2015), to check whether our manipulations were successful, we used perceived control as manipulation check for information delivery mechanisms and perceived popularity as manipulation check for social proof cues (see Appendix Table 15). First, participants perceived greater control in pull-based $M = 4.76$; $SD = 1.82$) than in push-based conditions $M = 3.96$; $SD = 2.25$; $F = 5.37$; $p < 0.05$). Second, we were also able to confirm that perceived popularity of the app was greater when social proof cues were present $M = 4.80$; $SD = 1.54$) than when they were absent $M = 4.23$; $SD = 1.36$; $F = 5.58$; $p < 0.05$). Therefore, both manipulations were successful.

4.5.2 Main Effect Analysis for Information Delivery Mechanisms and Social Proof

We conducted a two-stage hierarchical logistic regression on the dependent variable actual location information disclosure to test our direct hypotheses H1 and H3 (see Table 13). In the

first stage, after examining the effects of the mediators and controls on location information disclosure (Block 1), we included the independent variables information delivery mechanism and social proof in the second stage (Block 2). Nagelkerke R^2 and χ^2-statistics were computed to evaluate the models' fit for both stages. None of the controls had a significant effect on location information disclosure.

	Block1		Block2	
	Coefficient	**SE**	**Coefficient**	**SE**
Intercept	2.164	2.875	1.266	3.464
Manipulations				
Information Delivery Mechanism †	-	-	1.450*	0.576
Social Proof ††	-	-	2.450***	0.629
Mediators				
Trusting Beliefs	0.547***	0.149	0.557**	0.173
Privacy Concerns	-0.742**	0.251	-1.133**	0.331
Controls				
Prior Mobile Apps Experience	0.206	0.182	0.132	0.205
Prior Privacy Experiences	-0.127	0.192	-0.101	0.228
Privacy Concern Type	0.013	0.23	0.121	0.261
Age (years)	0.091	0.076	0.126	0.089
Gender (males)	0.536	0.473	0.763	0.548
Education	-0.293	0.176	-0.298	0.203
Log Likelihood	122.512		97.455	
Nagelkerke R^2	0.477		0.622	
Omnibus Model χ^2	60.953**		86.011**	
*Note: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; N= 143; † 0 = Push, 1 = Pull; †† 0 = Absent, 1 = Present*				

Table 13: Logistical Regression Analysis on Actual Location Information Disclosure.

The results of the logistical regression demonstrated a significant effect of pull-based information delivery $b = 1.450$; *Wald statistic(1)* = 6.335; $p < 0.05$) and social proof $b = 2.424$; *Wald statistic(1)* = 14.870; $p < 0.001$) on actual location information disclosure (see Table 13). Participants were significantly more likely to disclose location information when they were treated with pull-based information delivery compared to push-based information delivery (57% vs 27%; $t = 11.89$; $p < 0.01$). Moreover, the presence of social proof cues had a statistically significant impact (64% vs. 36%; $t = 18.53$; $p < 0.01$) on actual location information disclosure.

In order to highlight the practical significance of our findings, we computed the average marginal effects of information delivery mechanisms and social proof cues (see Figure 13).

Under the assumption that all other manipulations stay equal, we found an 18.7 percentage point increase in disclosure likelihood when changing the information delivery mode from push to pull. Likewise, we would expect a 35.9 percentage point increase in location information disclosure likelihood in presence (vs. absence) of social proof cues.

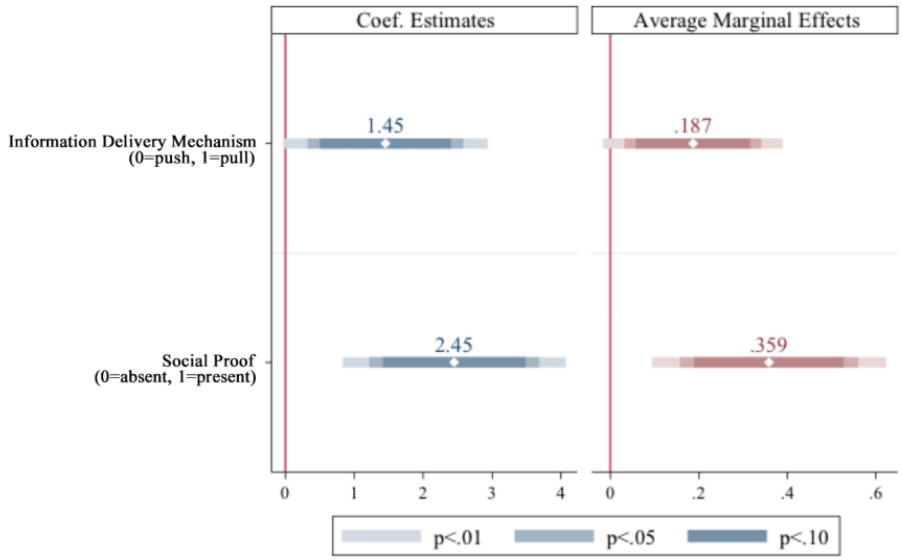


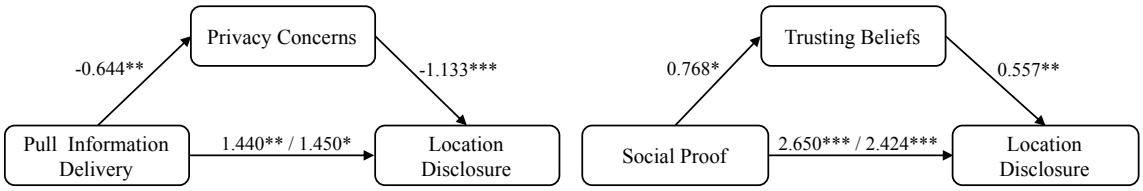
Figure 13: Coefficient estimates and average marginal effects.

4.5.3 Mediation Analysis for Information Delivery Mechanisms and Social Proof

We argued that perceived privacy concerns mediate the effect of information delivery mechanisms on actual location disclosure (H2), while we hypothesized that the effect of social proof on location information disclosure is mediated by trusting beliefs (H4). We used the bootstrap mediation technique suggested by Andrew F Hayes (2013) with 10,000 samples and a 95% bias-corrected confidence interval to examine these mediation hypotheses (see Figure 14).

First, to investigate the process driving the effect of pull information delivery on location information disclosure, we entered privacy concerns as potential mediator between the independent and dependent variable. The indirect effect of pull information delivery through privacy concerns on location information disclosure was statistically significant *indirect effect* = 0.73; *standard error* = 0.572; 95% *bias-corrected confidence interval (CI)* = [0.067, 1.853]), in support of H2. Additionally, the direct effect of pull information delivery on location information disclosure remained significant even after privacy concerns were added as mediator, representing a partial mediation (Andrew F Hayes, 2013). Furthermore, pull information delivery significantly reduced privacy concerns $b = -0.64$; $p < 0.01$), while privacy

concerns had a negative effect on location information disclosure $b = -1.13$; $p < 0.001$). Hence, the analysis confirmed that pull-based information delivery reduced users' privacy concerns and, in doing so, increased the likelihood of actual location information disclosure.



Note: The first coefficient on a given path represents the direct effect without the mediator in the model; the second represents the direct effect when the mediator is included in the model. Coefficients were computed using bootstrapping 10,000 samples and a 95% bias-corrected confidence interval (Hayes 2013). All controls as well as manipulations were included in the analysis.
** p < 0.05; ** p < 0.01; *** p < 0.001*

Figure 14: Mediation Results.

Second, to examine the process underlying the effect of social proof on the location information disclosure, we entered trusting beliefs as potential mediator into another mediation model. The results confirmed that trusting beliefs significantly mediated the effect of social proof on the location information disclosure *indirect effect* = 0.427; *standard error* = 0.28; *bias-corrected confidence interval (CI)* = [0.041, 1.004]), which is in support of H4. Adding trusting beliefs as mediator to the model, the direct effect of social proof on location information disclosure remained significant, which demonstrates partial mediation. Our results also showed that social proof positively influenced trusting beliefs $b = 0.768$; $p < 0.05$), while trusting beliefs also had a positive effect on actual location information disclosure $b = 0.557$; $p < 0.01$).

In addition, we conducted a supplementary analysis to test whether trusting beliefs qualified as a mediator for pull information delivery and whether privacy concerns qualified as valid mediator for social proof. However, both indirect effects turned out to be insignificant $p > 0.5$). In sum, the results show that both treatments have a positive and significant direct and indirect effect on users' location information disclosure. The effects occur either by decreasing privacy concerns which keeps mobile users from sharing information or by increasing trusting beliefs which improves app providers' trustworthiness.

4.5.4 Moderated Mediation Analysis for Social Proof

We hypothesized that the indirect effect of pull information delivery and location information disclosure through privacy concerns is moderated by social proof. Based on Hayes (2013), we

drew on a moderated mediation model using bootstrapping with 10,000 samples and a 95% bias-corrected confidence interval to test this conditional indirect effect.

The moderated mediation analysis was based on two separate multiple regression models. The first model included pull information delivery, social proof, and all controls as independent variables and privacy concerns as the dependent variable. The analysis confirmed a negative and statistically significant effect of pull information delivery on privacy concerns $b = -0.68$; $p < 0.01$). Consistent with Hayes (2013, model 14), the predictors in the second model included privacy concerns, social proof, the interaction term, all controls as independent variables as well as actual location information disclosure as dependent variable. The model revealed a positive and statistically significant interaction of social proof and privacy concerns $b = 2.311$; $p < 0.05$) on actual location information disclosure, demonstrating that social proof cues do interact with privacy concerns such that the relationship between privacy concerns and actual location information disclosure is weaker when social cues are present compared to when they are absent.

In addition, and more important to our theorizing, Table 14 sheds further light on the indirect effect of pull information delivery on actual location information disclosure via privacy concerns in the presence and absence of social proof cues. The results show that the indirect effect of pull-based information delivery on actual location information disclosure via privacy concerns is significant only in the absence of social proof cues *indirect effect* = 1.785; *CI* = [0.021, 6.235]) but not in their presence *indirect effect* = 0.213; *CI* = [-0.299, 1.387]), such that social proof overrides the positive effect of pull-based information delivery on location information disclosure, in support of H5.

Social Proof	**Coefficient for Indirect Effect**	**Boot SE**	**BootLLCI**	**BootULCI**
absent	1.785	2.203	0.021	6.235
present	0.213	0.520	-0.299	1.387
Note: Coefficients were computed based on moderated mediation analysis incl. all controls and using bootstrapping with 10,000 samples and a 95% bias-corrected confidence interval (Hayes 2013)				

Table 14: Conditional Indirect Effect of Pull Information Delivery on Location Information Disclosure.

Following P. Cohen, West, and Aiken (2014) procedure, we conducted a simple slope analysis and plotted the effect of privacy concerns on actual geolocation information disclosure at conditional values of social proof (i.e., absence vs. presence) to facilitate interpretation of social

proof's moderating effect. As shown in Figure 15, the effect of privacy concerns on actual location information disclosure is significant in the absence of social proof $b = -2.94$; $p < 0.05$), but becomes insignificant in the presence of social proof $b = -0.81$; $p > 0.05$). The results thus show that social proof cancels out the negative effects of privacy concerns on actual information location disclosure, providing additional support for H5.

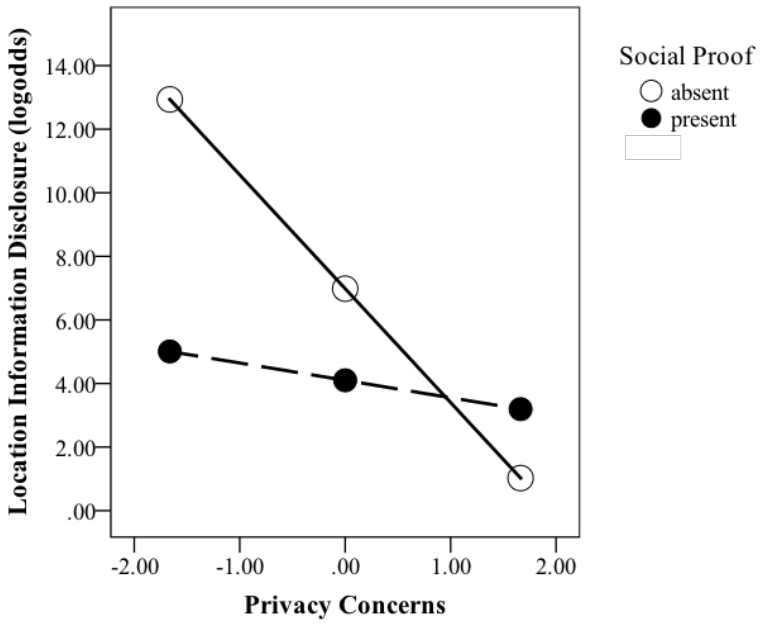


Figure 15: The Effects of Privacy Concerns on Location Information Disclosure in Absence and Presence of Social Proof.

4.6 Discussion

With the rise of the app economy and an increased demand for personalized products and services, requesting sensitive user data like geolocation information has almost become the default. While many companies have started to monetize on the collected data, users' privacy concerns have been steeply on the rise, making it challenging for app providers who do have genuine intentions to generate additional value through personalized services. While research and practice provide only little actionable advice on how to shape better privacy-related outcomes, this study aims to examine the potential of information delivery mechanisms and social proof in improving users' actual location information disclosure. Referring back to the research questions posed at the outset of this study, we can derive three important findings related to the distinct and joint effects of information delivery mechanisms and social proof cues.

First, we found that users are less concerned about pull- compared to push-based information disclosure requests and are therefore more likely to share their location information. Second,

we demonstrated that social proof increases trusting beliefs towards the provider by indicating higher popularity and social validation leading to increased location information disclosure. Third, and most interestingly, we revealed that social proof overrides the positive effect of pull-based information delivery on actual location information disclosure such that pull-based information delivery loses its effect when social proof cues come into play. The underlying rationale for this substitutive effect is that social proof cues induce popularity and social validation, which in turn moderates, or more specifically, "crowds out" the effect of privacy concerns on users' actual information disclosure decisions. Lastly, we were also able to rule out that the effects of pull-based information delivery and social proof were driven by other mediating factors such as prior privacy experiences, prior mobile app experience or privacy concern types.

This study contributes important insights to IS research on information privacy by expanding our understanding of the antecedents of privacy-related decision making in general, and geolocation information disclosure decisions in particular: First, we were able to corroborate the effect of privacy concerns on location information disclosure decisions in an randomized online experiment, which has previously been studied only with observational data (Junglas et al., 2008). We also expand on these findings as suggested by France Bélanger and Robert E Crossler (2011), who called for a more actionable stream of research on information privacy, by validating the efficacy of pull-based information delivery mechanisms as well as social proof cues in enhancing location information disclosure decisions (Gu et al., 2017; H. Xu et al., 2009b). Moreover, by investigating the interplay of information delivery mechanisms and social proof, our study sheds light on the joint effect of both design features on information disclosure decisions. In this regard, our experimental approach yielded evidence for a boundary condition of pull information delivery mechanisms; that is, they are more effective when social proof cues are absent than when they are present. Second, by drawing on privacy concerns and trusting beliefs as two salient antecedents of information disclosure decisions (Bansal et al., 2016), we explicated the psychological pathways through which the abovementioned design features shape location information disclosure decisions. We thus complement the findings of Smith et al. (2011a) by identifying relevant antecedents of disclosure decisions as well as the APCO framework by introducing an important layer of actionable levers (i.e., information delivery mechanisms and social proof cues) that emphasize tactics that effectively influence key intervening factors (i.e., privacy concerns and trusting beliefs) in the context of privacy-related decisions. Third, building on the research of Bansal et al. (2016), who showed that trusting beliefs are an important factor for users to make information disclosure decisions, we

expand the validity of their findings to location-based information disclosure decisions. In doing so, and following Beldad et al. (2010)'s call to investigate trusting beliefs' effect on actual privacy-related decision making, we provide empirical evidence for the effectiveness of social proof on actual location information disclosure through trusting beliefs in the under-researched context of LBS. Fourth, while prior research has primarily focused on disclosure outcomes in scenarios related to website registration (e.g., Pavlou, 2003, this study contributes to LBS research (Junglas et al., 2008; Junglas & Watson, 2008), which is particularly important against the backdrop of the fast-growing LBS industry.

While the preceding insights focus on contributions to research, our study's findings have several practical implications. As prior research was largely focused on how app providers can predict privacy concerns and balance between personalization and information privacy (Naveen Farag Awad & Mayuram S Krishnan, 2006; Sutanto et al., 2013), only more recent studies started to tap into unveiling how app providers can overcome privacy concerns with design tactics (Gu et al., 2017). In this respect, our results provide app providers — that do have genuine intentions to deliver additional value through personalization — with actionable strategies to increase mobile users' information disclosure decisions and decreasing privacy concerns. First, as the results imply, pull-based information delivery is a vital leverage point that could be implemented by app providers to alleviate users' privacy concerns. When users trigger the provision of information by themselves, they actively and deliberately pull the information on demand which reduces privacy concerns and increases users' actual location information disclosure. Second, explicit social proof cues may be used by app providers in their marketing efforts to increase users' trusting beliefs. Our study shows that explicit social proof cues increase a mobile application's popularity which creates trust towards the app provider, leading to higher location information disclosure. Moreover, our results show that the effect of pull-based information delivery will be overridden when explicit social proof cues are implemented simultaneously. Hence, when app providers can leverage explicit social proof cues (e.g., via app stores), they can focus more on building trust than trying to mitigate privacy concerns with pull-based information delivery mechanisms in order to increase actual location information disclosure. With explicit social proof cues being established, app providers may also benefit more from employing push-based information delivery mechanisms for actual location information disclosure to increase users' app usage comfort and provide more personalized information. On the other hand, when app providers are not able to rely on explicit social proof cues, they can draw on pull-based information delivery mechanisms, which increase actual information disclosure particularly in the absence of social proof cues. If pull-

based information delivery mechanisms are not an option (e.g., if an app is entirely dependent on access to geolocation information), it would be advisable for app providers to make their privacy practices more transparent and put users in control over their personal information. For example, app providers can install features that enable users to review and delete previously recorded location information (e.g., Google's search history) which they can promote on their app store page. Thereby, users become aware of the service provider's privacy practices and can make a better-informed choice when they have to disclose their location information.

4.6.1 Limitations, Future Research and Conclusion

Despite the contributions to research and practice discussed above, this study has some limitations which present avenues for further research. First, we conducted mediation analyses to ascertain how two design features (i.e., information delivery mechanisms and social proof cues) shape location information disclosure decisions. However, we observed partial mediation in both cases, suggesting that there are additional explanatory mechanisms at play that we did not measure in our study. Future research may analyze other potential factors that may transmit the effects of these design features. Second, we believe that the results can be transferred to mobile applications other than the one ("CouponMe") used in this study but caution should be taken from drawing conclusions more generally since this study is among few to contribute to the stream of research on LBS. Third, while our study shows that the presence of explicit social proof cues overrides users' privacy concerns, our findings should be interpreted with caution, as future studies have yet to figure out beyond which threshold levels of explicit social proof (e.g., 1.000 vs 1 million vs 50 million downloads) users' privacy concerns are attenuated and ultimately cancelled out. Furthermore, it remains to be examined at what level of explicit social proof consumers create a sufficient level of trusting beliefs to disclose their location information. We thus encourage future studies to examine various thresholds of the number of total downloads for triggering social proof effects and attenuating privacy concerns. Moreover, while our research captured trusting beliefs as a global and aggregate measure for competence, benevolence and integrity beliefs, future research should investigate how social proof shapes more specific trusting beliefs. Further, it would be highly interesting to investigate which trusting beliefs mitigate privacy concerns most effectively. Lastly, although we controlled for many constructs, there are still variables (e.g., perceived usefulness or ease of use) that should be considered for follow-up studies to further increase the internal validity of our findings (Orlikowski & Iacono, 2001). Anyhow, our full-factorial randomized experimental setup, using the same mobile application in each condition, should have ensured that such factors had no

systematic influence on our findings. Additionally, we want to encourage researchers to replicate our study within different cultures and societies.

Overall, this study illuminates the potential of information delivery mechanisms and social proof cues in separately and jointly shaping better geolocation information disclosure outcomes. We hope that this study will serve as a springboard for future research and also help practitioners in designing mobile apps that leverage the potential of LBS while mitigating mobile users' privacy concerns.

4.7 Appendix

Construct	Items	FL
Privacy Concerns (Chellappa & Sin, 2005) (CR = 0.83, AVE = 0.78)	• I am concerned that I could be identified by the company when using the application for finding Coupons around me • I am concerned with how information about me may be exploited by the company when using the application for finding Coupons around me • I am concerned with how the information captured during my use of the application to perform finding Coupons around me can be employed by the company to identify me as an individual	.85 .87 .90
Trusting Beliefs (Malhotra et al., 2004) (CR = 0.84, AVE = 0.7)	• I trust that the company providing the application would keep my best interests in mind when dealing with my information • The company providing the application would tell the truth and fulfill promises related to the information provided by me • The company providing the application is in general predictable and consistent regarding the usage of my information	.78 .89 .70
Prior Privacy Experience (H. Xu et al., 2009b)	How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers?	
Prior Experience in using Mobile applications (H. Xu et al., 2009b)	Indicate the number of times you had used mobile applications in the past six months	
Privacy Concern Type (Van Slyke et al., 2006) (CR = 0.79, AVE = 0.84)	• I'm concerned that companies are collecting too much personal information about me • Companies should have better procedures to correct errors in personal information • It usually bothers me when companies ask me for personal information	.71 .90 .88
Perceived Control (H. Xu, 2007)	How much control do you feel you have over the amount of your personal information collected by the company?	
Perceived Popularity (Van Herpen et al., 2009)	I think that many people want to download this application.	

Note: Items were measured using a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7) except for Prior Experience in using Mobile applications ranging from never (1) to 10 times and above (5), and Perceived Control ranging from none at all (1) to complete (5). FL = Factor Loadings

Table 15: Measurement Items.

	Constructs	Mean	StD	α	1	2	3	4	5	6	7	8
1	Age (in years)	25.08	3.27	-	-							
2	Gender (males)	.48	.50	-	-.19*	-						
3	Education [a]	4.75	1.75	-	.06	-.03	-					
4	Privacy Concerns [b]	5.55	1.64	.87	.12	.02	.35**	**.78**				
5	Trusting Beliefs [b]	3.50	1.80	.81	-.03	-.20*	-.10	-.16	**.70**			
6	Privacy Concern Type [b]	5.36	1.36	.82	.14	.08	.18*	.44**	-.31**	**.84**		
7	Prior Experience in using Mobile applications [c]	4.16	1.34	-	-.03	.03	.25**	.01	.00	.10	-	
8	Prior Privacy Experience [b]	5.21	1.72	-	-.00	.08	.29**	.27**	-.21*	.53**	.32**	-

*Note: N = 143; *p < .05; **p < .01; α = Cronbach Alpha; AVE (bolded cells);*
[a] Ordinal scale ranging from (1) some school/ no degree to (6) master's degree;
[b] Likert scale ranging from (1) strongly disagree to (7) strongly agree;
[c] Scale ranging from never (1) to 10 times and above (5)

Table 16: Descriptive Statistics, Internal Consistency, Discriminant Validity, and Construct Correlations.

Chapter 5: Chatbots with Low Message Interactivity and their Interaction with Platform Self-Disclosure

Title: Onboarding with a Chat – The Effects of Message Interactivity and Platform Self-Disclosure on User Disclosure Propensity

Authors: Martin Adam, Technische Universität Darmstadt, Germany
Johannes Klumpe, Technische Universität Darmstadt, Germany

Published in: European Conference on Information Systems (ECIS 2019), Stockholm-Uppsala, Sweden

Abstract

Activating users on online platforms is a critical endeavor that requires the employment of adequate user onboarding strategies, which focus on converting visitors into revenue-generating users. Despite a robust understanding of the antecedents of user onboarding behavior, researchers have devoted only little attention towards how platforms can actively influence desired user onboarding outcomes. Drawing on social response as well as social exchange theory, this study examines how disembodied interfaces like chatbots can facilitate the user onboarding process. In cooperation with a German startup company, we empirically tested in a randomized field experiment with 2095 visitors how low vs. high message interactivity (i.e., static vs. conversational presentation of requests) and platform self-disclosure (i.e., a platform providing information about itself) affect user disclosure propensity (i.e., likelihood that a user discloses information). Our results demonstrate that users in high message interaction conditions were significantly more likely to self-disclose in contrast to low message interaction conditions, while platform self-disclosure had a significant positive effect as well. Furthermore, high message interactivity significantly amplified the effect of platform self-disclosure on user disclosure propensity in contrast to low message interactivity. Consequently, our study provides novel findings on the effectiveness of disembodied interfaces to improve user onboarding behavior.

Keywords: Human-Computer-Interaction, User Onboarding, Chatbot, Message Interactivity, Social Exchange, Information Disclosure

5.1 Introduction

Nowadays, platform providers heavily struggle to turn visitors who reach their website into revenue-generating users. In fact, 96% of all website visits do not conclude in a purchase (Statista, 2018), and less than 25 percent of new app users return the day after the first use (Grennan, 2016). One of the reasons for this failure is that platforms face visitors with increasing privacy concerns and fears of privacy invasions due to platforms' tendencies to amass, process, and exploit users' personal data. Several studies in information systems (IS) have demonstrated that privacy concerns can thus hinder the willingness to accept new technologies (Corey M Angst & Ritu Agarwal, 2009), engage in e-commerce (Dinev & Hart, 2006a), and disclose personal information (Y. Lu, Tan, & Hui, 2004). User onboarding strategies can address these challenges and assist visitors in overcoming their initial reservations by methodologically educating these visitors about a platform's digital products (i.e., onboarding) and thereby driving desirable business outcomes (e.g., user sign-ups and revenue generation) (Nielsen Holdings, 2013).

Conversational agents (CAs), such as chatbots, are "user interfaces that emulate human-to-human communication using natural language processing, machine learning, and artificial intelligence" (Schuetzler, Giboney, Grimes, & Nunamaker, 2018, p. 283). These technological artefacts are considered potential cost-effective solutions (e.g., Hopkins & Silverman, 2016; Oracle, 2016) and may define the future of user-provider interactions (e.g., Knight, 2016; Knijnenburg & Willemsen, 2016; Luger & Sellen, 2016). CAs have become especially important in customer service contexts (e.g., Gnewuch, Morana, & Maedche, 2017; Wuenderlich & Paluch, 2017), where chatbots are of particular interest: For example, chatbots alone are expected to assist businesses in saving $8 billion per year in customer supporting costs by 2022 (Reddy, 2017). Thus, chatbots may pose strategic tools to facilitate user onboarding in various service encounters.

Although considerable research on the design of CAs has been conducted in IS, computer science, human-computer interaction (HCI), and adjacent fields, only few studies have tackled CAs in the context of user information disclosure success with regards to the design and incorporation of potential social cues (i.e., features that trigger social responses in individuals). Moreover, while prior studies on CAs have provided valuable contributions to research and practice (e.g., Hess, Fuller, & Campbell, 2009; Qiu & Benbasat, 2009a), their research primarily focused on embodied CAs that heavily rely on visual cues (e.g., physical embodiments). Yet, chatbots as disembodied CAs (Araujo, 2018) are considered significantly different from other

CAs, as they influence user perception primarily through verbal (e.g., small talk) and nonverbal cues (e.g., blinking dots) (Seeger, Pfeiffer, & Heinzl, 2018).

Accordingly, one of the prevailing questions that is still unfathomed is how message interactivity (i.e., the dependency of a message on another message) as a nonverbal cue influences user perception and behavior. More precisely, no study has compared how an interactive, conversational presentation of requests like in a human-human-interaction (i.e., a new question is only stated once the former question has been answered) impacts user onboarding behavior in contrast to a low interactive presentation of requests like in a classic form, in which all requests are presented at once in the beginning. Furthermore, although self-disclosure (i.e., process in which an actor self-discloses information to another person) has already proven impactful in face-to-face conversations (e.g., Collins & Miller, 1994), online user interactions in social media and forums (e.g., Barak & Gluck-Ofri, 2007; R. Lin & Utz, 2017), and conversations in HCI (e.g., S. Lee & Choi, 2017; Moon, 2000), this influence has not been investigated (1) in a field study to investigate actual user onboarding behavior, (2) in disembodied CAs that disclose information about their service platforms and not necessarily only about themselves, and (3) with regards to potential interactions with message interactivity. Indeed, both the underlying interactive design of chatbots and the reciprocal information disclosure are based on common human-human interactions where information is exchanged and revealed turn by turn and one after another. Thus, both cues are frequently used together in practice. Therefore, it is of utmost interest to analyze whether their underlying effects complement or substitute each other, as past studies have already indicated that different cues in CAs may interact surprisingly with one another (e.g., Seeger et al., 2018). The results of the investigation will provide learnings for both research and practice about the effects of employing these cues and whether there is benefit of using them together. Thus, to fill this gap, we raise the research question:

RQ: How do message interactivity and platform self-disclosure – in isolation and in combination - affect user onboarding behavior?

To answer this question, we conducted an online field experiment with 2095 participants in cooperation with a German startup company. Precisely, we empirically validated how message interactivity and platform self-disclosure, in isolation and in combination, affect user onboarding behavior at the example of user disclosure propensity (i.e., the likelihood that a user discloses information).

In doing so, we intend to contribute to research and practice in several important ways. First, following the call for increased research on the design of CAs (e.g., Gnewuch et al., 2017; Seeger et al., 2018), our study departs from prior research by investigating the effects of a verbal and a nonverbal cue in disembodied CAs like chatbots, which have been neglected in past studies. Second, our piece of research intends to reveal an interplay between these two cues, which have not been scientifically investigated together, though their combination seems intriguing and may reveal surprising interactions (e.g., Seeger et al., 2018). Third and lastly, our endeavour also aims to provide actionable and generalizable recommendations for practitioners by highlighting how highly interactive conversational interfaces, such as chatbots, can have a positive impact on user onboarding behavior in contrast to classic static forms that are widely deployed today.

5.2 Theoretical Background

5.2.1 User Onboarding

User onboarding is "the sum of methods and elements helping a new user to become familiar with a digital product. By providing onboarding mechanisms, users will be enabled to smoothly pass into the efficient usage of the digital product" (Renz, Staubitz, Pollack, & Meinel, 2014, p. 1, p. 1). Consequently, enhanced onboarding can help users in better evaluating a platform's products, while platform providers benefit from additionally generated revenues.

Facing the different stages of the conversion funnel (i.e., non-visitor, visitor, authenticated user, and converted customer) and the comparably high cost of user acquisition (i.e., turning non-visitors to visitors) (Gallo, 2014), platform and specifically app providers shift their attention towards increasing user activation outcomes (i.e., turning visitors into registered users) (Kireyev, Pauwels, & Gupta, 2016; Novak, Hoffman, & Duhachek, 2003). Extant research has unveiled a psychological disposition of new users to underestimate the benefits of unfamiliar products or services during user activation (Gourville 2006). That is why new users need to understand a product's scope and concept rapidly or they will churn away (Cooper et al. 2007). Consequently, user onboarding has become the most critical step in the user journey, as it assists users in understanding the value of the presented product as well as in convincing to capture it (Murphy, 2016).

Extant literature has investigated user onboarding mainly along two streams, namely organizational socialization and gamification: First, organizational socialization refers to utilizing user onboarding tactics to introduce new individuals to become members of an

organization (Bauer & Erdogan, 2011). Second, gamification literature has investigated how game design elements can help in meaningfully engaging new users in HCIs (Liu, Santhanam, & Webster, 2017). Albeit, these valuable contributions research has only recently started to investigate the concept of user onboarding to improve a new user's success with a product or service. A focal point of this nascent research stream has been to cluster typical design patterns which are used to improve user onboarding (Renz et al., 2014) and to investigate the long-term effectiveness of user onboarding on users' intentions to continuous use (Cardoso, 2017). Yet, despite tremendous efforts and research on antecedents of decision-making across the conversion funnel, actionable design recommendations to improve activation outcomes have received only little attention and are yet to be fathomed (Kireyev et al., 2016; Murphy, 2016; Novak et al., 2003).

5.2.2 Social Response Theory

Social response theory (Nass & Moon, 2000; Nass et al., 1994) constitutes that individuals tend to perceive HCIs as social encounters. Accordingly, individuals instinctively treat computers as social actors, even if they know that their counterpart is a mere computer. This inclination and the resulting social responses become even stronger the more social cues (i.e., features that are usually related to human behavior, such as language and turn-taking) the computers display (Moon & Nass, 1996; Nass, Moon, Fogg, Reeves, & Dryer, 1995). Thus, explicit and inexplicit rules that normally guide human-human-interactions and emerge from social norms (i.e., standards that are comprehended by members of a group and that guide social behavior) (Cialdini & Trost, 1998) can be transferred to HCI (e.g., Fogg & Nass, 1997; Nass, Moon, & Carney, 1999).

Numerous studies in HCI have demonstrated how the employment of CAs as well as the implementation of a few social cues can improve desirable business outcomes, such as purchase intention and company perceptions (e.g., Hess et al., 2009; Qiu & Benbasat, 2009a). Yet, most of this research focused on embodied CAs (Araujo, 2018) and neglected the newly establishing disembodied CAs like chatbots, which majorly employ and rely on verbal (e.g., small talk) and nonverbal cues (e.g., blinking dots), except for the normally static profile picture. Thus, though heavily applied in practice, disembodied CAs and their related cues are understudied in research (Araujo, 2018; Seeger et al., 2018).

5.2.3 Interactivity and Message Contingency

The term *interactivity* comprises "technological attributes of mediated environments that enable reciprocal communication or information exchange, which afford interaction between communication technology and users, or between users through technology" (Bucy & Tao, 2007, p. 647). *Web interactivity,* in this regard, can be defined as "interactive features embedded on computer website interfaces that allow reciprocal user-to-system or user-to-user communication" (Yang & Shen, 2017, p. 3).

Of the three distinct dimensions normally associated with web interactivity (i.e., modality, message, and source) (Sundar, 2012), *message interactivity*, which is defined as message contingency in that the "systems' output is contingent upon the user's output" (Guillory & Sundar, 2014, p. 3), is most essential to the user interaction with chatbots and has been found to be particularly essential in two-way communications like chat rooms or between users and website systems (Z. Jiang, Chan, Tan, & Chua, 2010; Tedesco, 2007). In fact, the sequential turn-taking, also known as the "conversational ideal" (Sundar, Bellur, Oh, Jia, & Kim, 2016), is a core characteristic of human-human-interaction and could thus be considered a separate nonverbal social cue, which has so far been unreflectively employed in several HCIs and specifically CA interactions (e.g., Cole et al., 2003; Häubl & Trifts, 2000; J. Xu, Benbasat, & Cenfetelli, 2010). Indeed, researchers have neglected a direct comparison of a turn-taking chatbot interaction with the chatbot interface-enabled alternative of showing all possible conversation turns at once, like it is abundantly done in common forms where all statements and inputs are revealed initially to the user.

5.2.4 Social Exchange Theory and Reciprocal Self-disclosure

Social exchange theory suggests that individuals establish mutual obligatory exchange relationships with other parties that are kept and developed by adhering to reciprocity norms, whereby positive or negative actions cause obligations to respond with similar actions, so that behaviors are normally repaid in kind (e.g., Blau, 2017; Cropanzano & Mitchell, 2005; Gouldner, 1960). The term *reciprocity* refers to the pan-cultural norm to repay any favor (e.g., benefits, gifts, treatments) received by an individual from another person (Sprecher, Treger, Wondra, Hilaire, & Wallpe, 2013) and can be comprehended as the perception of give-and-take in interactions (Weiss & Tscheligi, 2013). Moreover, the rule of reciprocity is considered elemental in human behavior (Gouldner, 1960), so that reciprocity can assist in creating the illusion that an agent is realistic (Becker & Mark, 1999).

Self-disclosure refers to any personal information that a social actor reveals to a different social actor (e.g., Collins & Miller, 1994; Wheeless & Grotz, 1976). Self-disclosure is essential for developing and keeping a relationship and decreases uncertainty between two actors by providing a means for reciprocal exchange of information (Collins & Miller, 1994). Extant literature has investigated self-disclosure along two different information revealing outcomes. On the one hand, research has aimed to unveil how individuals can be driven to disclose their inner feelings and overcome response biases (i.e., tendencies for users to respond inaccurately) (Jiang et al. 2013; Wakefield 2013). On the other hand, self-disclosure has been investigated as the disclosure of personal information during digital user journeys where users' privacy concerns are driven by the users' scrutiny towards the privacy practices of the information acquiring party (Klumpe et al. 2019; Lowry et al. 2011).

There is a significant body of literature that deals with self-disclosure and the dynamics associated with it. For instance, streams of research focused on social desirability bias (e.g., R. J. Fisher, 1993; Mick, 1996). Still other research has investigated the influence of interviewer variability (e.g., Bailar, Bailey, & Stevens, 1977; Webster, 1996) or liking (e.g., L. C. Jiang, Bazarova, & Hancock, 2011; Kashian, Jang, Shin, Dai, & Walther, 2017). Regarding CAs, researchers have analyzed aspects such as socially desirable responding (Schuetzler et al., 2018) and demonstrated that individuals can develop a relationship with a computer through the process of reciprocity and self-disclosure (S. Lee & Choi, 2017; Moon, 2000). In our study, we depart from prior research by empirically investigating the power of reciprocal self-disclosure in a real user onboarding setting with a chatbot that reveals information about the platform and not necessarily about itself (e.g., Saffarizadeh, Boodraj, & Alashoor, 2017; Zimmer et al., 2010), thus complementing prior research with actual user behavior in interactions with disembodied CAs.

5.3 Research Model and Hypothesis Development

As depicted in Figure 16, our research model examines the effects of high message interactivity (MI) and platform self-disclosure (PSD) on user disclosure propensity (H1/H2) as well as the role of MI in moderating the effect of PSD on user disclosure propensity (H3). Thus, we intend to investigate the isolated and combined effects of our chosen social cues.

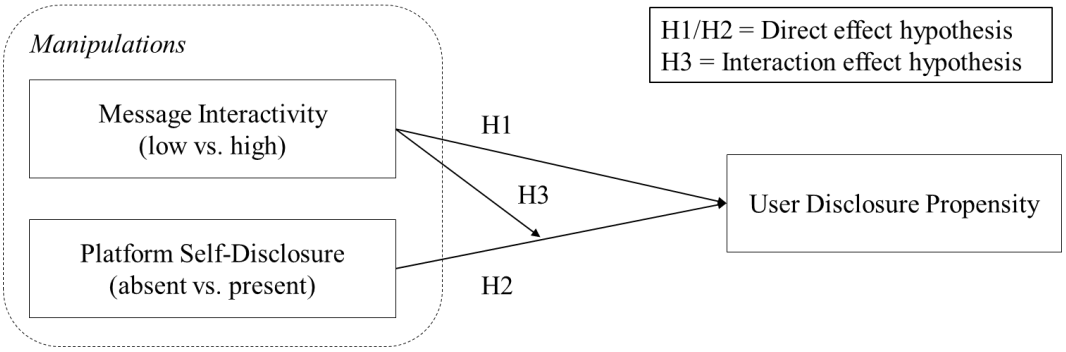


Figure 16: Research Model.

5.3.1 The Effect of Message Interactivity on User Disclosure Propensity

As described earlier, we intend to investigate what will happen when the requests are low in message interactivity, so that all questions are presented at once at the beginning like in a classic computer form, in contrast to a high message interactive condition, when the questions are presented stepwise and conversational like in a dynamic dialogue. Social response theory (Nass & Moon, 2000) suggests that the more social cues are present, the more will a user perceive a CA as a social actor (Nass et al., 1994), making the user respond more socially. Thus, the conversational turn-taking in a high message interactive condition may improve the perception of the chatbot as a social actor in contrast to a low message interactive condition, as one more essential nonverbal social cue is included in the former.

Indeed, research has shown that interactivity is related to the perception of social presence which has been found in studies on CAs as well. For instance, Skalski and Tamborini (2007) demonstrated that perceived interactivity can influence social presence, information processing, and persuasion. Regarding social presence, research on embodied CAs revealed that it directly influences trusting beliefs, perceived enjoyment, and ultimately usage intentions (e.g., Hess et al., 2009; Qiu & Benbasat, 2009a). Trusting beliefs, furthermore, were shown to influence privacy concerns as well as to increase user disclosure propensity (e.g., Smith, Dinev, & Xu, 2011b; Taddei & Contena, 2013). Consequently, based on previous research on the positive effects of interactivity on business-oriented outcomes and related research on CAs that linked these effects to other outcomes on user behavior and intentions, we hypothesize that high (vs. low) message interactivity can increase user disclosure propensity.

H1: *High (vs. low) message interactivity will positively affect user disclosure propensity.*

5.3.2 The Effect of Platform Self-Disclosure on User Disclosure Propensity

A considerable amount of research has used social exchange theory to explain the reciprocation of favorable and unfavorable behaviors between parties (Cropanzano & Mitchell, 2005) and found disclosure reciprocity as a meaningful social norm in many social exchange contexts (e.g., Cropanzano & Mitchell, 2005; Sprecher et al., 2013). When two individuals encounter each other, the ability to build rapport is contingent on both parties to reciprocate in a dialogue (Collins & Miller, 1994; Sprecher et al., 2013). Normally, adhering to social norms improves the relationship, while violating hurts it (e.g., Collins & Miller, 1994; Sprecher et al., 2013). Consequently, if a party fails to reciprocate, the relationship will less likely have a positive development (Sprecher et al., 2013).

Applied to our experiment, social exchange theory suggests that if a platform gives away a piece of information, the user tends to respond by providing a piece of information of similar value to adhere to social norms. Indeed, past studies on website disclosure (e.g., "unreasoned dyadic relationships" defined as the platform discloses information first before asking for similar information) (e.g., Zimmer et al., 2010) have already indicated this reaction, in that a user may perceive an appropriate and non-manipulative self-disclosure as a rewarding outcome and a cue to build trust (Collins & Miller, 1994), hence appreciating the action (Emerson, 1976) and tending to mimic the behavior (Chartrand & Bargh, 1999). Actually, reciprocal self-disclosure may even pose such a strong social norm that even information disclosure by a computer may be considered a verbal social cue and can, thus, create the perception of a social actor (Nass et al., 1994). Consequently, platform self-disclosures may create feelings of imbalance in users that are usually only created in human-human-interactions. As a result, a user desires to restore equality in the relationship (Sprecher et al., 2013) and reestablish an equilibrium with the computer (Homans, 1958). Thus, we expect that the self-disclosure of the platform in a disembodied CA will cause the user to self-disclose information more likely.

H2: *Platform self-disclosure will positively affect user disclosure propensity.*

5.3.3 The Moderating Role of Message Interactivity on the Effect of Platform Self-Disclosure on User Disclosure Propensity

Previous research has shown that social cues may surprisingly interact with each other, increasing the perception of social presence and related dimensions (e.g., Seeger et al., 2018). Regarding the effects of our investigated cues, the high message interactivity condition with its sequential turn-taking as a nonverbal cue, also known as prerequisite of the "conversational ideal" (Sundar et al., 2016), may be so essential that other cues can develop their potentials

more effectively in its presence. The verbal social cue self-disclosure may be a specifically intriguing candidate, as both cues are fundamental in common human-human interactions where information is exchanged and revealed turn by turn and one after another: Whereas high message interactivity is defined as one message is contingent on and only revealed after another message, reciprocal self-disclosure is built on the concept that one party starts to self-disclose so that the other party can socially respond by self-disclosing as well. Therefore, the perception of a give-and-take information exchange may flourish better when a user perceives a sequential turn-taking in form of high message interactivity, so that the user reasons that his or her self-disclosure has consequences on the conversation and, thus, on the relationship and following interaction between the user and the chatbot. Consequently, we believe that when both cues are presented together, they increase the chances that users will disclose information, in that high message interactivity enhances the effect of platform self-disclosure.

H3: *High message interactivity will moderate the effect of platform self-disclosures so that high message interactivity will enhance the effect of platform self-disclosures on user disclosure propensity.*

5.4 Research Methodology

5.4.1 Experimental Design and Procedure

We employed a 2 (MI: low vs. high) x 2 (PSD: absent vs. present) between-subject, full-factorial design to conduct both relative and absolute treatment comparisons and to isolate individual and interactive effects on information self-disclosure. The hypotheses were tested by means of a randomized field experiment in the context of a real online platform of a German startup company that provides a free matching service for students and companies based on interests in topics for university-related Master theses. We selected that startup company for three main reasons: First, startup companies usually lack an established customer base and are, therefore, highly dependent on acquiring new users. Second, startup companies find it usually hard to compete against and stand out from established companies and are, consequently, highly dependent on providing visible value and perceivable distinction, which can be amended by using new technologies such as CAs. Third, the startup company we worked with usually provides the service once to each of its active users, so improving user onboarding and convincing users to commit to related activities and products, such as newsletter signups and user referrals, is highly important for the company. For example, with the newsletter signups, the company cannot only inform users about new topics and lure them back to the website, but it can also generate revenues by placing advertisement in its newsletters.

In our field study, the instant messaging interface was self-designed and asked in all conditions for textual input. Consistent with previous studies and often applied in practice (e.g., Burger, 1999), we used the foot-in-the-door technique in all conditions in form of a continued-questions procedure in a same-requester/no-delay situation (see Figure 17): (1) First, a new website visitor was randomly assigned to one of the four conditions and (2) shown an instant messaging interface as a pop-up in which the interface introduced itself to assist the user in finding a topic for a potential thesis according to the user's interest. If the user did not want to use the interface, the user could easily just close the pop-up at the beginning or during the interaction with the interface and continue on the page. If the user decided to use the interface, he or she saw the design and content of the interface based on the condition that was assigned. (3) In all conditions, three questions about thesis- and company-relevant information (i.e., degree, major, and desired state of the company to be located) was asked first, which represented rather insensitive data of the user, since the given information applies to various people but still created involvement as participants had to answer them completely and truthfully to proceed and end up with personalized recommendations that fit to them. (4) Subsequently, depending on the condition and manipulation, the platform self-disclosed information through the interface by providing its service e-mail or presented a filler that did not contain any self-disclosure (see next section). (5) Afterwards, we placed our target request, which was one question about a potential newsletter sign-up, in which users had to respond with their personal e-mail address, if they wanted to sign-up. Otherwise the user left the field empty. Consequently, the target request was more sensitive since it asked for more intimate and user-unique information. (6) To proceed to the topics for a potential thesis, the user eventually clicked on a button and was sent to a different page with topics that were filtered based on the user's entries.

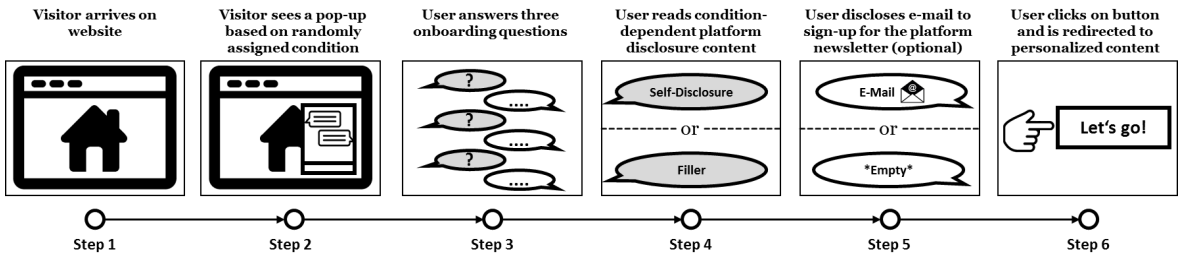


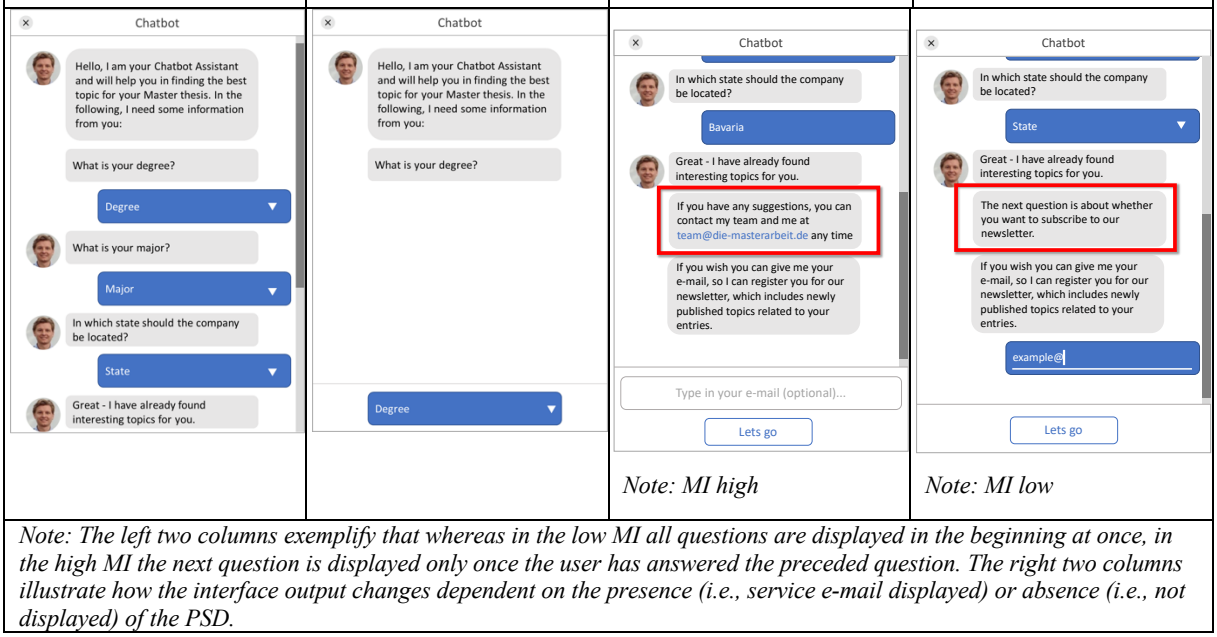
Figure 17: Experimental Procedure.

5.4.2 Manipulation of Independent Variables

Consistent with previous research on MI (e.g., Z. Jiang et al., 2010), we defined and manipulated MI as either low or high. In the low MI condition, all questions were shown at once in the beginning, so that a user immediately saw how many questions he or she had to

answer to proceed to the next page. In contrast, the high MI condition presented the questions one after another, so that the user could see only one question at a time and proceed only if he or she answered the question. The questions in both conditions could be answered through one of two predefined kinds of input fields, which are often applied in chatbots in practice: (1) The user could answer the first three questions by selecting one of the predefined answers in a drop-down list, as the website required a certain degree of input control to further process user input in its user-thesis-matchmaking. (2) The user could answer the target question about a potential newsletter sign-up with his or her e-mail in a free text input field (i.e., "Type in your e-mail (optional)…"). In the low MI condition, the input fields were located where the user's responses would normally be placed in a chat record. In the high MI condition, the input fields where placed at the bottom of the interface where they are usually displayed in turn-by-turn chatbot interactions (see Figure 18).

The target question, whether the user wants to sign-up for the newsletter with his or her e-mail, was preceded by a statement that was dependent on the presence or absence of the PSD. In accordance with past experiments on reciprocal interactions with computers (e.g., Moon, 2000), the platform first self-disclosed in the PSD present condition by providing its service e-mail through the interface before asking the user for his or her e-mail. Thus, we depart from prior limited research on disembodied CA self-disclosure (S. Lee & Choi, 2017; Saffarizadeh et al., 2017) by focusing on platform-related self-disclosure through the chatbot. Precisely, consistent with previous research (e.g., "We can be contacted at jmeyer@webmd.com" (Zimmer et al., 2010, p. 404)), we operationalized PSD in that the chatbot revealed information about the platform's customer service and not directly about itself: The chatbot provides a service e-mail for further customer support and not a private one (i.e., "In case you have any suggestions, feel free to contact my team and me at team@die-masterarbeit.de any time."). In doing so, we manipulated PSD as a piece of information that an automated first-level support in practice could provide to assist the user if the user requires human second-level support. In the PSD absent condition, to avoid confounding effects such as questions length (e.g., Koomen & Dijkstra, 1975), we followed Moon (2000) and showed a statement that did not contain any computer-disclosure content, but contained the same number of words as in the PSD present (untranslated) condition.



Note: The left two columns exemplify that whereas in the low MI all questions are displayed in the beginning at once, in the high MI the next question is displayed only once the user has answered the preceded question. The right two columns illustrate how the interface output changes dependent on the presence (i.e., service e-mail displayed) or absence (i.e., not displayed) of the PSD.

Figure 18: Translated excerpts from the experimental conditions.

We developed our stimuli and evaluated the success of our manipulations by replicating the experimental design and conducting a pretest in form of an online experiment, involving 160 students (mean age = 23; 63% male). Students were explicitly chosen as they would represent the customer group that would also visit the start-up website. We incentivized participation through a voluntary raffle of three Euro 20 vouchers for Amazon and exposed each participant to one of the four aforementioned conditions. Instead of user disclosure propensity, we measured Social Presence (Gefen & Straub, 2003) in a post-experimental questionnaire, as this variable has demonstrated to be essentially related to social cues (e.g, Qiu & Benbasat, 2009a) as well as interactivity (e.g., Skalski & Tamborini, 2007). Indeed, participants perceived greater Social Presence when they were exposed to a high MI ($M = 3.45$; $StD = 1.37$) compared to when they were exposed to a low MI ($M = 2.71$; $StD = 1.46$; $F(1,159) = 11.16$; $p < 0.01$). Likewise, participants that encountered PSD perceived greater Social Presence ($M = 3.33$; $StD = 1.39$) than when PSD was absent ($M = 2.79$; $StD = 1.49$; $F(1,159) = 5.65$; $p < 0.05$). Consequently, the results of our pretest indicated that our manipulations should also be successful on the real platform.

5.4.3 Dependent Variable and Control Variables

We measured user disclosure propensity based on a binary variable, defined as a point estimator P :

$$P \quad (\text{user disclosure propensity}) = \frac{\sum_{k=1}^{n} x_k}{n}$$

where n denotes the total number of unique new website visitors in the respective condition who finished the interaction (i.e., answering all three mandatory questions and hitting the proceed button) and x_k is a binary variable which equals 1 when the user self-disclosed by inserting an e-mail and 0 if not. Furthermore, in case the user provided his or her e-mail, an e-mail was sent to the mentioned address to verify and confirm the active usage of that e-mail by the user.

Moreover, we also checked for various control variables: First, we measured whether users used a mobile device to visit the website. Second, we recorded the day the user participated in the experiment. Lastly, we measured the total time of the session duration that the user needed to complete the journey.

5.5 Results

5.5.1 Sample Description and Control Variables

We recorded all our variables via clickstream analysis over a 30-day period in March and April 2018. From 2095 visitors with a unique IP address, 202 used the interface till the end (8.4% conversion rate). We eliminated 26 subjects that disclosed false email addresses, resulting in a sample size of 176 subjects (see Table 17, Table 18). Regarding our dependent variable disclosure propensity, the distribution of disclosures across the experimental groups was as follows: In conditions where MI was low, disclosure propensity was 15% when PSD was absent and 26% in the presence of PSD. While in conditions where MI was high, disclosure propensity was 19% when PSD was absent and 68% in the presence of PSD.

	Total	Low MI x PSD absent	High MI x PSD absent	Low MI x PSD present	High MI x PSD present
Participants	2095	523	501	569	502
Mobile Usage	1617	394	400	440	383
Submitted	202	46	40	53	63

Table 17: Descriptive Statistics of Website Visitors.

	Mean	StD
Dependent Variable		
Disclosure Propensity	0.27	
Independent Variables & Controls		
MI (low=0, high=1)	0.38	
PSD (absent=0, present=1)	0.52	
Mobile Usage	0.98	
Experiment Day (days)	13.07	7.882
Duration of Session (seconds)	44.06	23.795

Table 18: Descriptive Statistics of Analyzed Data Set.

In order to confirm the randomized assignment of the participants to the experimental conditions, we conducted several one-way ANOVAs. We found no statistically significant difference in mobile usage ($F = 0.628$; $p > 0.05$), day of the experiment ($F = 0.437$; $p > 0.05$), and session duration ($F = 0.446$; $p > 0.05$) between all experimental groups, which confirmed that the randomization was successful.

5.5.2 Main Effect Analyses for MI and PSD

To test H1 and H2, we conducted a three-stage hierarchical logistic regression on the dependent variable user disclosure propensity. First, we included all control variables (Stage 1), then we added the independent variables MI and PSD (Stage 2), and lastly we inserted the interaction term of MI x PSD (Stage 3). Our results showed that both MI and PSD significantly affected user disclosure propensity (see Table 19).

Intercept	Stage 1			Stage 2			Stage 3		
	Coeff	*StE*	*Exp(B)*	*Coeff*	*StE*	*Exp(B)*	*Coeff*	*StE*	*Exp(B)*
Constant	-2.091	1.431	.124	-4.438**	1.537	.012	-4.143**	1.572	.016
Manipulations									
MI †				1.830***	.421	6.235	.813	.593	2.256
PSD ††				1.208**	.409	3.345	.272	.555	1.312
MI x PSD							1.766*	.799	5.846
Controls									
Mobile Usage	.407	1.325	1.503	.705	1.315	2.025	1.066	1.376	2.904
Experiment Day	-.018	.023	.982	-.008	.026	.992	-.010	.026	.990
Duration of Session	.020**	.007	1.021	.029***	.008	1.029	.029***	.008	1.030
Nagelkerke's R^2	.074			.265			.297		
-2 (Log-Likelihood)	197.001			170.701			165.812		
Omnibus-Tests	9.255*			35.554***			40.443***		

*Note: N = 176; * p < 0.05; ** p < 0.01; *** p < 0.001; StE= Standard Error, Coeff = Coefficient;*
† low=0, high=1; †† absent=0, present=1

Table 19: Main Effect Analysis – Binary Logistic Regression on User Disclosure Propensity.

Supporting H1 and H2, the binary logistical regression in Stage 2 demonstrated a statistically significant main effect for MI (b = 1.830; Wald statistic (1) = 18.867; p < 0.001) and PSD (b = 1.208; Wald statistic (1) = 8.707; p < 0.01). More precisely, users in the high MI have 6.24 times higher odds to self-disclose compared to the low MI, while users in the PSD present condition have 3.35 times higher odds compared to the absent PSD conditions. Furthermore, the results of Stage 3 demonstrated a statistically significant positive interaction effect of MI and PSD on user disclosure propensity (b = 1.766; Wald statistic (1) = 4.889; p < 0.05), giving a first indication in support of our H3.

5.5.3 Interaction Effect Analysis for MI and PSD

We suggest in H3, that MI will moderate the effect of PSD on user disclosure propensity. Our binary logistic regression has already indicated this moderation effect. Thus, we conducted a bootstrap moderation analysis with 10,000 samples and a 95% bias-corrected confidence interval to test whether MI moderates the effect of PSD (Andrew F Hayes, 2017, model 1). The results of our moderation analysis show that the effect of PSD on user disclosure propensity is

moderated by MI such that the effect is enhanced when MI is high (effect = 2.579, standard error = 0.559) compared to when MI is low (effect = 0.813, standard error = 0.593). Furthermore, the analysis unveiled that the effect of PSD is only statistically significant in presence of high MI (95% bias-corrected confidence interval (CI) = [1.483, 3.675]) but not when low (95% bias-corrected confidence interval (CI) = [-0.349, 1.976]). To compare the interaction effect with the individual factors, we conducted a simple slope analysis (see Figure 19). The effect of PSD on user disclosure propensity in the high MI condition is higher (24.54%) than the effect of low MI on user disclosure propensity when MI is low (15.91%). On the other hand, the isolated effects are each outperformed when both manipulations are employed together (71.39%).

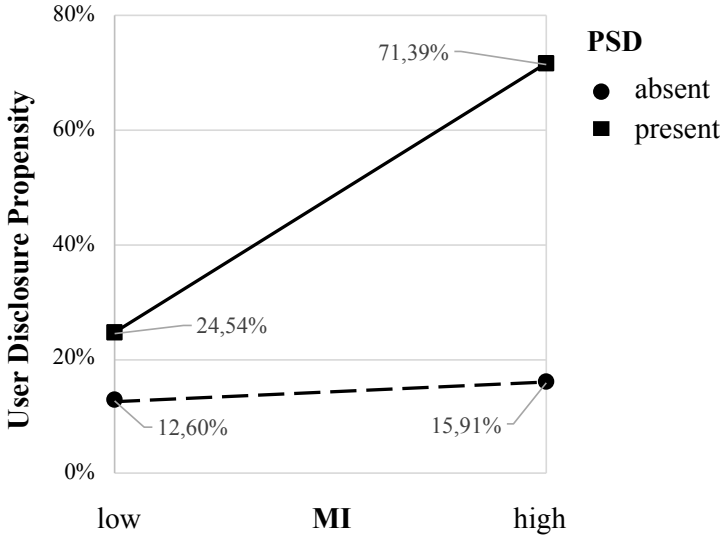


Figure 19: Simple slope moderation analysis.

5.6 Discussion and Implications

E-commerce has been experiencing dramatic growth over the past decade and online competition has becoming fiercer for online platforms. As a result, potential users are overwhelmed with offers and information of various providers, leading to small conversion rates and increased churn rates. Consequently, providers have to come up with better onboarding strategies to convert mere visitors to revenue-generating users. CAs, such as chatbots, have been becoming popular in various customer service settings and are considered potential strategic tools to facilitate the user onboarding process.

Our empirical investigation examined how platforms can employ a chatbot with different social cues in their user onboarding strategy to positively influence user disclosure propensity. Specifically, we analyzed how the nonverbal cue MI and the verbal cue PSD used in an instant

messenger interface on a real online platform affects user information disclosure in form of newsletter sign-ups. Our results demonstrated that both independent variables had a distinct and significant impact, in that users in the high MI were more likely to self-disclose their e-mail in contrast to the low MI, while users in the PSD present condition (in contrast to the PSD absent condition) were more likely to self-disclose as well. However, our results showed a statistically significant positive interaction effect of MI and PSD on user disclosure propensity, in that the effects could be observed only when both cues were present.

This research contributes to IS in three important ways. First, following the call for a more actionable research on the design of CAs (e.g., Gnewuch et al., 2017; Seeger et al., 2018), our piece of research extends prior research by addressing disembodied CAs like chatbots, which have been neglected in past studies. More specifically, we investigated the effects of one nonverbal (i.e., message interactivity) and one verbal cue (i.e., self-disclosure), which are understudied yet widely applied in practice. Most importantly, our findings speak to the psychological importance of message interactivity: We analyzed the effect of visualized turn-taking, which before has been unreflectively and abundantly applied in chatbots both in research and practice, neglecting an examination of the fundamental nonverbal cue for the "conversation ideal" (Sundar et al., 2016) on its own. Moreover, we depart from prior research on computer self-disclosure that profoundly investigated website self-disclosure (e.g., Zimmer et al., 2010) and particularly CA self-disclosure (e.g., S. Lee & Choi, 2017) by having a more practice-oriented approach: Whereas past studies on CAs primarily investigated self-disclosure as a piece of information that is directly related to the social actor (e.g., providing information about the CA's own identity or feelings) (e.g., Moon, 2000; Saffarizadeh et al., 2017), we investigate platform self-disclosure in that the chatbot reveals primarily information about the platform and the platform's (human) customer service (Zimmer et al., 2010) and not directly about itself.

Second, our study addressed an interplay between the analyzed cues, which seems especially worthwhile due to recent surprising findings on the combination of different cues (e.g., Seeger et al., 2018). This interplay of our cues has not been investigated in disembodied CAs before, though a combination seemed particularly intriguing as both cues are fundamental in human-human interactions where information is exchanged turn by turn and one after another. Based on our reasoning, it seems that the nonverbal cue of message interactivity is so essential that other cues, such as self-disclosure, can develop their effect only or at least better when a user perceives a certain degree of message interactivity. Thus, our results indicate, also in a broader context, that studies on information disclosure need to consider the degree of (message)

interactivity to correctly interpret the resulting disclosure effects (e.g., Chu & Kim, 2017; Weisband & Kiesler, 1996).

Third and lastly, we provide findings on actual user onboarding behavior. Precisely, our sample consisted of real visitors who intentionally and self-motivated entered a website and who voluntarily and out of self-interest provided their e-mail to become registered users. This procedure is unprecedented in contrast to previous studies that were limited to laboratory experiments and user intentions. Moreover, instead of creating a complex personality for the CA (e.g., Holzwarth, Janiszewski, & Neumann, 2006), which has been shown to even create negative reactions in some settings (e.g., Mimoun, Poncin, & Garnier, 2012), we kept the chatbot simple, generalizable, and easily implementable for service-oriented purposes of practitioners. Consequently, we deliver actionable recommendations as well, in that these findings help providers in their decision-making to use and design highly interactive formats like chatbots if they desire better user onboarding outcomes in contrast, for instance, to plentifully employed, but lowly interactive forms.

5.7 Limitations and Directions for Future Research

The conducted study should be treated as an initial empirical investigation into the realm of disembodied CAs and onboarding strategies and, thus, needs to be understood with respect to some noteworthy limitations which at the same time represent opportunities for future research.

First, although we carefully designed our experiment, we could not fully control the website of the platform and check user characteristics. Potential confounding effects might have influenced our results, although a pretest ascertained internal validity for our manipulations. Future studies may try to replicate our field study on a platform with more control over potential confounds and even in an experiment to identify and measure potential effects of moderators, mediators, and other control variables quantitatively (e.g., user characteristics and cultural contexts).

Second, in our study we investigated one specific design of message interactivity and self-disclosure on one particularly designed interface in one product category of one platform with respect to one onboarding outcome. Thus, we encourage future studies to test other forms of these cues and evaluate their effects in the same and other product categories and dependent variables, especially with regard to revealed interaction effect of our analyzed manipulations. It would be interesting to see in future HCI studies, how these cues will perform in product categories with higher involvement (e.g., car and camera purchases) (Praveen Aggarwal,

Vaidyanathan, & Rochford, 2007), in more sensitive privacy disclosure environments (e.g., health care or recruiting) (e.g., Sah & Peng, 2015; Schuetzler et al., 2018), and in combination with other cues (Seeger et al., 2018). The investigation of adjustments and variations in our experimental design, such as number of questions and number of self-disclosures, could also be a worthwhile endeavor. Moreover, other dependent variables, such as purchase behavior and user referral, may also be examined.

Third and lastly, researchers and practitioners should be careful with our results, as the phenomenon of disembodied CAs is quite new in practice. Only recently chatbots have sparked great interest in companies (Knight, 2016; Luger & Sellen, 2016). Users may get familiar with the presented cues and will adjust their behavior over time, once they get accustomed with the new technology.

Chapter 6: Thesis Conclusion and Contributions

Overall, the thesis provides a broad understanding of the role of intrusive and mitigating technology features in privacy choice environments. This thesis is motivated by the need for a better understanding of how technology features in information privacy contexts affect and alleviate privacy-related stressors, specifically by drawing on social nudges. In view of this, four empirical studies were conducted, each contributing actionable design recommendations to mitigating social nudges in privacy choice environments. Sections 6.1 and 6.2 summarize and discuss the main theoretical and practical contributions of these studies. Section 6.3 summarizes our limitations, considers steps towards future research, and concludes this thesis.

6.1 Theoretical Contributions

First, due to articles 1 & 2, we were able to advance the understanding of how intrusive technology features drive privacy-related stressors and thereby affect general and situational strains. More precisely, we provided evidence on how specific technology features invade users' privacy and thus influence their decision-making and psychological strain in privacy choice environments. We found that both information delivery mechanisms and user voice interfaces (unintentional voice activations) stimulate privacy-related stress through different psychological pathways, namely privacy invasions, and privacy concerns. In this regard, the first study links intrusive features of smart home assistants to individual's strain via privacy invasion. Additionally, we extended the P-T model by showing how the detrimental effects of intrusive SHA features can even spill over to social outcomes at home. Thus, the first study contributes to research on intrusive technology features by explaining the broader effects of digital technologies on an individual's psychology and their social environment. The second study expands on those findings by showing that push-based information delivery invades users' privacy through driving privacy concerns and thus affects users' willingness to disclose geolocation information. Thereby, this study shows the psychological pathways through which the above mentioned design features shape behavioral strain, explicating privacy concerns as a driver of privacy-related stress. In doing so, these findings address the call of IS scholars for research on specific and context-related intrusive technology features with actionable design recommendations (Ayyagari et al., 2011; Speier, Vessey, & Valacich, 2003). In sum, by illuminating the psychological processes underlying the effects of these intrusive technology features and revealing how they stimulate privacy invasions, we contribute to IS research on privacy choice environments and more general psychology research related to technology-induced stress.

Second, this study extends the P-T model with a layer of mitigating technology features by integrating the Person-Technology fit model and literature on social nudging, to show how mitigating technology features can help attenuate and even cancel out the effects of intrusive technology features. In the first study, we demonstrated how anthropomorphic social cues can mitigate the impact of privacy invasions and thereby decrease individuals' strain. The underlying rationale is that anthropomorphic cues act as normative social influences such that they seem to compensate for lack of trust, increase perceived control, and thus help users to better deal with privacy invasions. Further, in the second study, we explored how social proof mitigates the induced privacy concerns of push-based information delivery mechanisms. Therefore we demonstrate how social proof can be employed as mitigating technology features and how it can help to reduce behavioral strain during decision-making on geolocation information disclosure. Lastly, the third study demonstrates how platform self-disclosure can overcome the intrusive nature of low message interactivity chat conversations and improve information disclosure. The underlying rationale here is that self-disclosure acts as a mitigator, which creates feelings of imbalance in users that are usually only created in human-to-human interactions, pushing users to reciprocate information disclosure. This research contributes to a more nuanced understanding of the circumstances under which the adverse effects of intrusive technology features are likely to occur, and thus extend the Person-Technology fit model by introducing a novel, IT artifact-based mitigating layer in the technology-stressor-strain causal chain of relationships.

Lastly, following the calls of Kretzer and Maedche (2018) and Mirsch et al. (2017), this study contributes to actionable social nudge designs and refinements by demonstrating and testing their effects in privacy choice environments. Hence, this research illustrates how social nudges can be incorporated in privacy choice environments as mitigating technology features. The first study demonstrates how anthropomorphism works as a normative social influence by providing smart home assistant with traits of a social actor. The second study shows how social proof acts as an informational social cue that drives users to build trusting beliefs and thereby mitigates the effects of privacy concerns. The third study leverages the reciprocal nature of platform self-disclosure to create an imbalance that puts a normative influence on users and hereby increasing their likelihood to disclose information. In sum, this study contributes to research on social nudges more broadly by investigating the context of privacy choice environments with specific and actionable design recommendations.

From a more theoretical perspective, this thesis expands the understanding of social nudges and how these may be used to mitigate the effects of intrusive technology features within privacy choice environments, thus allowing service providers to reduce behavioral and psychological strains.

6.2 Practical Contributions

The preceding insights focus on theoretical contributions to research, this study's findings yield important practical implications:

First, this study helps practitioners to better predict the effects of intrusive technology features in privacy choice environments. The results demonstrate that it is imperative for service providers to understand how intrusive technology features may not only increase user strain through privacy invasion but also impair their usage behavior. The first study provides evidence that voice user interfaces increase individual and interpersonal conflicts by driving privacy invasions. Therefore, we demonstrate how intrusive technology features cause psychological and behavioral strain in home environments such as private households. Thus, practitioners may proactively increase anonymity on the one hand, and lower presenteeism and unintentional voice activation on the other, when designing digital services, to decrease privacy invasion of ubiquitous digital assistants. The second study links push information delivery mechanisms to privacy concerns, causing decreased geographical location information disclosure. Consequently, this demonstrates how pull-based information delivery is a vital leverage point that should be considered by service providers to alleviate privacy concerns. The results show that self-triggered provision of information corresponds to deliberately pulling information on demand, which reduces invasion of users' privacy. Thus, service providers can reduce the effect of intrusive technology features by putting users in control. In this regard, the third study expands these findings by showing how low message interactivity corresponds to a more invasive human-computer relationship. The findings support that users are more likely to disclose personally identifiable information when the conversational ideal (Sundar et al., 2016) is recreated by high message interactivity. Hence, practitioners can act precautious by shaping information acquisition in a less invasive form.

Second, the study provides recommendations on the design of social nudges, specifically for enhancing privacy-related outcomes. We contribute to a better understanding of the intricate (and often delicate) interplay between intrusive versus mitigating technology features. Thereby, we put together a selection of actionable social nudges that can be employed by practitioners to

proactively reduce the effect of privacy-related stressors in privacy choice environments. In this regard, the first study elaborates on the effectiveness of normative anthropomorphic design cues and how they may serve as a buffer to attenuate the potentially harmful effects of intrusive technology features. The second study shows how service providers can overcome privacy concerns with informational social proof cues, providing evidence for augmenting effect of social proof nudges on users' trusting beliefs. Lastly, the third study shows how unprompted disclosure of information from service providers can trigger users to behave in compliance with normative social influences and hereby reciprocate with self-disclosure.

6.3 Limitations, Future Research and Conclusion

Two limitations of this thesis are noteworthy and inform future research. First, this thesis is among the first to examine the effect of social nudges in privacy choice environments. Therefore, our findings should be treated with caution when concluding more generally. Consequently, future research may examine the generalizability of the thesis's findings for other IS contexts. Second, this thesis incorporates a mix of laboratory and field experiments that respectively exert external or internal validity, yet our research still may suffer from methodological limitations. For example, controlled laboratory experiments checked user behavior at a single point of time under supervised conditions, thus exerting high internal validity but neglecting external validity. Future research may complement and support these initial findings by conducting longitudinal field studies.

Despite these limitations, our study provides several avenues for future research. First, the scope of this thesis was chosen to examine specific intrusive technology features from different information services and their interplay with social nudges while neglecting other privacy-related stressors, such as negative affect or demographic and cultural differences. Therefore, future research might further investigate how social nudges might attenuate privacy-related stress. Second, this thesis focused on privacy-related stressors and intrusive technology features. This research can be regarded as an impetus for future research into how social nudges can be leveraged to enhance decision making within other contexts.

In conclusion, information privacy choice environments are an integral part of today's digital service landscapes. Although their characteristics have been widely studied from a rational and thoughtful decision making perspective, their nature and consequences from a non-rational and fast thinking perspective have remained underexplored so far. Although this thesis is only a first step to extend the understanding from this perspective, we were able to demonstrate in four

empirical experiments that the effects of intrusive technology features on user strain and usage decision-making are salient and thus cannot be neglected. Through the interplay with mitigating technology features, service providers are presented with possibilities to attenuate these stress-related privacy outcomes. As a result, we can empower companies with the knowledge of how to shape privacy choice environments. Following this notion, we hope that this substantial shift in perspective and relatively unexpected results will foster further research by other IS scholars in this direction.

References

Adam, M., & Klumpe, J. (2019). *Onboarding with a Chat–The Effects of Message Interactivity and Platform Self-Disclosure on User Disclosure Propensity*. Retrieved from

Adam, M., Wessel, M., & Benlian, A. (2019). Of early birds and phantoms: how sold-out discounts impact entrepreneurial success in reward-based crowdfunding. *Review of Managerial Science, 13*(3), 545-560.

Adjerid, I., Acquisti, A., & Loewenstein, G. (2018). Choice architecture, framing, and cascaded privacy choices. *Management science, 65*(5), 2267-2290.

Aggarwal, P., & McGill, A. L. (2007). Is that car smiling at me? Schema congruity as a basis for evaluating anthropomorphized products. *Journal of Consumer Research, 34*(4), 468-479.

Aggarwal, P., & McGill, A. L. (2012). When brands seem human, do humans act like brands? Automatic behavioral priming effects of brand anthropomorphism. *Journal of Consumer Research, 39*(2), 307-323.

Aggarwal, P., Vaidyanathan, R., & Rochford, L. (2007). The wretched refuse of a teeming shore? A critical examination of the quality of undergraduate marketing students. *Journal of Marketing Education, 29*(3), 223-233.

Aguinis, H., & Bradley, K. J. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods, 17*(4), 351-371. doi:10.1177/1094428114547952

Aiken, L. S., & West, S. G. (1991). *Multiple Regression: Testing and Interpreting Interactions*. Newbury Park, CA: Sage Publications.

Al-Natour, S., Benbasat, I., & Cenfetelli, R. T. (2006). The Role of Design Characteristics in Shaping Perceptions of Similarity: The Case of Online Shopping Assistants. *Journal of the Association for Information Systems, 7*(12), 821-861. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=24979090&site=ehost-live

Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology, 86*(4), 797.

Allen, D. K., & Shoard, M. (2005). Spreading the load: Mobile information and communications technologies and their effect on information overload. *Information Research: An International Electronic Journal, 10*(2), n2.

Amblee, N., & Bui, T. (2011). Harnessing the influence of social proof in online shopping: The effect of electronic word of mouth on sales of digital microproducts. *International journal of electronic commerce, 16*(2), 91-114.

Amstad, F. T., Meier, L. L., Fasel, U., Elfering, A., & Semmer, N. K. (2011). A meta-analysis of work-family conflict and various outcomes with a special emphasis on cross-domain versus matching-domain relations. *Journal of Occupational Health Psychology, 16*(2), 151-169. doi:10.1037/a0022170

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339-370.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS quarterly, 33*(2), 339-370. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=38224406&site=ehost-live

Araujo, T. (2018). Living up to the chatbot hype: The influence of anthropomorphic design cues and communicative agency framing on conversational agent and company perceptions. *Computers in Human Behavior, 85*, 183-189.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research, 14*(3), 396-402.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of marketing research*, 396-402.

Awad, N. F., & 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*, 13-28.

Awad, N. F., & 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), 13-28. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=19754858&loginpage=Login.asp&site=ehost-live

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly, 35*(4), 831-858. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=67123598&site=ehost-live

Bailar, B., Bailey, L., & Stevens, J. (1977). Measures of interviewer bias and variance. *Journal of Marketing Research*, 337-343.

Bakker, A. B., & Demerouti, E. (2013). The spillover-crossover model. In *New frontiers in work and family research.* (pp. 55-70). New York, NY, US: Psychology Press.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems, 49*, 138-150.

Bansal, G., & Zahedi, F. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *ICIS 2008 Proceedings*, 7.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.

Barak, A., & Gluck-Ofri, O. (2007). Degree and reciprocity of self-disclosure in online forums. *CyberPsychology & Behavior, 10*(3), 407-417.

Barber, L. K., Taylor, S. G., Burton, J. P., & Bailey, S. F. (2017). A Self-Regulatory Perspective of Work-to-Home Undermining Spillover/Crossover: Examining the Roles of Sleep and Exercise. *Journal of Applied Psychology, 102*(5), 753-763. doi:10.1037/apl0000196

Barker, T. (2016). Why privacy is the killer app. *TechCrunch*.

Barkhuus, L. (2004). *Privacy in location-based services, concern vs. coolness*. Paper presented at the Workshop on Location System Privacy and Control at MobileHCI.

Barkhuus, L., & Dey, A. K. (2003). *Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns.* Paper presented at the Interact 2003.

Baroudi, J. J., & Orlikowski, W. J. (1989). The problem of statistical power in MIS research. *MIS quarterly*, 87-106.

Bartneck, C., Kulić, D., Croft, E., & Zoghbi, S. (2009). Measurement Instruments for the Anthropomorphism, Animacy, Likeability, Perceived Intelligence, and Perceived Safety of Robots. *International Journal of Social Robotics, 1*(1), 71-81. doi:10.1007/s12369-008-0001-3

Bauer, T. N., & Erdogan, B. (2011). Organizational socialization: The effective onboarding of new employees. *APA Handbook of Industrial and Organizational Psychology, 3*, 51-64.

Baumeister, R. F., Vohs, K. D., & Tice, D. M. (2007). The Strength Model of Self-Control. *Current Directions in Psychological Science, 16*(6), 351-355. doi:10.1111/j.1467-8721.2007.00534.x

Bearden, W. O., & Rose, R. L. (1990). Attention to social comparison information: An individual difference factor affecting consumer conformity. *Journal of Consumer Research, 16*(4), 461-471.

Becker, B., & Mark, G. (1999). Constructing social systems through computer-mediated communication. *Virtual Reality, 4*(1), 60-73.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-A1036. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=67123613&site=ehost-live

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly, 35*, 1017-1042.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*, 245-270. doi:10.1016/S0963-8687(02)00018-5

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2016). An empirical test of an Antecedents–Privacy Concerns–Outcomes model. *Journal of Information Science*, 0165551516653590.

Benlian, A. (2015). IT feature use over time and its impact on individual task performance. *Journal of the Association for Information Systems, 16*(3), 144-173.

Benlian, A. (2015). Web personalization cues and their differential effects on user assessments of website value. *Journal of Management Information Systems, 32*(1), 225-260.

Benlian, A. (2020). A daily field investigation of technology-driven stress spillovers from work to home. *MIS Quarterly, forthcoming*.

Benlian, A., & Hess, T. (2011). The Signaling Role of IT Features in Influencing Trust and Participation in Online Communities. *International Journal of Electronic Commerce, 15*(4), 7-56. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=61988870&site=ehost-live

Benlian, A., Klumpe, J., & Hinz, O. (2019). *Mitigating the Intrusive Effects of Smart Home Assistants by using Anthropomorphic Design Features: A Multi-Method Investigation*. Retrieved from

Best, S. J., Krueger, B. S., & Ladewig, J. (2006). Privacy in the information age. *International Journal of Public Opinion Quarterly, 70*(3), 375-401.

Blau, P. (2017). *Exchange and power in social life*: Routledge.

Brevers, D., Foucart, J., Turel, O., Bertrand, A., Alaerts, M., Verbanck, P., . . . Bechara, A. (2018). The impact of self-control cues on subsequent monetary risk-taking. *J Behav Addict*, forthcoming. doi:10.1556/2006.7.2018.97

Brislin, R. W. (1990). *Applied Cross-Cultural Psychology*. Thousand Oaks, California: SAGE Publications, Inc.

Brod, C. (1984). *Technostress: The human cost of the computer revolution*: Addison Wesley Publishing Company.

Bruner, G. C., & Kumar, A. (2007). Attitude toward location-based advertising. *Journal of Interactive advertising, 7*(2), 3-15.

Bucy, E. P., & Tao, C.-C. (2007). The mediated moderation model of interactivity. *Media Psychology, 9*(3), 647-672.

Buhr, S. (2016). An Amazon Echo may be the key to solving a murder case. Retrieved from https://techcrunch.com/2016/12/27/an-amazon-echo-may-be-the-key-to-solving-a-murder-case/

Burger, J. M. (1999). The foot-in-the-door compliance procedure: A multiple-process analysis and review. *Personality and Social Psychology Review, 3*(4), 303-325.

Burgoon, J. K., Bonito, J. A., Bengtsson, B., Cederberg, C., Lundeberg, M., & Allspach, L. (2000). Interactivity in human–computer interaction: a study of credibility, understanding, and influence. *Computers in human behavior, 16*(6), 553-574. doi:https://doi.org/10.1016/S0747-5632(00)00029-7

Burleigh, T., Schoenherr, J., & L. Lacroix, G. (2013). Does the uncanny valley exist? An empirical test of the relationship between eeriness and the human likeness of digitally created faces. *Computers in Human Behavior, 29*(3), 759-771. doi:10.1016/j.chb.2012.11.021

Byron, K. (2005). A meta-analytic review of work–family conflict and its antecedents. *Journal of Vocational Behavior, 67*(2), 169-198. doi:https://doi.org/10.1016/j.jvb.2004.08.009

Cardoso, M. C. (2017). *The onboarding effect: Leveraging user engagement and retention in crowdsourcing platforms.* Paper presented at the Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems.

Chae, S. W., Lee, K. C., & Seo, Y. W. (2016). Exploring the Effect of Avatar Trust on Learners' Perceived Participation Intentions in an e-Learning Environment. *International Journal of Human-Computer Interaction, 32*(5), 373-393. doi:10.1080/10447318.2016.1150643

Chartrand, T. L., & Bargh, J. A. (1999). The chameleon effect: the perception–behavior link and social interaction. *Journal of Personality and Social Psychology, 76*(6), 893.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2-3), 181-202.

Chen, A., & Karahanna, E. (2018). Life Interrupted: The Effects of Technology-Mediated Work Interruptions on Work and Nonwork Outcomes. *MIS quarterly, 42*(4), 1023-1042. doi:10.25300/MISQ/2018/13631

Chen, K., & Rea, A. I. J. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems, 44*(4), 85-92.

Cheverst, K., & Smith, G. (2001). *Exploring the notion of information push and pull with respect to the user intention and disruption.* Paper presented at the International workshop on Distributed and Disappearing User Interfaces in Ubiquitous Computing.

Chu, S.-C., & Kim, Y. (2017). The influence of perceived interactivity of social media advertising and voluntary self-disclosure on attitudes and intentions to pass along. In *Advertising and Branding: Concepts, Methodologies, Tools, and Applications* (pp. 1388-1405): IGI Global.

Cialdini, R. B. (2001). Harnessing the science of persuasion. *Harvard Business Review, 79*(9), 72-81.

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*: Collins New York.

Cialdini, R. B., & Garde, N. (1987). *Influence* (Vol. 3): A. Michel.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol., 55*, 591-621.

Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In D. T. Gilbert, S. T. Fiske, & L. G. (Eds.), *The Handbook of Social Psychology* (pp. 151-192). New York: McGraw-Hill.

Ciechanowski, L., Przegalinska, A., Magnuski, M., & Gloor, P. (2019). In the shades of the uncanny valley: An experimental study of human–chatbot interaction. *Future Generation Computer Systems, 92*(March), 539-548. doi:https://doi.org/10.1016/j.future.2018.01.055

Cohen, J. (1992). A power primer. *Psychological bulletin, 112*(1), 155.

Cohen, P., West, S. G., & Aiken, L. S. (2014). *Applied multiple regression/correlation analysis for the behavioral sciences*: Psychology Press.

Cole, R., Van Vuuren, S., Pellom, B., Hacioglu, K., Ma, J., Movellan, J., . . . Yan, J. (2003). Perceptive animated interfaces: First steps toward a new paradigm for human-computer interaction. *Proceedings of the IEEE, 91*(9), 1391-1405.

Collins, N. L., & Miller, L. C. (1994). Self-disclosure and liking: a meta-analytic review. *Psychological Bulletin, 116*(3), 457.

Cooper, C. L., Dewe, P. J., & O'Driscoll, M. P. (2001). *Organizational stress: A review and critique of theory, research, and applications*: Sage.

Crist, R., & Gebhart, A. (2018). Everything you need to know about the Amazon Echo. Retrieved from https://www.cnet.com/how-to/amazon-echo-alexa-everything-you-need-to-know/

Cropanzano, R., & Mitchell, M. S. (2005). Social exchange theory: An interdisciplinary review. *Journal of Management, 31*(6), 874-900.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*, 104-115. doi:10.1287/orsc.10.1.104

D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the" Dark Side" of Information Technology Use. *CAIS, 35*, 5.

D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the "Dark Side" of Information Technology Use. *Communications of the AIS, 35 (Article 5)*, 109-118.

Dalton, R. (2004). Lion Man Oldest Statue. *Nature News Service / Macmillan Magazines*.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Davis, G. B. (2002). Anytime/anyplace computing and the future of knowledge work. *Communications of the ACM, 45*(12), 67-73.

de Ridder, D. T. D., Lensvelt-Mulders, G., Finkenauer, C., Stok, F. M., & Baumeister, R. F. (2012). Taking Stock of Self-Control: A Meta-Analysis of How Trait Self-Control Relates to a Wide Range of Behaviors. *Personality and Social Psychology Review, 16*(1), 76-99. doi:10.1177/1088868311418749

Deng, H., Coyle-Shapiro, J., & Yang, Q. (2018). Beyond Reciprocity: A Conservation of Resources View on the Effects of Psychological Contract Violation on Third Parties. *Journal of Applied Psychology, 103*(5), 561-577. doi:10.1037/apl0000272

Deng, H., Wu, C.-H., Leung, K., & Guan, Y. (2016). Depletion from Self-Regulation: A Resource-based Account of the Effect of Value Incongruence. *Personnel Psychology, 69*, 431–465.

DeTienne, K. B. (1993). Big brother or friendly coach? Computer monitoring in the 21st century. *The Futurist, 27*(5), 33.

DeWall, C. N., Baumeister, R. F., Stillman, T. F., & Gailliot, M. T. (2007). Violence restrained: Effects of self-regulation and its depletion on aggression. *Journal of Experimental Social Psychology, 43*(1), 62-76. doi:https://doi.org/10.1016/j.jesp.2005.12.005

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Dinev, T., & Hart, P. (2006b). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*, 61-80. doi:10.1287/isre.1060.0080

Dinev, T., McConnell, A. R., & 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), 639-655.

Dinev, T., McConnell, A. R., & Smith, H. J. (2016). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research, 26*(4), 639–655. doi:doi:10.1287/isre.2015.0600

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), 295–316.

Duan, W., Gu, B., & Whinston, A. B. (2009). Informational cascades and software adoption on the internet: an empirical investigation. *MIS quarterly*, 23-48.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Eddy, E. R., Stone, D. L., & Stone-Romero, E. E. (1999). The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel psychology, 52*(2), 335-358.

Edwards, J. R. (1991). *Person-job fit: A conceptual integration, literature review, and methodological critique*: John Wiley & Sons.

Edwards, J. R. (1996). An examination of competing versions of the person-environment fit approach to stress. *Academy of Management Journal, 39*(2), 292-339. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9605140865&site=ehost-live

Edwards, J. R., Cable, D. M., Williamson, I. O., Lambert, L. S., & Shipp, A. J. (2006). The phenomenology of fit: linking the person and environment to the subjective experience of person-environment fit. *Journal of Applied Psychology, 91*(4), 802.

Edwards, J. R., & Cooper, C. L. (1988a). Research in stress, coping, and health: Theoretical and methodological issues. *Psychological medicine, 18*(1), 15-20.

Edwards, J. R., & Cooper, C. L. (1988b). Research in stress, coping, and health: theoretical and methodological issues1. *Psychological medicine, 18*(1), 15-20.

Edwards, J. R., & Lambert, L. S. (2007). Methods for Integrating Moderation and Mediation: A General Analytical Framework Using Moderated Path Analysis. *Psychological Methods, 12*(1), 1-22.

Elahi, S. (2009). Privacy and consent in the digital era. *Information Security Technical Report, 14*, 113-118. doi:10.1016/j.istr.2009.10.004

eMarketer. (2016). Are Mobile Users Returning to Apps After Trying Them Out? Retrieved from https://www.emarketer.com/Article/Mobile-Users-Returning-Apps-After-Trying-Them-Out/1014039

Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology, 2*(1), 335-362.

Ennis, L. A. (2005). The evolution of technostress. *Computers in libraries, 25*(8), 10-12.

Epley, N., Waytz, A., & Cacioppo, J. T. (2007). On seeing human: a three-factor theory of anthropomorphism. *Psychological review, 114*(4), 864.

Etherington, D. (2019). Apple is now the privacy-as-a-service company. Retrieved from https://techcrunch.com/2019/06/03/apple-is-now-the-privacy-as-a-service-company/

Evans, J. S. B. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annu. Rev. Psychol., 59*, 255-278.

Eyssel, F., Hegel, F., Horstmann, G., & Wagner, C. (2010). *Anthropomorphic inferences from emotional nonverbal cues: A case study.* Paper presented at the RO-MAN, 2010 IEEE.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior research methods, 41*(4), 1149-1160.

Feeney, J. A. (2002). Attachment, marital interaction, and relationship satisfaction: A diary study. *Personal Relationships, 9*(1), 39-55. doi:doi:10.1111/1475-6811.00003

Finkel, E. J., DeWall, C. N., Slotter, E. B., Oaten, M., & Foshee, V. A. (2009). Self-regulatory failure and intimate partner violence perpetration. *Journal of Personality and Social Psychology, 97*(3), 483-499. doi:10.1037/a0015433

Fisher, C. D., & To, M. L. (2012). Using experience sampling methodology in organizational behavior. *Journal of Organizational behavior, 33*(7), 865-877. doi:10.1002/job.1803

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research, 20*(2), 303-315.

Fleischmann, M., Amirpur, M., Benlian, A., & Hess, T. (2014). Cognitive biases in information systems research: a scientometric analysis.

Fleischmann, M., Amirpur, M., Grupp, T., Benlian, A., & Hess, T. (2016). The role of software updates in information systems continuance—An experimental study from a user perspective. *Decision Support Systems, 83*, 83-96.

Fogg, B. J., & Nass, C. (1997). Silicon sycophants: The effects of computers that flatter. *International Journal of Human-Computer Studies, 46*(5), 551-561.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, 382-388.

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of public policy & marketing*, 106-119.

Freedman, J. L., & Fraser, S. C. (1966). Compliance without pressure: the foot-in-the-door technique. *Journal of personality and social psychology, 4*(2), 195.

Frey, B. S. (1993). Does monitoring increase work effort? The rivalry with trust and loyalty. *Economic Inquiry, 31*(4), 663-670.

Frone, M. R., Yardley, J. K., & Markel, K. S. (1997). Developing and Testing an Integrative Model of the Work–Family Interface. *Journal of Vocational Behavior, 50*(2), 145-167. doi:https://doi.org/10.1006/jvbe.1996.1577

Gallo, A. (2014). The value of keeping the right customers. *Harvard Business Review*.

Galluch, P. S., Grover, V., & Thatcher, J. B. (2015). Interrupting the workplace: Examining stressors in an information technology context. *Journal of the Association for Information Systems, 16*(1), 1.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9284295&loginpage=Login.asp&site=ehost-live

Gefen, D., & Straub, D. (2003). Managing user trust in B2C e-services. *e-Service, 2*(2), 7-24.

Ghosh, A. K., & Swaminatha, T. M. (2001). Software security and privacy risks in mobile e-commerce. *Communications of the ACM, 44*(2), 51-57.

Gilovich, T., Griffin, D., & Kahneman, D. (2002). *Heuristics and biases: The psychology of intuitive judgment*: Cambridge university press.

Gneezy, A. (2017). Field Experimentation in Marketing Research. *Journal of marketing research, 54*(1), 140-143. doi:10.1509/jmr.16.0225

Gnewuch, U., Morana, S., & Maedche, A. (2017). *Towards designing cooperative and social conversational agents for customer service.* Paper presented at the Proceedings of the Thirty Eighth International Conference on Information Systems (ICIS).

Goldbach, T., Benlian, A., & Buxmann, P. (2018). Differential effects of formal and self-control in mobile platform ecosystems: Multi-method findings on third-party developers' continuance intentions and application quality. *Information & management, 55*(3), 271-284. doi:https://doi.org/10.1016/j.im.2017.07.003

Goldbach, T., Kemper, V., & Benlian, A. (2014). Mobile Application Quality and Platform Stickiness under Formal Vs. Self-Control—Evidence from an Experimental Study. *International Conference on Information Systems*.

Gouldner, A. W. (1960). The norm of reciprocity: A preliminary statement. *American Sociological Review*, 161-178.

Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies, 58*(6), 783-812.

Greenhaus, J. H., & Beutell, N. J. (1985). Sources of Conflict Between Work and Family Roles. *Academy of Management Review, 10*(1), 76-88. doi:10.5465/AMR.1985.4277352

Grennan, T. (2016). App User Retention: Less Than 25% Of New App Users Return The Day After First Use (Here's What To Do About It). Retrieved from https://www.braze.com/blog/app-customer-retention-spring-2016-report/.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19-28.

Guadagno, R. E., & Cialdini, R. B. (2005). Online persuasion and compliance: Social influence on the Internet and beyond. *The social net: The social psychology of the Internet*, 91-113.

Guillory, J. E., & Sundar, S. S. (2014). How does web site interactivity affect our perceptions of an organization? *Journal of Public Relations Research, 26*(1), 44-61.

Guthrie, J., Mancino, L., & Lin, C. T. J. (2015). Nudging consumers toward better food choices: policy approaches to changing food consumption behaviors. *Psychology & Marketing*. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/mar.20795/full

Hair, J. F., Black, W. C., Anderson, R. E., & Babin, B. J. (2018). *Multivariate Data Analysis*. Boston, MA: Cengage Learning EMEA.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-Sem)*. Thousand Oaks, CA: SAGE Publications.

Halbesleben, J. R. (2006). Sources of social support and burnout: a meta-analytic test of the conservation of resources model. *Journal of Applied Psychology, 91*(5), 1134-1145. doi:10.1037/0021-9010.91.5.1134

Hammer, L. B., Bauer, T. N., & Grandey, A. A. (2003). Work-family conflict and work-related withdrawal behaviors. *Journal of Business and Psychology, 17*(3), 419-436.

Hatmake, T. (2017). A messed up Google Home Mini recorded a tech reporter 24/7. Retrieved from https://techcrunch.com/2017/10/10/google-home-mini-recorded-24-7-androidpolice/

Häubl, G., & Trifts, V. (2000). Consumer decision making in online shopping environments: The effects of interactive decision aids. *Marketing Science, 19*(1), 4-21.

Hauk, J., & Padberg, J. (2016). The Customer in the Center of Digital Transformation. *Detecon Management Report 1/2016*.

Hawk, S. T., Keijsers, L., Hale III, W. W., & Meeus, W. (2009). Mind your own business! Longitudinal relations between perceived privacy invasion and adolescent-parent conflict. *Journal of Family Psychology, 23*(4), 511.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*: Guilford Press.

Hayes, A. F. (2017). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach* (2 ed.): Guilford Publications.

Hayes, A. F. (2018). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-based Approach* (Vol. 2nd Edition). New York, NY: Guilford Press.

Hess, T. J., Fuller, M., & Campbell, D. E. (2009). Designing interfaces with social presence: Using vividness and extraversion to create social recommendation agents. *Journal of the Association for Information Systems, 10*(12), 1.

Higgins, E. T. (1998). Promotion and Prevention: Regulatory Focus as A Motivational Principle. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 30, pp. 1-46): Academic Press.

Hinz, O., Spann, M., & Hann, I.-H. (2015). Research Note—Can't Buy Me Love…Or Can I? Social Capital Attainment Through Conspicuous Consumption in Virtual Environments. *Information Systems Research, 26*(4), 859-870. doi:10.1287/isre.2015.0596

Ho, S. Y., Bodoff, D., & Tam, K. Y. (2011). Timing of adaptive web personalization and its effects on online consumer behavior. *Information systems research, 22*(3), 660-679.

Hofmann, D. A., & Gavin, M. B. (1998). Centering Decisions in Hierarchical Linear Models: Implications for Research in Organizations. *Journal of Management, 24*(5), 623-641. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=1618053&site=ehost-live

Hogg, T., & Lerman, K. (2014). Effects of social influence in peer online recommendation. *arXiv preprint arXiv:1410.6744*.

Holzwarth, M., Janiszewski, C., & Neumann, M. M. (2006). The influence of avatars on online consumer shopping behavior. *Journal of Marketing, 70*(4), 19-36.

Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology, 63*(6), 597-606.

Hopkins, B., & Silverman, A. (2016). The Top Emerging Technologies To Watch: 2017 To 2021. Retrieved from https://www.forrester.com/report/The+Top+Emerging+Technologies+To+Watch+2017+To+2021/-/E-RES133144

Inzlicht, M., & Schmeichel, B. J. (2012). What Is Ego Depletion? Toward a Mechanistic Revision of the Resource Model of Self-Control. *Perspectives on Psychological Science, 7*(5), 450-463. doi:10.1177/1745691612454134

Jameson, A., Berendt, B., Gabrielli, S., Cena, F., Gena, C., Vernero, F., & Reinecke, K. (2014). Choice architecture for human-computer interaction. *Foundations and Trends® in Human–Computer Interaction, 7*(1–2), 1-235.

Jan R. Landwehr, Ann L. McGill, & Herrmann, A. (2011). It's Got the Look: The Effect of Friendly and Aggressive "Facial" Expressions on Product Liking and Sales. *Journal of marketing, 75*(3), 132-146. doi:10.1509/jmkg.75.3.132

Jenero, K. A., & Mapesriordan, L. D. (1992). Electronic monitoring of employees and the elusive right to privacy. *Employee Relations Law Journal, 18*(1), 71-102.

Jiang, L. C., Bazarova, N. N., & Hancock, J. T. (2011). The disclosure–intimacy link in computer-mediated communication: An attributional extension of the hyperpersonal model. *Human Communication Research, 37*(1), 58-77.

Jiang, Z., Chan, J., Tan, B. C., & Chua, W. S. (2010). Effects of interactivity on website involvement and purchase intention. *Journal of the Association for Information Systems, 11*(1), 1.

Jick, T. D. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative science quarterly, 24*(4), 602-611. doi:10.2307/2392366

Johnson, E. J., Shu, S. B., Dellaert, B. G., Fox, C., Goldstein, D. G., Häubl, G., . . . Schkade, D. (2012). Beyond nudges: Tools of a choice architecture. *Marketing Letters, 23*(2), 487-504.

Johnson, R. E., Lin, S.-H., & Lee, H. W. (2018). Self-control as the fuel for effective self-regulation at work: Antecedents, consequences, and boundary conditions of employee self-control. In A. J. Elliott (Ed.), *Advances in Motivation Science* (Vol. 5, pp. 87–128). San Diego, CA: Academic Press.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

Junglas, I. A., & Watson, R. T. (2008). Location-based services. *Communications of the ACM, 51*(3), 65-69.

Kagal, L., & Abelson, H. (2010). *Access control is an inadequate framework for privacy protection.* Paper presented at the W3C Privacy Workshop.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *The journal of economic perspectives*. Retrieved from http://www.jstor.org/stable/1942711

Kakabadse, A. K., Kouzmin, A., & Kakabadse, N. K. (2017). Technostress: over identification with information technology and its impact on employees and managerial effectiveness. In *Creating futures: Leading change through information systems* (pp. 279-316): Routledge.

Kardes, F. R., Posavac, S. S., & Cronley, M. L. (2004). Consumer inference: A review of processes, bases, and judgment contexts. *Journal of consumer psychology, 14*(3), 230-256.

Kashian, N., Jang, J.-w., Shin, S. Y., Dai, Y., & Walther, J. B. (2017). Self-disclosure and liking in computer-mediated communication. *Computers in Human Behavior, 71*, 275-283.

Kazai, G., & Milic-Frayling, N. (2008). *Trust, authority and popularity in social information retrieval.* Paper presented at the Proceedings of the 17th ACM conference on Information and knowledge management.

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

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. *Journal of conflict resolution, 2*(1), 51-60.

Kendall, J. E., & Kendall, K. E. (1999). Information delivery systems: an exploration of web pull and push technologies. *Communications of the AIS, 1*(4es), 1.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision support systems, 44*(2), 544-564.

Kim, S., & McGill, A. L. (2011). Gaming with Mr. Slot or gaming the slot machine? Power, anthropomorphism, and risk perception. *Journal of Consumer Research, 38*(1), 94-107.

Kinsella, B. (2018). Rise from $4.4 Billion to $17.4 Billion by 2022. Retrieved from https://www.voicebot.ai/2018/03/29/idc-says-smart-speaker-sales-rise-4-4-billion-17-4-billion-2022/

Kireyev, P., Pauwels, K., & Gupta, S. (2016). Do display ads influence search? Attribution and dynamics in online advertising. *International Journal of Research in Marketing, 33*(3), 475-490.

Klumpe, J., Koch, O. F., & Benlian, A. (2019a). How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets*, 1-18.

Klumpe, J., Koch, O. F., & Benlian, A. (2019b). How pull vs. push information delivery and social proof affect information disclosure in location based services. *Electronic Markets, forthcoming*. doi:10.1007/s12525-018-0318-1

Knight, W. (2016). 10 breakthrough technologies: Conversational interfaces. Retrieved from https://www.technologyreview.com/s/600766/10-breakthrough-technologies-2016-conversational-interfaces

Knijnenburg, B. P., & Willemsen, M. C. (2016). Inferring capabilities of intelligent agents from their external traits. *ACM Transactions on Interactive Intelligent Systems (TiiS), 6*(4), 28.

Koch, O. F., & Benlian, A. (2015). Promotional tactics for online viral marketing campaigns: how scarcity and personalization affect seed stage referrals. *Journal of Interactive Marketing, 32*, 37-52.

Koch, O. F., & Benlian, A. (2017). The effect of free sampling strategies on freemium conversion rates. *Electronic Markets, 27*(1), 67-76. doi:10.1007/s12525-016-0236-z

Koohikamali, M., Gerhart, N., & Mousavizadeh, M. (2015). Location disclosure on LB-SNAs: The role of incentives on sharing behavior. *Decision Support Systems, 71*, 78-87.

Koomen, W., & Dijkstra, W. (1975). Effects of question length on verbal behavior in a bias-reduced interview situation. *European Journal of Social Psychology, 5*(3), 399-403.

Krasnova, H., Widjaja, T., Buxmann, P., Wenninger, H., & Benbasat, I. (2015). Research Note—Why Following Friends Can Hurt You: An Exploratory Investigation of the Effects of Envy on Social Networking Sites among College-Age Users. *Information Systems Research, 26*(3), 585-605. doi:doi:10.1287/isre.2015.0588

Kretzer, M., & Maedche, A. (2018). Designing Social Nudges for Enterprise Recommendation Agents: An Investigation in the Business Intelligence Systems Context. *Journal of the Association for Information Systems, 19*(12), 1145-1186.

Kumar, N., Scheer, L. K., & Steenkamp, J.-B. E. (1995). The effects of perceived interdependence on dealer attitudes. *Journal of marketing research*, 348-356.

Lanier, C. D., Rader, C. S., & Fowler, A. R. (2013). Anthropomorphism, marketing relationships, and consumption worth in the Toy Story trilogy. *Journal of Marketing Management, 29*(1-2), 26-47. doi:10.1080/0267257X.2013.769020

Lau, J., Zimmerman, B., & Schaub, F. (2018). *Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers*. Paper presented at the Proceedings of the ACM on Human-Computer Interaction.

Lee, A. (2011). Social Proof Is The New Marketing. Retrieved from https://techcrunch.com/2011/11/27/social-proof-why-people-like-to-follow-the-crowd/

Lee, S., & Choi, J. (2017). Enhancing user experience with conversational agent for movie recommendation: Effects of self-disclosure and reciprocity. *International Journal of Human-Computer Studies, 103*, 95-105.

Lee, Y.-K., Chang, C.-T., Lin, Y., & Cheng, Z.-H. (2014). The dark side of smartphone usage: Psychological traits, compulsive behavior and technostress. *Computers in human behavior, 31*, 373-383.

Li, H., Edwards, S. M., & Lee, J.-H. (2002). Measuring the Intrusiveness of Advertisements: Scale Development and Validation. *Journal of Advertising, 31*(2), 37-47. doi:10.1080/00913367.2002.10673665

Li, T., Pavlou, P., & Santos, G. d. (2013). What drives users' website registration? A randomized field experiment. *ICIS 2013 Proceedings*.

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems, 57*, 343-354.

Liang, T.-P., Chen, H.-Y., & Turban, E. (2009). *Effect of personalization on the perceived usefulness of online customer services: A dual-core theory.* Paper presented at the Proceedings of the 11th International Conference on Electronic Commerce.

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*, 501. doi:10.1145/2370216.2370290

Lin, R., & Utz, S. (2017). Self-disclosure on SNS: Do disclosure intimacy and narrativity influence interpersonal closeness and social attraction? *Computers in Human Behavior, 70*, 426-436.

Liu, D., Santhanam, R., & Webster, J. (2017). Toward Meaningful Engagement: A Framework for Design and Research of Gamified Information Systems. *MIS Quarterly, 41*(4).

Lowry, P., Moody, G. D., & Chatterjee, S. (2017). Using IT Design to Prevent Cyberbullying. *Journal of Management Information Systems, 34*(3), 863-901. doi:10.1080/07421222.2017.1373012

Lowry, P. B., Moody, G. D., Galletta, D. F., & Vance, A. (2013). The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems, 30*(1), 153-190.

Lu, C.-q., Lu, J.-j., Du, D.-y., & Brough, P. (2016). Crossover effects of work-family conflict among Chinese couples. *Journal of Managerial Psychology, 31*(1), 235-250. doi:10.1108/JMP-09-2012-0283

Lu, J., Yao, J. E., & Yu, C.-S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *The Journal of Strategic Information Systems, 14*(3), 245-268.

Lu, Y., Tan, B., & Hui, K.-L. (2004). *Inducing customers to disclose personal information to internet businesses with social adjustment benefits.* Paper presented at the Twenty-Fifth International Conference on Information Systems (ICIS).

Luchies, L. B., Finkel, E. J., & Fitzsimons, G. M. (2011). The Effects of Self-Regulatory Strength, Content, and Strategies on Close Relationships. *Journal of Personality, 79*(6), 1251-1280. doi:doi:10.1111/j.1467-6494.2010.00701.x

Luger, E., & Sellen, A. (2016). *Like having a really bad PA: the gulf between user expectation and experience of conversational agents.* Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS quarterly, 35*(2), 293-334.

Maedche, A., Legner, C., Benlian, A., Berger, B., Gimpel, H., Hess, T., . . . Söllner, M. (2019). AI-Based Digital Assistants. *Business & Information Systems Engineering, 61*(4), 535-544.

Maier, C., Laumer, S., Eckhardt, A., & Weitzel, T. (2015). Giving too much social support: social overload on social networking sites. *European Journal of Information Systems, 24*(5), 447-464.

Maier, C., Laumer, S., Weinert, C., & Weitzel, T. (2015). The effects of technostress and switching stress on discontinued use of social networking services: a study of Facebook use. *Information Systems Journal, 25*(3), 275-308.

Maier, C., Wirth, J., Laumer, S., & Weitzel, T. (2017). Personality and Technostress: Theorizing the influence of IT mindfulness.

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

Mathur, M. B., & Reichling, D. B. (2016). Navigating a social world with robot partners: A quantitative cartography of the Uncanny Valley. *Cognition, 146*, 22-32. doi:https://doi.org/10.1016/j.cognition.2015.09.008

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

Mazmanian, M. (2013). Avoiding the Trap of Constant Connectivity: When Congruent Frames Allow for Heterogeneous Practices. *Academy of management journal, 56*(5), 1225-1250. doi:10.5465/amj.2010.0787

McCabe, C. J., Kim, D. S., & King, K. M. (2018). Improving Present Practices in the Visual Display of Interactions. *Advances in Methods and Practices in Psychological Science*, 2515245917746792.

McFarlane, D. C., & Latorella, K. A. (2002). The scope and importance of human interruption in human-computer interaction design. *Human-Computer Interaction, 17*(1), 1-61.

McGee, M. K. (1996). Burnout! *InformationWeek*(569), 34-38.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research, 13*(3), 334-359. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=7360955&loginpage=Login.asp&site=ehost-live

McKnight, H. D., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

McNall, L. A., & Roch, S. G. (2007). Effects of Electronic Monitoring Types on Perceptions of Procedural Justice, Interpersonal Justice, and Privacy1. *Journal of Applied Social Psychology, 37*(3), 658-682. doi:doi:10.1111/j.1559-1816.2007.00179.x

Mick, D. G. (1996). Are studies of dark side variables confounded by socially desirable responding? The case of materialism. *Journal of Consumer Research, 23*(2), 106-119.

Mimoun, M. S. B., Poncin, I., & Garnier, M. (2012). Case study—Embodied virtual agents: An analysis on reasons for failure. *Journal of Retailing and Consumer Services, 19*(6), 605-612.

Mingers, J. (2001). Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research, 12*(3), 240-259. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=5647745&loginpage=Login.asp&site=ehost-live

Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital Nudging: Altering User Behavior in Digital Environments.

Moe, W. W., & Fader, P. S. (2004). Dynamic conversion behavior at e-commerce sites. *Management Science, 50*(3), 326-335.

Monteserin, A., & Amandi, A. (2015). Whom should I persuade during a negotiation? An approach based on social influence maximization. *Decision Support Systems, 77*, 1-20.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 26*(4), 323-339.

Moon, Y., & Nass, C. (1996). How "real" are computer personalities? Psychological responses to personality types in human-computer interaction. *Communication Research, 23*(6), 651-674.

Moore, J. E. (2000). One road to turnover: An examination of work exhaustion in technology professionals. *MIS Quarterly, 24*(1), 141-168. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=3205164&site=ehost-live

Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *the Journal of Marketing*, 81-101.

Moos, R. H. (1990). Conceptual and Empirical Approaches to Developing Family-Based Assessment Procedures: Resolving the Case of the Family Environment Scale. *Family process, 29*(2), 199-208. doi:doi:10.1111/j.1545-5300.1990.00199.x

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *the Journal of Marketing*, 20-38.

Mori, M. (1970). The Uncanny Valley. *Energy, 7*(4), 33–35.

Mori, M., MacDorman, K. F., & Kageki, N. (2012). The Uncanny Valley. *IEEE Robotics & Automation Magazine, 19*(2), 98-100. doi:10.1109/MRA.2012.2192811

Morley, K. (2017). Amazon Echo rogue payment warning after TV show causes 'Alexa' to order dolls houses. Retrieved from https://www.telegraph.co.uk/news/2017/01/08/amazon-echo-rogue-payment-warning-tv-show-causes-alexa-order/

Mourey, J. A., Olson, J. G., & Yoon, C. (2017). Products as Pals: Engaging with Anthropomorphic Products Mitigates the Effects of Social Exclusion. *Journal of Consumer Research, 44*(2), 414-431. doi:10.1093/jcr/ucx038

Mulligan, B. (2014). The Right Way To Ask Users For iOS Permissions. Retrieved from https://techcrunch.com/2014/04/04/the-right-way-to-ask-users-for-ios-permissions/

Muraven, M., & Baumeister, R. F. (2000). Self-regulation and depletion of limited resources: Does self-control resemble a muscle? *Psychological Bulletin, 126*(2), 247-259. doi:10.1037/0033-2909.126.2.247

Murphy. (2016). The Secret to Successful Customer Onboarding. Retrieved from http://sixteenventures.com/customeronboarding

Nass, C., Fogg, B. J., & Moon, Y. (1996). Can computers be teammates? *International Journal of Human-Computer Studies, 45*(6), 669-678. doi:https://doi.org/10.1006/ijhc.1996.0073

Nass, C., & Moon, Y. (2000). Machines and mindlessness: Social responses to computers. *Journal of Social Issues, 56*(1), 81-103.

Nass, C., Moon, Y., & Carney, P. (1999). Are people polite to computers? Responses to computer-based interviewing systems. *Journal of Applied Social Psychology, 29*(5), 1093-1109.

Nass, C., Moon, Y., Fogg, B., Reeves, B., & Dryer, D. C. (1995). Can computer personalities be human personalities? *International Journal of Human-Computer Studies, 43*(2), 223-239.

Nass, C., Steuer, J., & Tauber, E. R. (1994). *Computers are social actors.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Neate, R. (2018). Over $119bn wiped off Facebook's market cap after growth shock. Retrieved from https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock

Nielsen Holdings, N. (2013). The Mobile Consumer: A Global Snapshot. *Nueva York, Estados*.

Novak, T. P., Hoffman, D. L., & Duhachek, A. (2003). The influence of goal-directed and experiential activities on online flow experiences. *Journal of Consumer Psychology, 13*(1-2), 3-16.

Nowak, G. J., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Interactive Marketing, 11*(4), 94-108.

Nunamaker, J. F., Derrick, D. C., Elkins, A. C., Burgoon, J. K., & Patton, M. W. (2011). Embodied conversational agent-based kiosk for automated interviewing. *Journal of Management Information Systems, 28*(1), 17-48.

Oracle. (2016). Can Virtual Experiences Replace Reality? Retrieved from https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc35/CXResearchVirtualExperiences.pdf

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information systems research, 12*(2), 121-134.

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., . . . Myllymäki, P. (2012). *Long-term effects of ubiquitous surveillance in the home*. Paper presented at the Proceedings of the 2012 ACM Conference on Ubiquitous Computing, Pittsburgh, Pennsylvania.

Pan, L.-Y., & Chiou, J.-S. (2011). How much can you trust online information? Cues for perceived trustworthiness of consumer-generated online information. *Journal of Interactive Marketing, 25*(2), 67-74.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce, 7*(3), 101-134.

Perez, S. (2018). 39 million Americans now own a smart speaker, report claims. Retrieved from https://techcrunch.com/2018/01/12/39-million-americans-now-own-a-smart-speaker-report-claims/

Pfeuffer, N., Benlian, A., Gimpel, H., & Hinz, O. (2019). Anthropomorphic Information Systems. *Business & Information Systems Engineering, forthcoming*.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2-17.

Pickard, M. D., Burgoon, J. K., & Derrick, D. C. (2014). Toward an Objective Linguistic-Based Measure of Perceived Embodied Conversational Agent Power and Likeability. *International Journal of Human-Computer Interaction, 30*(6), 495-516. doi:10.1080/10447318.2014.888504

Pinsonneault, A., & Heppel, N. (1997). Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *Journal of Management Information Systems, 14*(3), 89-108.

Piszczek, M. M., Pichler, S., Turel, O., & Greenhaus, J. (2016). The Information and Communication Technology User Role: Implications for the Work Role and Inter-Role Spillover. *Frontiers in Psychology, 7*, 2009-2009. doi:10.3389/fpsyg.2016.02009

Podsakoff, P. M., Mackenzie, S. B., Lee, J., & 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), 879-903.

Porter, C. E., & Donthu, N. (2008). Cultivating trust and harvesting value in virtual communities. *Management Science, 54*(1), 113-128.

Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011). When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information System Security, 7*(1), 24–47.

Pseekos, A. C., Bullock-Yowell, E., & Dahlen, E. R. (2011). Examining holland's person—environment fit, workplace aggression, interpersonal conflict, and job satisfaction. *Journal of Employment Counseling, 48*(2), 63-71. doi:doi:10.1002/j.2161-1920.2011.tb00115.x

Qiu, L., & Benbasat, I. (2009a). Evaluating anthropomorphic product recommendation agents: A social relationship perspective to designing information systems. *Journal of Management Information Systems, 25*(4), 145-182.

Qiu, L., & Benbasat, I. (2009b). Evaluating anthropomorphic product recommendation agents: A social relationship perspective to designing information systems. *Journal of Management Information Systems, 25*(4), 145-181. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=38418417&loginpage=Login.asp&site=ehost-live

Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19*(4), 417-433.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Qiang, T. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19*(4), 417-433. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=36002096&site=ehost-live

Reddy, T. (2017). Chatbots for Customer Service Will Help Businesses Save $8 Billion Per Year. Retrieved from https://www.ibm.com/blogs/watson/2017/05/chatbots-customer-service-will-help-businesses-save-8-billion-per-year/

Renz, J., Staubitz, T., Pollack, J., & Meinel, C. (2014). Improving the Onboarding User Experience in MOOCs. *Proceedings EduLearn*.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods, 12*(4), 762-800. doi:10.1177/1094428109332834

Richter, F. (2017). What Are Smart Speakers Used For? Retrieved from https://www.statista.com/chart/9579/smart-speaker-use-cases/

Riedl, R., Mohr, P. N. C., Kenning, P. H., Davis, F. D., & Heekeren, H. R. (2014). Trusting Humans and Avatars: A Brain Imaging Study Based on Evolution Theory. *Journal of Management Information Systems, 30*(4), 83-114. doi:10.2753/MIS0742-1222300404

Rigdon, E. E., Sarstedt, M., & Ringle, C. M. (2017). On Comparing Results from Cb-Sem and Pls-Sem: Five Perspectives and Five Recommendations. *Marketing ZFP, 39*(3), 4-16.

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3. *Boenningstedt: SmartPLS GmbH, http://www.smartpls.com*.

Roberts, J. A., & David, M. E. (2016). My life has become a major distraction from my cell phone: Partner phubbing and relationship satisfaction among romantic partners. *Computers in human behavior, 54*, 134-141. doi:https://doi.org/10.1016/j.chb.2015.07.058

Rodden, T., Friday, A., Muller, H., & Dix, A. (2002). A lightweight approach to managing privacy in location-based services. *Technical Report Equator-02-058, University of Nottingham and Lancaster University and University of Bristol 2002*.

Rodriguez, S. (2018). Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018

. Retrieved from https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html

Roethke, K., Klumpe, J., Adam, M., & Benlian, A. (2020). Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations. *Decision Support Systems, forthcoming*.

Saffarizadeh, K., Boodraj, M., & Alashoor, T. M. (2017). *Conversational Assistants: Investigating Privacy Concerns, Trust, and Self-Disclosure.* Paper presented at the Proceedings of the Thirty Eighth International Conference on Information Systems (ICIS).

Sah, Y. J., & Peng, W. (2015). Effects of visual and linguistic anthropomorphic cues on social perception, self-awareness, and information disclosure in a health website. *Computers in Human Behavior, 45*, 392-401.

Sanz-Vergel, A. I., Rodríguez-Muñoz, A., & Nielsen, K. (2015). The thin line between work and home: The spillover and crossover of daily conflicts. *Journal of Occupational and Organizational Psychology, 88*(1), 1-18. doi:doi:10.1111/joop.12075

Schenk, E., & Guittard, C. (2011). Towards a characterization of crowdsourcing practices. *Journal of Innovation Economics Management*(1), 93-107.

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing, 70*(2), 133-148.

Schneider, C., Weinmann, M., & vom Brocke, J. (2017). Digital Nudging–Influencing Choices by Using Interface Design.

Schneider, D. (2017). Rewarding Prosociality on Non-Commercial Online Sharing Platforms. *Proceedings of the 25th European Conference on Information Systems (ECIS)*, 2269-2284.

Schneider, D., Klumpe, J., Adam, M., & Benlian, A. (2019). *Nudging Users into Electronic Identification Adoption: The Case of E-Government Services*. Retrieved from

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*(3), 2-16.

Schuetzler, R. M., Giboney, J. S., Grimes, G. M., & Nunamaker, J. F. (2018). *The Influence of Conversational Agents on Socially Desirable Responding.* Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences.

Seeger, A.-M., Pfeiffer, J., & Heinzl, A. (2018). *Designing Anthropomorphic Conversational Agents: Development and Empirical Evaluation of a Design Framework*. Paper presented at the Proceedings of the Thirty Ninth International Conference on Information Systems (ICIS).

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston: Houghton-Mifflin.

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13*(4), 24-38.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing, 19*(1), 62-73.

Siemsen, E., Roth, A., & Oliveira, P. (2010). Common Method Bias in Regression Models With Linear, Quadratic, and Interaction Effects. *Organizational Research Methods, 13*(3), 456-476. doi:10.1177/1094428109351241

Skalski, P., & Tamborini, R. (2007). The role of social presence in interactive agent-based persuasion. *Media Psychology, 10*(3), 385-413.

Smith, H. J., Dinev, T., & Xu, H. (2011a). Information privacy research: an interdisciplinary review. *MIS quarterly, 35*, 989-1016.

Smith, H. J., Dinev, T., & Xu, H. (2011b). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Speier, C., Vessey, I., & Valacich, J. S. (2003). The Effects of Interruptions, Task Complexity, and Information Presentation on Computer-Supported Decision-Making Performance. *Decision Sciences, 34*(4), 771-797.

Speier, C., Vessey, I., & Valacich, J. S. (2003). The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance. *Decision sciences, 34*(4), 771-797.

Sprecher, S., Treger, S., Wondra, J. D., Hilaire, N., & Wallpe, K. (2013). Taking turns: Reciprocal self-disclosure promotes liking in initial interactions. *Journal of Experimental Social Psychology, 49*(5), 860-866.

Srivastava, S. C., Chandra, S., & Shirish, A. (2015). Technostress creators and job outcomes: theorising the moderating influence of personality traits. *Information Systems Journal, 25*(4), 355-401.

Stanley, S. M., Markman, H. J., & Whitton, S. W. (2002). Communication, conflict, and commitment: Insights on the foundations of relationship success from a national survey. *Family process, 41*(4), 659-675.

Statista. (2018). Conversion rate of online shoppers in the United States as of 3rd quarter 2017, by device. Retrieved from https://www.statista.com/statistics/234884/us-online-shopper-conversion-rate-by-device/

Straub, D., & Karahanna, E. (1998). Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organization Science, 9*(2), 160-175.

Sundar, S. S. (2012). Social psychology of interactivity in human-website interaction. *Oxford Handbook of Internet Psychology*.

Sundar, S. S., Bellur, S., Oh, J., Jia, H., & Kim, H.-S. (2016). Theoretical importance of contingency in human-computer interaction: effects of message interactivity on user engagement. *Communication Research, 43*(5), 595-625.

Sunstein, C. R. (2014). Nudging: a very short guide. *Journal of Consumer Policy*. Retrieved from http://link.springer.com/article/10.1007/s10603-014-9273-1

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS quarterly, 37*, 1141-1164.

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

Takac, C., Hinz, O., & Spann, M. (2011). The social embeddedness of decision making: opportunities and challenges. *Electronic Markets, 21*(3), 185-195. doi:10.1007/s12525-011-0066-y

Tams, S., Thatcher, J., & Grover, V. (2018). Concentration, Competence, Confidence, and Capture: An Experimental Study of Age, Interruption-based Technostress, and Task Performance. *Journal of the Association for Information Systems, 19*(9), 857-908.

Tarafdar, M., Cooper, C. L., & Stich, J.-F. (2019). The technostress trifecta - techno eustress, techno distress and design: Theoretical directions and an agenda for research. *Information Systems Journal, 29*(1), 6-42. doi:doi:10.1111/isj.12169

Tarafdar, M., Pullins, E. B., & Ragu-Nathan, T. (2015). Technostress: negative effect on performance and possible mitigations. *Information Systems Journal, 25*(2), 103-132.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. (2007). The impact of technostress on role stress and productivity. *Journal of Management Information Systems, 24*(1), 301-328.

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems, 27*(3), 303-334.

Tedesco, J. C. (2007). Examining Internet interactivity effects on young adult political information efficacy. *American Behavioral Scientist, 50*(9), 1183-1194.

Terres, P., Klumpe, J., Jung, D., & Koch, O. (2019). *Digital Nudges for User Onboarding: Turning Visitors into Users*. Retrieved from

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving Decisions About Health, Wealth, and Happiness. In: HeinOnline.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2014). Choice Architecture. *SSRN Electronic Journal*. doi:10.2139/ssrn.2536504

Thies, F., Wessel, M., & Benlian, A. (2016). Effects of Social Interaction Dynamics on Platforms. *Journal of Management Information Systems, 33*(3), 843-873.

Todri, V., & Adamopoulos, P. (2014). Social commerce: An empirical examination of the antecedents and consequences of commerce in social network platforms.

Touré-Tillery, M., & McGill, A. L. (2015). Who or What to Believe: Trust and the Differential Persuasiveness of Human and Anthropomorphized Messengers. *Journal of Marketing, 79*(4), 94-110. Retrieved from

http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=103543708&site=ehost-live

Trinkaus, E. (2005). The Adiposity Paradox in the Middle Danubian Gravettian. *Anthropologie, 43*(2-3), 263-271.

Trougakos, J. P., Beal, D. J., Cheng, B. H., Hideg, I., & Zweig, D. (2015). Too drained to help: a resource depletion perspective on daily interpersonal citizenship behaviors. *Journal of Applied psychology, 100*(1), 227-236. doi:10.1037/a0038082

Truong, Y., & Simmons, G. (2010). Perceived intrusiveness in digital advertising: strategic marketing implications. *Journal of Strategic Marketing, 18*(3), 239-256.

Tu, Q., Wang, K., & Shu, Q. (2005). Computer-related technostress in China. *Communications of the ACM, 48*(4), 77-81.

Turel, O., Cavagnaro, D. R., & Meshi, D. (2018). Short abstinence from online social networking sites reduces perceived stress, especially in excessive users. *Psychiatry Research, 270*, 947-953. doi:https://doi.org/10.1016/j.psychres.2018.11.017

Turel, O., Cheung, C., Matt, C., & Trenz, M. (2018). The Digitization of the Individual (DOTI). *Information Systems Journal, Special Issue Editorial*, forthcoming.

Turel, O., Cheung, C., Matt, C., & Trenz, M. (2019). The Digitization of the Individual (DOTI). *Information Systems Journal, Special Issue Editorial*.

Turel, O., & Gaudioso, F. (2018). Techno-stressors, distress and strain: the roles of leadership and competitive climates. *Cognition, Technology & Work, 20*(2), 309-324. doi:10.1007/s10111-018-0461-7

Unni, R., & Harmon, R. (2007). Perceived effectiveness of push vs. pull mobile location based advertising. *Journal of Interactive advertising, 7*(2), 28-40.

Van Herpen, E., Pieters, R., & Zeelenberg, M. (2009). When demand accelerates demand: Trailing the bandwagon. *Journal of consumer psychology, 19*(3), 302-312.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems, 7*(1).

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS quarterly, 37*(1), 21-54.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS quarterly*, 115-139.

Wang, N., Zhang, B., Liu, B., & Jin, H. (2015). *Investigating Effects of Control and Ads Awareness on Android Users' Privacy Behaviors and Perceptions.* Paper presented at the Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services.

Wang, W., & Benbasat, I. (2007). Recommendation agents for electronic commerce: Effects of explanation facilities on trusting beliefs. *Journal of Management Information Systems, 23*(4), 217-246.

Wang, W., & Benbasat, I. (2016). Empirical assessment of alternative designs for enhancing different types of trusting beliefs in online recommendation agents. *Journal of Management Information Systems, 33*(3), 744-775.

Warkentin, M., Goel, S., & Menard, P. (2017). Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption? *Journal of the Association for Information Systems, 18*(11), 758-786.

Warren, T. (2018). Amazon explains how Alexa recorded a private conversation and sent it to another user. Retrieved from https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation

Watkins Allen, M., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly, 21*(2), 172-200.

Waytz, A., Heafner, J., & Epley, N. (2014). The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle. *Journal of Experimental Social Psychology, 52*, 113-117.

Webster, C. (1996). Hispanic and Anglo interviewer and respondent ethnicity and gender: The impact on survey response quality. *Journal of Marketing Research*, 62-72.

Weil, M. M., & Rosen, L. D. (1997). *Technostress: Coping with technology@ work@ home@ play*: Wiley New York.

Weinert, C., Laumer, S., Maier, C., & Weitzel, T. (2013). The Effect of Coping Mechanisms on Technology Induced Stress: Towards a Conceptual Model.

Weinert, C., Maier, C., & Laumer, S. (2014). *The Relationship between Psychological, Physiological, and Behavioral Strain towards Technostress*: Otto-Friedrich-Universität Bamberg.

Weinmann, M., Schneider, C., & Brocke, J. v. (2016). Digital Nudging. *Business and Information Systems Engineering, 58*, 433-436. doi:10.1007/s12599-016-0453-1

Weisband, S., & Kiesler, S. (1996). *Self disclosure on computer forms: Meta-analysis and implications.* Paper presented at the Proceedings of the SIGCHI conference on human factors in computing systems.

Weiss, A., & Tscheligi, M. (2013). Rethinking the human–agent relationship: Which social cues do Interactive agents really need to have? In *Believable Bots* (pp. 1-28): Springer.

Wen, W. E., Peng, C. R., & Jin, L. (2017). Judging a Book by Its Cover? The Effect of Anthropomorphism on Product Attribute Processing and Consumer Preference. *Journal of Consumer Research, 43*(6), 1008-1030. doi:10.1093/jcr/ucw074

Wessel, M., Adam, M., & Benlian, A. (2019). The impact of sold-out early birds on option selection in reward-based crowdfunding. *Decision Support Systems, 117*, 48-61.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 338-346.

Wong, J. C. (2019). The Cambridge Analytica Scandal Changed the World–but It Didn't Change Facebook. *The Guardian*.

Worchel, S., Lee, J., & Adewole, A. (1975). Effects of supply and demand on ratings of object value. *Journal of personality and social psychology, 32*(5), 906.

Wueest, C. (2017). A guide to the security of voice-activated smart speakers. *An ISTR Special Report, November 2017*.

Wuenderlich, N. V., & Paluch, S. (2017). *A nice and friendly chat with a bot: User perceptions of AI-based service agents.* Paper presented at the Proceedings of the Thirty Eighth International Conference on Information Systems (ICIS).

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *ICIS 2007 proceedings*, 125.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 Proceedings*, 6.

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*(2-3), 137-149.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009a). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Xu, H., Teo, H.-H., Tan, B. C., & 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), 1342-1363.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009b). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*, 135-174.

Xu, J., Benbasat, I., & Cenfetelli, R. T. (2010). *Does live help service matter? An empirical test of the DeLone and McLean's extended model in the e-service context.* Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

Yang, F., & Shen, F. (2017). Effects of web interactivity: A meta-analysis. *Communication Research, 45*(5), 1-24.

Yun, H., Lee, G., & Kim, D. J. (2014). A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns : Antecedents , Outcomes , and Moderators. *International Conference on Information Systems*, 1-13.

Zaichkowsky, J. L. (1985). Measuring the involvement construct. *Journal of Consumer Research, 12*, 341-352.

Zhou, S., & Guo, B. (2017). The order effect on online review helpfulness: A social influence perspective. *Decision Support Systems, 93*, 77-87.

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems, 48*(2), 395-406.

Zweig, D., & Webster, J. (2002). Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational behavior, 23*(5), 605-633.

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt und indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher nicht zu Prüfungszwecken verwendet und noch nicht veröffentlicht.

_____

Johannes Klumpe