Journal of the Association for Information Systems (2019) **20**(6), 787-823
doi: 10.17705/1jais.00551

RESEARCH PAPER

ISSN 1536-9323

"They're All the Same!" Stereotypical Thinking and Systematic Errors in Users' Privacy-Related Judgments About Online Services

Jin P. Gerlach[1], Peter Buxmann[2], Tamara Dinev[3]

[1]Technische Universität Darmstadt, Germany, gerlach@is.tu-darmstadt.de
[2]Technische Universität Darmstadt, Germany, buxmann@is.tu-darmstadt.de
[3]Florida Atlantic University, USA, tdinev@fau.edu

Abstract

Given the ever-increasing volume of online services, it has become impractical for Internet users to study every company's handling of information privacy separately and in detail. This challenges a central assumption held by most information privacy research to date—that users engage in deliberate information processing when forming their privacy-related beliefs about online services. In this research, we complement previous studies that emphasize the role of mental shortcuts when individuals assess how a service will handle their personal information. We investigate how a particular mental shortcut—users' stereotypical thinking about providers' handling of user information—can cause systematic judgment errors when individuals form their beliefs about an online service. In addition, we explore the effectiveness of counter-stereotypic privacy statements in preventing such judgment errors. Drawing on data collected at two points in time from a representative sample of smartphone users, we studied systematic errors caused by stereotypical thinking in the context of a mobile news app. We found evidence for stereotype-induced errors in users' judgments regarding this provider, despite the presence of counter-stereotypic privacy statements. Our results further suggest that the tone of these statements makes a significant difference in mitigating the judgment errors caused by stereotypical thinking. Our findings contribute to emerging knowledge about the role of cognitive biases and systematic errors in the context of information privacy.

Keywords: Information Privacy, Systematic Error, Stereotypical Thinking, Cognitive Bias, Privacy Statement, Privacy Risk

Paul Lowry was the accepting senior editor. This research article was submitted on August 22, 2017, and went through two revisions.

1 Introduction

In recent years, a large number of attention-grabbing media reports characterize online service providers as companies who sell user data to third parties or collect and analyze user data without consent. A *Forbes* report, which states that "a huge percentage of mobile apps are sharing your data with third parties" (Mathews, 2017) provides just one example and similar reports have appeared on a consistent basis on many news websites over the years (e.g., Bradley, 2013; Vaas, 2016). Meanwhile, incidents such as the one involving Facebook in 2018, in which personal user information was acquired by Cambridge Analytica without the users' consent seem to confirm this reputation of companies collecting and using large amounts of data for monetization (e.g., Confessore, 2018). These widespread reports paint a rather questionable picture of Internet-based services, and users, who may tend not to differentiate between services, might believe that all such companies engage in these practices. In this research, we investigate the potential that an

individual's generalized picture of online service providers may lead to biased judgments about a specific service and we explore what privacy-friendly companies can do to counteract such overgeneralizations.

A large body of research in the field of information privacy helps clarify how users form judgments about online services. Scholars have investigated a wide range of topics along these lines—such as different dimensions of privacy concerns (e.g., Malhotra, Kim, & Agarwal, 2004; Smith, Milberg, & Burke, 1996), the role of IT design (e.g., Sutanto, Palme, Tan, & Phang, 2013; Xu, Crossler, & Bélanger, 2012), and cultural influences (e.g., Dinev et al., 2006; Lowry, Cao, & Everard, 2011)—and have also explored a variety of contexts such as e-commerce (e.g., Pavlou, Huigang, & Yajiong, 2007; Xu, Dinev, Smith, & Hart, 2011), healthcare (e.g., Angst & Agarwal, 2009; Parks, Xu, Chu, & Lowry, 2017), and social networking sites (e.g., Cavusoglu, Phan, Cavusoglu, & Airoldi, 2016; Gerlach, Widjaja, & Buxmann, 2015; Ozdemir, Smith, & Benamati, 2017). The above seminal studies offer valuable insights but have mostly assumed that Internet users engage in deliberate and systematic information processing when it comes to their privacy online (Acquisti & Grossklags, 2005; Adjerid, Peer, & Acquisti, 2018; Dinev, McConnell, & Smith, 2015). Dinev et al. (2015, pp. 641-642) observe that the macromodels of information privacy research that integrate the rich body of extant literature "share a critical assumption that *responses to external stimuli result in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviors*" (emphasis in original). The authors point out that users' mental shortcuts have, for the most part, been overlooked in this research (Dinev et al., 2015).

This is a significant problem for companies that rely solely on those research results. For instance, many studies suggest that companies just need to act in a more privacy-friendly manner to reduce users' privacy risks and to benefit from higher service adoption numbers as a result. However, this overlooks the possibility that users might not actually recognize a privacy-friendly service as such, given their tendency to take mental shortcuts. But privacy-related information is often presented in overwhelming formats and individuals can hardly process all information relevant for their privacy (e.g., Kokolakis, 2017; Pan & Zinkhan, 2006). Thus, individuals do take mental shortcuts, making their judgments prone to systematic errors or predictable mistakes when judging specific services (e.g., Acquisti, Taylor, & Wagman, 2016). However, most privacy research does not adequately address the role of mental shortcuts in our everyday lives that has long been established in psychology research (e.g., Gabrielcik & Fazio, 1984; Tversky & Kahneman, 1974), and this is a critical gap that needs to be addressed.

This study adds to the small group of information privacy studies that challenge the prevailing view of Internet users as deliberate information processors when forming beliefs and making decisions. It aims to draw more attention to the perspective of mental shortcuts and the resulting potential for systematic errors in users' judgments about online services. We investigate a particular form of mental shortcut that individuals tend to employ, namely, *stereotypical thinking*. Stereotypical thinking is a natural human tendency that involves attributing certain characteristics that come readily to mind to the members of a group in an overgeneralized manner (e.g., Greenwald & Banaji, 1995; Judd & Park, 1993). Regarding online privacy, the constant and widespread media reports about online service providers who collect and monetize as much user data as they can make such companies a potential subject of negative stereotypical thinking. Indeed, it seems that users' general perceptions of how online service providers handle personal information involve strong beliefs that these companies sell personal information to third parties or engage in otherwise unethical or inappropriate behaviors (Sutanto et al., 2013).

Negative stereotypical thinking about online service providers has the potential to cause serious problems for privacy-friendly companies, which might fail to gain a competitive advantage in or even access to the market. For instance, users might believe that all Internet service providers collect more user data than they need or that all such companies sell these data to third parties. This stereotype could lead to undifferentiated and erroneous judgments about online services, as the generalized belief that all providers collect more data than they need might not apply to specific companies that do not rely on monetizing personal information to make a profit. Such erroneous judgments could, if unresolved, lead to overestimations of privacy risks and, hence, potential rejection of a privacy-friendly service. As a result, benefits for both the service's potential users—who might reject a promising service—as well as the service provider would be lost without any valid reason. To investigate this possible error in privacy-related judgments, our first research question (RQ) is:

RQ1: Are users' estimations of privacy risks prone to systematic errors due to stereotypical thinking?

To overcome the potential challenges associated with users' stereotypical thinking, companies might try to provide privacy assurances (e.g., privacy statements) that counter users' stereotypic beliefs in order to prevent systematic errors when users make judgments about the activities of the company. Given the potentially detrimental effects of stereotypical thinking, companies need to know whether such counter-stereotypic privacy information is effective for mitigating users' reliance on stereotypic beliefs, which

are usually rather robust (Stangor, 2000; Trope & Thompson, 1997). Moreover, we can observe that in practice, privacy statements tend to be written in different styles (e.g., with rational and fact-based vs. empathic and caring language) and, as we will detail below, this might influence the effectiveness of such information (e.g., Chaudhuri & Buck, 1995; Goodstein, 1993; Maheswaran & Chaiken, 1991; Rosselli, Skelly, & Mackie, 1995; Schmid Mast, Hall, & Roter, 2007). Thus, our second research question is:

RQ2: (How) can providers of services prevent systematic errors that are due to stereotypical thinking? In particular, will offering stereotype-deviating information that is toned a certain way mitigate the effects of the stereotypical thinking?

To explore these questions, we collected survey data from a representative sample of smartphone users at two points in time. Our results show that many users indeed subscribe to the stereotype that providers of online services generally collect and monetize personal user information extensively. We demonstrate participants' systematic judgment errors regarding the activities of a privacy-friendly mobile app provider, despite exposure to counter-stereotypic privacy statements. Interestingly, differently toned privacy statements varied in their effectiveness to prevent the systematic errors, which suggests that a provider's mere communication of a privacy statement is, by itself, not sufficient in this regard. Rather, to mitigate the consequences of stereotyping, it seems to be important that the provider addresses users on an emotional level and conveys a feeling of empathy, concern, and caring.

In the next section, we provide theoretical background on individuals' use of heuristics and stereotypical thinking, as well as an overview of privacy research that considers users' mental shortcuts in privacy-related judgments. Following that, we proceed with our hypotheses and describe our methodology. We then test our hypotheses and present the results of our data analysis. We conclude by discussing the implications and limitations of our research.

2 Theoretical Background

As detailed below, stereotypical thinking belongs to the family of heuristics, which represents different ways that humans form beliefs and make judgments by taking mental shortcuts (e.g., Chaiken, 1980; Petty & Cacioppo, 1986). Before we elaborate on stereotypical thinking, we briefly provide some background on heuristics in order to embed stereotypical thinking in its larger theoretical context.

2.1 The Role of Heuristics in Human Judgments

Humans do not always carefully gather and process all information that is available to them when they need to make decisions or judgments. What are now widely known as dual-process theories comprise a group of theories that share the idea of humans being cognitive misers who engage in effortful information processing only if they are motivated and have the cognitive capacities to do so (e.g., Maheswaran & Chaiken, 1991; Priester & Petty, 1995). These theories differentiate between two ways of processing information: one effortful processing system that is used when motivation and/or capacity are high, and one low-effort system that is used when motivation and/or capacity are low. Prominent representatives of these dual-process theories include the heuristic-systematic model (HSM), which distinguishes between systematic and heuristic information processing (e.g., Chaiken, 1977, 1980), and the elaboration-likelihood model (ELM), which refers to a central and a peripheral processing mode (Petty & Cacioppo, 1986). Both models were originally developed in the context of persuasion but apply universally to other judgment tasks as well (Chaiken & Maheswaran, 1994; Maheswaran & Chaiken, 1991; Rucker & Petty, 2006).

Dual-process theories represent fairly general frameworks for organizing and understanding the basic processes underlying human judgment (Chaiken, Liberman, & Eagly, 1989; Petty & Cacioppo, 1986). They all include the idea that, in contexts where motivation and cognitive capacity are rather low, different heuristics come into play when humans make judgments (Chaiken & Maheswaran, 1994; Dinev et al., 2015; Evans, 2008; Kahneman, 2003; Kahneman & Frederick, 2002; Petty & Cacioppo, 1986; Wegener, Clark, & Petty, 2006). Heuristics can be defined as "learned, declarative or procedural knowledge structures stored in memory" (Chen & Chaiken, 1999, p. 82). They represent general rules such as scripts and schemas that have been developed by individuals through experience and observation and reduce complexity by substituting attributes of judgment objects with heuristic attributes which come more readily to mind (Chaiken, 1980; Kahneman & Frederick, 2002). Among the family of heuristics is the heuristic of stereotypical thinking, which we describe in more detail in the following section.

2.2 Stereotypical Thinking: A Central Heuristic in Everyday Life

In general, people classify objects in their surroundings into categories and apply prior knowledge they have acquired about these categories (e.g., Maheswaran, 1994). These knowledge structures ("schemas") present "organized patterns of expectations about the

environment" (Sujan, 1985, p. 31). When an individual develops an impression about a specific member of the category, an immediate impression is formed based on the existing knowledge about the category that becomes salient (Fiske, Lin, & Neuberg, 1999; Petty & Wegener, 1999). We will discuss how additional, individuating information might be used by the perceiver to reevaluate this initial impression below. Stereotypes are knowledge categories that consist of (over)generalized beliefs about the members of a group, for instance, "Japanese cars are reliable" or "Germans are punctual" (e.g., Greenwald & Banaji, 1995; Judd & Park, 1993; Stangor, 2000). Acknowledging different definitions of the concept of a stereotype (e.g., Greenwald & Banaji, 1995), we follow Judd and Park (1993, p. 110), who consider a stereotype to be "an individual's set of beliefs about the characteristics or attributes of a group".

Due to the efficiency and speed with which category-based knowledge becomes available in a perceiver's mind, stereotypes are used as a heuristic (e.g., Bodenhausen, 1990; Bodenhausen, Sheppard, & Kramer, 1994; Macrae, Milne, & Bodenhausen, 1994; Wegener et al., 2006). In particular, stereotypical thinking has been categorized as an instance of the availability heuristic, which describes peoples' tendency to overestimate the frequency of a class or the probability of a certain event based on how easily it can be brought to mind (Tversky & Kahneman, 1974). Stereotypic beliefs about a group are those that are easily remembered and thus come to mind very easily—they are "available" in individuals' minds (e.g., Goldstein, 2005; Taylor, 1982). Thus, as a heuristic, stereotypical thinking belongs to the low-effort mode of information processing, which can be activated for a variety of reasons, such as a lack of motivation, time constraints, limited cognitive resources, lack of subject knowledge, certain emotions or moods, or an individual's need for cognition (e.g., Bodenhausen, 1990; Bodenhausen et al., 1994; Dinev et al., 2015; Macrae et al., 1994; Wegener et al., 2006). For instance, Macrae et al. (1994, p. 38), who label stereotypes as "energy-saving devices", mention that stereotypes are likely to be activated when individuals lack the ability to process a certain stimulus more carefully: "The message emerging from this research [on stereotypes] is a fairly consistent one: When the processing environment reaches a sufficient level of difficulty, and perceivers' resources are correspondingly depleted, stereotypes are likely to be activated and applied in judgmental tasks".

The problem with stereotypes is that they can lead to misjudgments of targets that generally belong to the stereotyped group but deviate from the stereotype (e.g., Judd & Park, 1993; Maheswaran, 1994). How can such misjudgments be avoided or prevented? Research suggests that stereotypic beliefs are not necessarily equivalent to an individual's final beliefs about a target of judgment if a judging person is given individuating and counter-stereotypic information (e.g., Blair, 2002; Chaiken & Maheswaran, 1994; Dasgupta, 2009; Fiske et al., 1999; Lai et al., 2014; Mitchell, Nosek, & Banaji, 2003). If such information is incongruent with the stereotypic beliefs, this can undermine the stereotypic inferences and trigger a more careful and systematic information-processing mode in order to make sense of this lack of congruency (e.g., Gawronski & Sritharan, 2010; Goodstein, 1993; Lai et al., 2014; Maheswaran & Chaiken, 1991). We will argue how this mechanism can be used to investigate our second research question below.

In sum, stereotypical thinking is a ubiquitous feature of everyday life and is used as a heuristic for category-based belief formation and judgment—one of different elements inside an individual's "cognitive toolbox" (Macrae et al., 1994). The significant role of stereotypes in human judgment is reflected by the wealth of research in psychology that has been dedicated to this heuristic. Many scholars, including the original developers of the HSM and ELM themselves, have studied stereotypical thinking as one particular heuristic and representative of the heuristic or peripheral processing mode considered in dual-process frameworks (Bodenhausen et al., 1994; Chaiken & Maheswaran, 1994; Dinev et al., 2015; Petty & Wegener, 1999; Wegener et al., 2006). Figure 1 illustrates how stereotypical thinking, as a particular heuristic, presents one way in which humans form beliefs and make judgments and shows how it is part of a broader dual-information-processing system, as explained by the HSM or ELM.

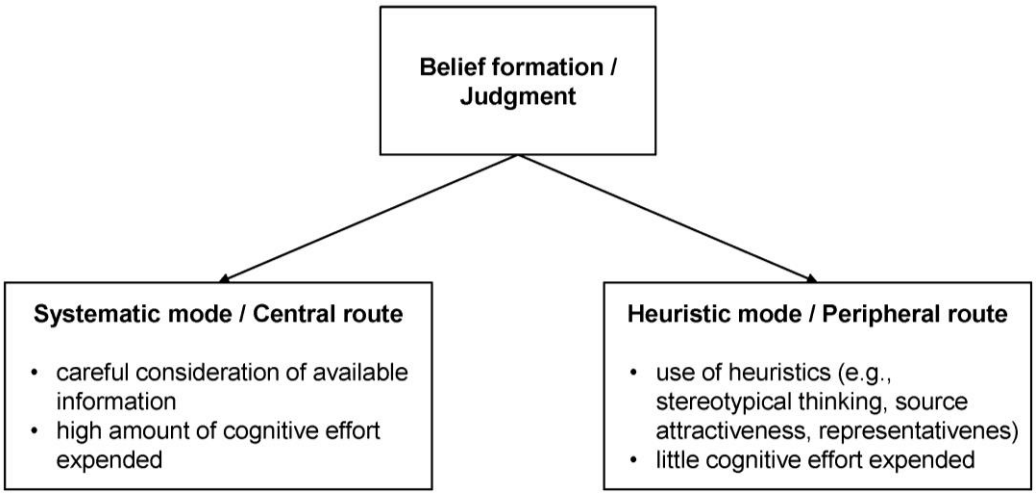

Figure 1. Dual-Processes in Humans' Belief Formation and Judgments (Simplified)

2.3 Individuals' Processing of Privacy-Related Information

As mentioned above, privacy research has largely assumed that individuals base their judgments on systematic information processing when assessing their privacy in the context of online services and has mostly overlooked the possibility that individuals' beliefs about an offering might be based on heuristics (Acquisti & Grossklags, 2005; Dinev et al., 2015). Only a few notable exceptions in the information privacy literature support this perspective (e.g., Acquisti & Grossklags, 2005; Angst & Agarwal, 2009; Lowry et al., 2012). Given the well-established centrality of mental short-cuts and heuristics in our everyday lives as well as in other areas of IS research (e.g., Arnott, 2006; George, Duffy, & Ahuja, 2000; Ramachandran & Gopal, 2010; Tversky & Kahneman, 1974), there is a pressing need for information privacy research to direct more attention to such heuristics and low-effort thinking.

This urgency becomes particularly relevant when considering the subset of privacy research concerned with how users deal with privacy-related information such as privacy statements and privacy seals. To date, these studies have produced highly mixed results in terms of whether and how such privacy-related information affects users' beliefs, attitudes, and behaviors (e.g., Bansal, Zahedi, & Gefen, 2015; Gerlach et al., 2015; Lowry et al., 2012). It stands to reason that the issue of heuristic information processing should be particularly relevant for this area of research. Thus, it is surprising that only very few models and theories include concepts or mechanisms which represent the idea that Internet users might not systematically process every piece of available information (e.g., Kovar, Burke, & Kovar, 2000; Lowry et al., 2012; Yang, Hung, Sung, & Farn, 2006).

The vast majority of existing research on privacy policies or statements and privacy seals includes no such concepts or mechanisms. Some studies in this area have even purposely diminished the possibility of low-effort processing by forcing participants to read privacy policies or by excluding participants from their analysis who did not pay attention to the information provided. A detailed overview of empirical research on the role of privacy-related information (e.g., policies, seals, other statements) in users' beliefs, attitudes, and behaviors can be found in Appendix A.

A few important exceptions exist that do consider individuals' low-effort information processing in their theorizing. Table 1 provides an overview of these studies' objectives and the findings most relevant to our research. They all acknowledge the possibility that humans might not carefully process all available information but instead rely on simple heuristics and mental shortcuts to form their beliefs and attitudes toward an online service. For instance, different characteristics of a website, such as its quality or the mere presence of privacy policies or privacy seals might increase individuals' perceptions of trust or privacy assurance (Bansal et al., 2015; Kovar et al., 2000; Lowry et al., 2012). Interestingly, these studies focus on mental shortcuts that individuals use to form their beliefs based on information that is provided by the online service itself and thus is *external* to the individual—such as privacy statements, privacy seals, or a website's design or information quality (e.g., Bansal et al., 2015; Lowry et al., 2012; Pan & Zinkhan, 2006; Yang et al., 2006).

In sum, most theories and models that are concerned with individuals' interactions with privacy-related information have neglected the idea that users might not systematically process all available information. The few studies shown in Table 1 provide valuable insights regarding individuals' low-effort information

processing but have focused on heuristic belief formation that uses information *external* to the individual, such as privacy seals or website design. But heuristics also include mental shortcuts where individuals form beliefs or make judgments based on structures that are *internal* to them, such as stereotypic beliefs or affect (e.g., Bodenhausen, 1990; Forgas, 1995). This perspective of heuristic belief formation based on information *internal* to an individual, such as stereotypes (i.e., stored knowledge structures), is still missing from the privacy literature. This gap calls for the attention of privacy researchers, especially since general research on stereotypes has emphasized this heuristic's importance in complex processing environments (e.g., Macrae et al., 1994)—for example, the privacy context, which is characterized by a complex abundance of privacy-related information. In this study, we seek to integrate research on privacy statements and stereotypes by investigating stereotypical thinking as a heuristic belief-formation device in a privacy context, and by examining the role of privacy statements as counter-stereotypic information capable of influencing individuals' heuristic, stereotype-based judgments.

Table 1. Studies Considering Low-Effort Processing of Privacy Information

Study	Objective	Relevant findings
Adjerid, Acquisti, Brandimarte, and Loewenstein (2013)	Illustrate how privacy notices' effects on disclosure behavior might be biased due to bounded rationality	The effects of privacy statements on individuals' behavior are subject to bounded rationality.
Bansal et al. (2015)	Examine how privacy assurance mechanisms influence trust from an ELM perspective	Several factors serve as peripheral cues that can increase an individuals' trust toward a website. These effects are moderated by an individual's privacy concerns.
Kovar et al. (2000)	Explore the influence of privacy assurance on individuals' online shopping from an ELM perspective	Noticing a privacy seal affects individuals' expectations and intentions to shop online.
Lowry et al. (2012)	Explore conditions under which privacy assurance is more or less effective from an ELM perspective	Several factors serve as peripheral cues on a website that increase an individuals' perceived privacy assurance. The presence of privacy statements serves as such a cue while privacy seals only do so if individuals understand and associate privacy assurance with them.
Pan and Zinkhan (2006)	Explore the impact of privacy statements on individuals' trust in an e-tailer	Individuals tend to read more of a privacy policy when the statement is short and straightforward.
Yang et al. (2006)	Investigate initial website trust formation from an ELM perspective	Privacy seals affect individuals' trust formation through peripheral route processing when product involvement is low or trait anxiety is high.

3 Research Framework and Hypotheses

Before proceeding to our research framework, we first clarify the specific stereotype that we examine in this research. As defined above, a stereotype presents a set of beliefs about the characteristics of a group (Judd & Park, 1993). Of course, multiple stereotypes can be associated with a single stimulus, such as a particular person who falls into several stereotypical categories at once (e.g., race, gender, and occupation-related stereotypes). In line with previous research on stereotypes (Darke & Ritchie, 2007; Maheswaran, 1994), we focus on one particular stereotype, which we describe next.

In this study, we investigate individual differences in terms of the extent to which users hold the stereotype that online service providers collect large amounts of user data and seek to monetize these data, but do not communicate clearly how they handle user information. We argue that this stereotype has developed for a significant proportion of people for several reasons. First, we conducted an inductive prestudy (details are reported in the methods section) to freely elicit participants' beliefs about how online service providers handle user information. The stereotypical attributes we have described above emerged as most relevant from this prestudy and this motivated us to continue research in this direction. Second, the development of such stereotypes can, to a significant degree, be generally attributed to mass media that often emphasize certain attributes of a group (e.g., Dasgupta & Greenwald, 2001; Wegener & Petty, 1997). In the case of online service providers, there is a wealth of media reports about the topic of Internet privacy, which contain generalized statements about the extensive collection and use of personal information by such companies (e.g., Bradley, 2013; Mathews, 2017; Vaas, 2016). As stereotypes develop through repeated activation in memory (e.g., Devine, 1989), these and other media reports likely contributed

to the development of this stereotype. Third, statistics of Internet users seem to confirm that beliefs about the extensive collection and commercial use of personal information are widely held in our societies. For instance, one study reports that the majority of American adults are not too confident or not at all confident that records of their activities maintained by different companies such as search engine providers or social media providers will remain private and secure (Madden & Rainie, 2015). Therefore, while acknowledging that other stereotypes associated with providers of online services might exist, our study focuses on the stereotype that such companies collect large amounts of user data and utilize these data for monetization but do not communicate clearly how they handle user information.

Note that stereotypes are not a purely human affair but can exist for other categories, such as products, services, institutions, or other living creatures as well (e.g., Darke & Ritchie, 2007; Foroni & Mayr, 2005). For instance, many consumers have developed the stereotype that advertising (as a category) is deceptive and can undermine trust "even in the face of strong product benefits" (Darke & Ritchie, 2007, p. 124). Likewise, stereotypes can influence product-related attitudes, if consumers engage in category-based judgments based on the products' country of origin (e.g., Bilkey & Nes, 1982). Our stereotype should be associated with the category "providers of online services". In effect, this stereotype is indirectly attributed to human decision makers because providers of online services are represented by people who make the decisions about what data to collect and how to use them.

3.1 Overview of the Research Model

In the following subsections, we develop our research model, which is summarized in Figure 2. At an abstract level, this model integrates the notion of stereotypes with research on privacy statements to demonstrate the potential of systematic judgment errors in the context of online privacy and the role of counter-stereotypic information in this regard. As a heuristic, stereotypical thinking is used by individuals by relying on (seemingly appropriate) category-based knowledge (Macrae et al., 1994; Maheswaran, 1994; Schneider, 2005). But heuristics, in general, and stereotypical thinking, in particular, can lead to severe but predictable misjudgments (i.e., systematic errors) (e.g., Goldstein, 2005; Judd & Park, 1993; Macrae et al., 1994; Taylor, 1982; Tversky & Kahneman, 1974), and thus to overestimated risk perceptions. This consequence is significant, as unjustified inferences can have strong implications for both the misjudging individual and the target.

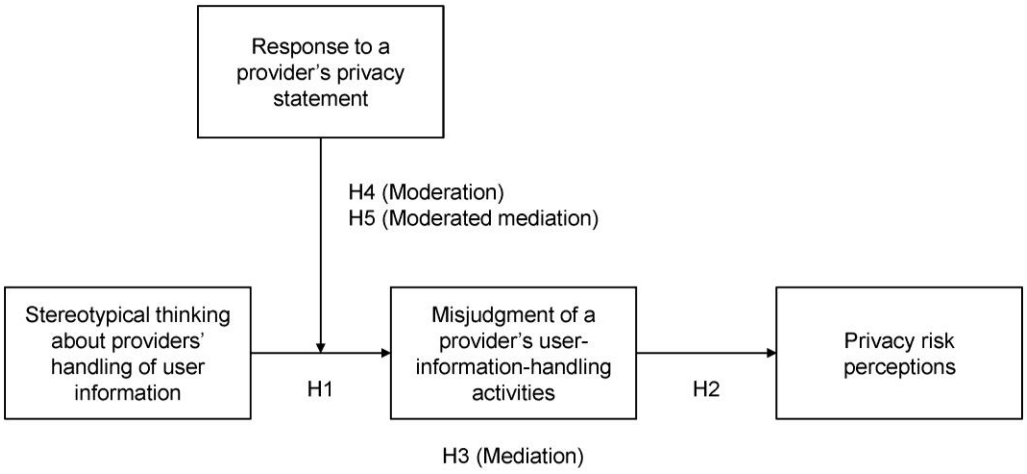

Figure 2. Dual-Processes in Humans' Belief Formation and Judgments (Simplified)

To clarify the boundaries of our study, our research model focuses on misjudgment that works *against* providers of online services as it can eventually result in an *overestimation* of privacy risks. This complements the abovementioned privacy research that considers heuristics that work *in favor* of an online service provider. For instance, these studies have demonstrated that the presence of a company's physical address and contact information, its design appeal, and the mere presence of a privacy statement can serve as heuristic cues that *increase* users' perceived privacy assurance or trust (e.g., Bansal et al., 2015; Lowry et al., 2012; Yang et al., 2006).

3.2 Stereotypical Thinking, Misjudgment, and Privacy Risk Perceptions

We first hypothesize that stereotypical thinking will lead to systematic errors (i.e., misjudgments) when our stereotype is applied to a privacy-friendly service. In line with previous research (e.g., Greenwald & Banaji, 1995; Judd & Park, 1993) and based on the stereotype we investigated in our study, we define a user's stereotypical thinking about online service providers' handling of user information as the extent to which the individual perceives providers of online services as a homogenous group that extensively collects and monetizes such information and does not communicate these practices clearly. For example, a user might believe that *all* online services collect more data from their users than they actually need and that they use these data for extensive profiling without clearly communicating this to users.

Stereotypical thinking, as defined above, should not be confused with the concept of individuals' dispositional privacy concerns (e.g., Smith et al., 1996). Although both concepts pertain to the practices of online firms with regard to user data, stereotypical thinking reflects the extent to which an individual *generalizes* regarding the practices of online companies, whereas privacy concerns indicate the degree to which a user *worries* about adverse outcomes of submitting personal information on the Internet (Malhotra et al., 2004; Smith et al., 1996). Users may worry to a great extent about their privacy, but that does not necessarily mean that they think that every company acts in the same way ("they're all the same"). Conversely, users may not be concerned about their privacy online (e.g., due to a lack of personal involvement) but still think that all online service providers gather as much data as they can. Dispositional privacy concerns also capture an individual's values—in other words: how the world *should* be with respect to these companies' handling of user information (Malhotra et al., 2004; Smith et al., 1996). In contrast, stereotypical thinking does not capture an individual's beliefs with respect to what online companies *should* do but what this group of providers *actually does*. In this research, we want to explore systematic judgment errors which are due to humans' tendencies to overgeneralize in situations where individuation is necessary. This objective requires us to consider individuals' stereotypical thinking as opposed to their privacy concerns, which do not capture the same concept.

Following prior work on systematic errors in peoples' judgments (e.g., Gabrielcik & Fazio, 1984; Hamilton & Gifford, 1976), we assume that users form a set of beliefs about a target entity's properties when assessing that entity. These beliefs then serve as a foundation for subsequent evaluations such as benefits and risks of a situation, but they can be incorrect from an objective standpoint. Based on research on systematic errors and misjudgments (Judd & Park, 1993; Tversky & Kahneman, 1974), we define a user's misjudgment of a provider's user-information-handling activities as the strength of the user's erroneous beliefs about how the provider collects and uses personal information. Users who strongly misjudge a target will be confident that their (objectively false) beliefs about the target are correct. Users who do not misjudge the target will not include false assumptions regarding how the provider handles user data among their beliefs.

As stated above, stereotypical thinking is categorized as an instance of the availability heuristic and is used by individuals as a cognitive shortcut to make sense of a situation (Maheswaran, 1994; McGarty, Yzerbyt, & Spears, 2002). Stereotypical thinking as a low-effort belief-formation device can thus lead to the misjudgment of a target that deviates from the stereotype, because individuals make the mistake of overgeneralizing beliefs that are readily available (e.g., Judd & Park, 1993; Maheswaran, 1994)—that is, they apply general beliefs without taking specific characteristics of the given entity into account. As Stangor (2000, p. 7) points out, "using stereotypes is unfair to the individuals being judged, because since no stereotype is true of all of the category members, it may not be true of this individual". Misjudgment is facilitated even further because people tend to make sense of ambiguous information in a manner that is consistent with their stereotypes (Sagar & Schofield, 1980; Trope & Thompson, 1997).

Turning to the context of online services, users are usually uncertain about the actual activities of providers regarding their personal information (e.g., Acquisti, Brandimarte, & Loewenstein, 2015; Pavlou et al., 2007; Peslak, 2005). As argued above, we believe that many users hold stereotypic beliefs about providers of Internet-based services, shaped by current media reports that emphasize the negative treatment of user information by those providers. Furthermore, privacy-related information that could serve individuals' careful information processing and more

systematic belief formation (e.g., privacy policies, privacy seals) is usually presented in overwhelming formats. This can include large amounts of text that uses legalese and/or technical language (e.g., Pan & Zinkhan, 2006) or symbols that do not carry any meaning for many individuals (e.g., Lowry et al., 2012), which reduces their ability to process and interpret such information. Research on stereotypes suggests that in complex processing environments such as the privacy context, individuals increasingly rely on stereotypes as energy-saving belief-formation devices (e.g., Bodenhausen et al., 1994; Macrae et al., 1994; Wegener et al., 2006). As a result, users should tend not to assess each service provider individually and instead apply their stereotypic beliefs generally to all providers. Given a provider who conducts a privacy-friendly business, such stereotypical thinking will lead to systematic misjudgment of this specific provider, who will therefore not receive a thoughtful assessment from the user. We hypothesize:

H1: Higher levels of stereotypical thinking (i.e., how strongly an individual holds the particular stereotype described above) are associated with greater degrees of misjudgment regarding a provider's activities.

Next, we argue that users' misjudgments affect their perceptions of privacy risk. A user's perceived privacy risk is defined as "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm" (Smith, Dinev, & Xu, 2011, p. 1001). Privacy risk perceptions play an important role in a user's privacy calculus that determines how to act in Internet settings (e.g., Dinev & Hart, 2006; Ozdemir et al., 2017; Xu, Teo, Tan, & Agarwal, 2009). In this calculus, privacy risk perceptions indicate the costs that users associate with giving up personal information to a firm, the costs that are weighed against the benefits to decide whether to disclose information (e.g., Dinev & Hart, 2006).

It is important to note that individuals' privacy risk perceptions (i.e., fear of loss) are distinct from their misjudgments (i.e., erroneous beliefs about a business's information-handling activities). Individuals who strongly misjudge a provider may nevertheless perceive little or no associated risk ("Yes, I know they all collect and sell my data, and I am sure this provider does it too, but I don't care"). Thus, two users with equally strong erroneous beliefs about a provider's activities might still differ in their risk perceptions. This is supported by research that points to individual differences in the perceptions of certain privacy-related practices and argues that the same practices might be perceived as more or less harmful by different individuals (Hann, Hui, Lee, & Png, 2007; Karwatzki, Trenz, Tuunainen, & Veit, 2017).

When a user believes that a provider engages in extensive collection and use of personal information, but this is actually not the case, the user misjudges the provider's information-handling activities. The stronger the erroneous beliefs (i.e., the misjudgment), the more certain the user will be about the provider's acquisition and use of personal information. In turn, the belief that a provider engages in these activities will constitute a basis for perceiving an actual potential for loss (i.e., a privacy risk; e.g., Dinev & Hart, 2006). Therefore, a strong misjudgment ("because everybody collects data, I am sure this provider does it too") will be associated with a stronger fear of loss, that is, with a stronger perception of risks. Hence, stronger misjudgments of privacy-friendly providers' practices should be associated with higher risk perceptions:

H2: An individual's misjudgment of a provider's personal data collection activities is positively associated with the individual's privacy risk perceptions.

We also propose a mediation hypothesis suggesting an indirect effect of stereotypical thinking on perceived privacy risks—that is, stereotypical thinking might also distort users' privacy risk perceptions. This is similar to news reports about plane crashes that can trigger heuristic processing and lead to overestimations of one's own flying risks (Slovic, Fischhoff, & Lichtenstein, 1980). Based on our arguments leading to H1 and H2, misjudgments about the activities of a provider should mediate the relationship between a user's stereotypic beliefs about providers of online services in general and the risk perceptions regarding the specific service:

H3: An individual's misjudgment of a provider's personal data collection activities mediates the effect of stereotypical thinking on the individual's privacy risk perceptions.

3.3 Users' Responses to Stereotype-Deviating Privacy Statements

Providers of privacy-friendly services must, by all means, avoid having interested users unnecessarily scared away due to misjudgments. A central question for privacy-friendly companies is, therefore, whether users' stereotypical thinking might lead to misjudgments of their service even when these users are provided with information that contrasts their stereotypic beliefs. According to dual-process theories, category-based beliefs such as stereotypes are very accessible in memory and therefore come to mind easily and quickly (e.g., Fiske et al., 1999; Petty & Wegener, 1999). However, dual-process theories, in general, and research on stereotypes, in particular, also support that although many people hold stereotypes and activate them, these stereotypic thoughts do not necessarily equate with their final beliefs about a

judgment stimulus. Instead, activated category-based beliefs can be altered in a specific context if the perceiver can be effectively provided with individuating information that better represents the specific characteristics of a particular category member (e.g., Blair, 2002; Chaiken & Maheswaran, 1994; Dasgupta, 2009; Fiske et al., 1999; Lai et al., 2014; Mitchell et al., 2003). This information might be incongruent with existing beliefs about the stereotyped group and thus undermine the validity of stereotypic, heuristic-based inferences (e.g., Gawronski & Sritharan, 2010; Goodstein, 1993; Lai et al., 2014).

In general, such belief-altering information must be made very accessible to individuals whose beliefs are to be changed (Gawronski & Sritharan, 2010). In this research, we thus focus on concise privacy statements which are made highly accessible to individuals. This focus aligns with previous arguments and findings that privacy-related information must be made very accessible to individuals and must not require much effort on part of the users if a provider wants users to pay attention to this information (Milne & Culnan, 2004; Pennington, Wilcox, & Grover, 2003; Tsai, Egelman, Cranor, & Acquisti, 2011). Thus, we do not consider privacy policies that require higher amounts of effort on part of the individual to access and understand or privacy seals that may not be understood in their meaning at all (e.g., Kim, Steinfield, & Lai, 2008; Lowry et al., 2012). If users are provided with highly accessible counter-stereotypic information, they may discard stereotype-based beliefs and rely more on the individuating information in this situation.

Before stating our hypotheses based on the arguments above, we want to note that it is important that individuals are not only provided with but that they actually *perceive* privacy-related information (e.g., Lowry et al., 2012). Thus, to assess the effectiveness of counter-stereotypic information, we consider individuals' responses to differently toned privacy statements they are provided with. To investigate a first baseline effect, we define an individual's basic response to a stereotype-deviating privacy statement as the degree to which a user feels provided with information that simply contrasts the stereotype but does not include any additional persuasive arguments. Such statements with a lack of additional persuasion (1) represent privacy statements in practice that do not include any arguments in addition to their plain factual statements, and (2) serve as a foundation to investigate privacy statements that do include such additional persuasive arguments. We now hypothesize that such basic counter-stereotypic information, if perceived by the user, might weaken the influence of stereotype-based beliefs, and therefore the relationship between stereotypical thinking and a user's misjudgment of a provider.

H4a: An individual's basic response to a highly accessible stereotype-deviating privacy statement moderates the positive relationship between stereotypical thinking and misjudgment of a specific provider's activities. In a situation in which a user feels provided with counter-stereotypic information, the user's stereotypical thinking will lead to less misjudgment.

Departing from this baseline hypothesis that is concerned with an individual's basic response to counter-stereotypic information, we now argue that additional appeals make a difference in how the individual feels addressed by such information. In practice, a provider might want to enrich pure counter-stereotypic information with additional appeals to increase the information's argument strength. A stronger argument could, in turn, enhance the persuasiveness of counter-stereotypic information (e.g., Chaiken & Maheswaran, 1994; Rucker & Petty, 2006). To capture individuals' perceptions of additional appeals, we rely on communication research that commonly distinguishes between cognitive and emotional appeals of persuasive messages (e.g., Aaker & Williams, 1998; Adler, Iacobelli, & Gutstein, 2016; Fox & Amichai-Hamburger, 2001; Schmid Mast et al., 2007). Communication research distinguishes whether a communication affects the receiver on a cognitive, reason-based level or on a more emotional level. In our study, we therefore consider how pure counter-stereotypic information can be augmented by adding information that increases the message's cognitive or emotional appeal. We accordingly define an individual's cognitive response to a stereotype-deviating privacy statement as the degree to which a user feels provided with counter-stereotypic information that also addresses the individual on a logical, reason-oriented level. Similarly, we define an individual's emotional response to a stereotype-deviating privacy statement as the extent to which a user feels provided with counter-stereotypic information that also conveys a sense of empathy, caring, or concern on part of the provider. In line with H4a, we hypothesize that both cognitive and emotional responses moderate the effect of stereotypical thinking on misjudgment.

H4b: An individual's cognitive response to a highly accessible stereotype-deviating privacy statement moderates the positive relationship between stereotypical thinking and misjudgment of a specific provider's activities.

H4c: An individual's emotional response to a highly accessible stereotype-deviating privacy statement moderates the positive relationship between stereotypical thinking and misjudgment of a specific provider's activities.

Moreover, communication research further suggests that cognitive and emotional appeals might be more or less effective, depending on the specific context of

communication (e.g., Fox & Amichai-Hamburger, 2001; Schmid Mast et al., 2007). We argue that, in our context, emotional appeals that convey a sense of an empathic provider who shows "other-focused" emotions (i.e., care, empathy, or concern) should be less congruent with the stereotype of a self-centered, utility-maximizing company. Cognitive communication, on the other hand, focuses on explanations, reasons, and rationalization (e.g., Fox & Amichai-Hamburger, 2001) and thus is more congruent with the stereotype of a utility-maximizing provider. According to dual-process research, incongruent information that is atypical of an evoked schema should be more effective in preventing heuristic processing and should elicit more extensive processing by individuals (e.g., Goodstein, 1993; Maheswaran & Chaiken, 1991). Furthermore, other-focused, empathic communication that involves caring about the user instead of focusing on the provider increases the personal relevance of the privacy statement for the user and therefore the attention paid to it (Bodenhausen, 1990; Lai et al., 2014; Rucker & Petty, 2006). Hence, we expect that a user's emotional response to a stereotype-deviating privacy statement will be more effective in preventing stereotype application than a cognitive response. We propose:

H4d: The stereotype-mitigating effect is stronger for an emotional response to a privacy statement than for a cognitive response.

The full research framework is shown in Figure 2 at the beginning of this section. Together, our hypotheses specify a moderated mediation model (e.g., Preacher, Rucker, & Hayes, 2007) that suggests that the indirect effect of stereotypical thinking on privacy risk perceptions is conditional on users' responses to a provider's privacy statement. Consistent with H3 and H4a-d, we expect that users' responses to a stereotype-deviating privacy statement will also influence the strength of the indirect effect of stereotypical thinking on perceived privacy risk:

H5: An individual's responses to a stereotype-deviating privacy statement moderate the mediated effect of stereotypical thinking on perceived privacy risk.

4 Research Methods

We conducted a survey in the context of mobile apps, which have often been criticized for privacy violations and thus make this market a highly relevant context to study (e.g., Bradley, 2013; Keith, Babb, Lowry, Furner, & Abdullat, 2015; Keith, Thompson, Hale, Lowry, & Greer, 2013; Vaas, 2016). Participants were asked to judge the provider of a specific app in terms of collection and use of personal information. The company addressed by the survey deviates from the stereotype in a privacy-friendly way, and participants were provided with counter-stereotypic information, allowing for an assessment dedicated to this specific provider.

4.1 App Description and Presentation

As our study context, we selected a real app over a hypothetical mock-up scenario to increase the realism for our participants and to stay consistent with research on systematic errors, which requires the researchers to assess deviations between participants' estimates and objective facts (e.g., Gabrielcik & Fazio, 1984; Hamilton & Gifford, 1976; Tversky & Kahneman, 1974). We chose an existing mobile app that is available for both Apple iOS and Android and basically provides users with personalized news reports collected from different sources. Based on personalization algorithms, the app determines which news articles might be most interesting to individual users. We selected this app for two reasons. First, the authors had a trusting relationship with the app's provider. Thus, we could be sure that our information about the actual practices of data collection and use were accurate. This perspective would be central to our assessment of users' misjudgments, as we knew whether participants' beliefs about the provider's activities related to user data were objectively correct. Second, our hypotheses required a context in which we could actually demonstrate systematic errors in users' judgments. Therefore, a second prerequisite for our study was that the chosen app needed to provide a privacy-friendly case that deviates from users' stereotypic beliefs. This is in line with extant studies on systematic biases and judgment errors, which present study participants with stimuli that researchers know are prone to misjudgments (e.g., Tversky & Kahneman, 1973, 1974). Hence, we selected a provider who cares about users' privacy and collects very little information from its users, using it only for purposes related to the service's functionality.

As part of our survey, all participants were shown the official app description copied from Apple's iTunes store as well as relevant information such as the price (free), space requirements, screenshots, and average user ratings. This setting would thus resemble the situation in which a user who is interested in a mobile app first assesses the service by looking at its description. To exclude the factor of app quality from our study, we increased the app's star rating from 4.0 (as shown by the app store's information) to 4.5. The app's name was hidden, to preserve the provider's anonymity and prevent users from looking up additional information during the survey.

With the provider's permission, we complemented the app description with a concise and highly accessible privacy statement that included counter-stereotypic information and allowed for an assessment of the provider. The privacy statement was a brief text that was included in the app description (for a similar

procedure, see Keith et al., 2015). We created differently toned versions of this statement to elicit variations in the response types, as needed to test our hypotheses. The statements offered similar content that deviated from users' stereotypic beliefs (i.e., no collection of unnecessary data, no selling of personal information, no use beyond news personalization), but they differed in how this content was communicated. In accordance with H4a, we first constructed a version of the statement that included basic counter-stereotypic information without any additional persuasion. In line with H4b-d, and based on research on communication styles (e.g., Marcus, 2000; Rosselli et al., 1995; Schmid Mast et al., 2007), we constructed two augmented statements with increased argument strength: one version that, in addition to the pure counter-stereotypic information, addressed the readers' cognitions and reasoning, and a second, emotion-oriented version intended to convey the feeling of an empathic provider who understands and cares about its users' concerns. Table 2 presents the three statements.

Table 2. Stereotype-Deviating Privacy Statements

Style	Privacy statement
Basic information	"We do not collect any unnecessary data or sell personal information to third parties. Your personal information is only used to provide news that will be interesting to you personally".
Cognitive, reason-oriented	"We earn money exclusively through premium-content subscriptions. Therefore, we offer in-app sales to interested users for 4.99€ per month. This means that our business model is not based on the collection of unnecessary data or selling personal information to third parties. Your personal information is only used to provide news that will be interesting to you personally".
Emotional, empathic	"To all our users: We are smartphone users like you who value our own privacy. We know about the concerns many users have about their data these days. We therefore assure you that we do not collect any unnecessary data or sell personal information to third parties. Your personal information is only used to provide news that will be interesting to you personally".

4.2 Data Collection and Sample

Participants were recruited by invitation through a professional survey firm in 2016 following a procedure similar to other studies using third-party services(e.g., Berger, Matt, Steininger, & Hess, 2015; Bulgurcu, Cavusoglu, & Benbasat, 2010). While recruitment was outsourced to this vendor, we hosted the survey itself. We aimed at collecting a sample that was representative for the population of smartphone users in our country (Germany).

We collected our data at two points in time to prevent common method bias (CMB) (e.g., Podsakoff, MacKenzie, & Podsakoff, 2012). [1] In particular, we needed to avoid the possibility that, after assessing the indicators for stereotypical thinking, the participants would try to appear consistent when judging our mobile app. We therefore surveyed users' stereotypic beliefs and the control variables in a first questionnaire independent of the mobile app survey. A week later, we contacted all participants again to present information about the mobile app, as described above, and asked them to assess scales regarding the app and the provider (e.g., misjudgment of a provider's activities, privacy risk). We matched data from the rounds using the participants' survey IDs provided by the vendor. Participants were assured of anonymity because their email addresses were known only by the vendor, while the survey data were only available to us.

For the first round, 491 invitations were sent to individuals who were registered with the survey firm as smartphone users. A common practice when working with a survey firm is to screen out ineligible participants at the beginning of the survey (e.g., Bulgurcu et al., 2010). As a result, we immediately screened out 62 participants because enough individuals in their age or gender classes had already participated. This allowed us to achieve age and gender distributions that matched those of the general population as closely as possible. We rejected another 36 individuals due to failed attention checks. Specifically, we included an item in our questionnaire that required participants to always check the "strongly agree" option. Of the remaining 393 participants, 376 completed the first-round questionnaire (95.7 percent). These 376 individuals received an invitation to the second round one week after their initial participation. In sum, 368 participants accessed the second survey, 26 of these were excluded due to failed attention checks, as reported above. Three hundred twenty-one of the remaining 342 participants completed the second round (93.9 percent) and therefore comprised our final sample. Table 3 shows the demographic characteristics of our final sample.

[1] Please refer to Appendix B for additional ways how we counteracted CMB.

Table 3. Sample Characteristics

Variable		Data	Variable		Data
Age	14-19	36 (11.2 %)	Occupation	Student	79 (24.6 %)
	20-29	88 (27.4 %)		Employee	169 (52.6 %)
	30-39	70 (21.8 %)		Self-Employed	24 (7.5 %)
	40-49	71 (22.1 %)		Unemployed	5 (1.6 %)
	50-59	41 (12.8 %)		Retired	17 (5.3 %)
	60-69	11 (3.4 %)		Homemaker	21 (6.5 %)
	≥ 70	4 (1.2 %)		Other	6 (1.9 %)
Gender	female	153 (47.7 %)			
	male	168 (52.3 %)			
Total		**321 (100 %)**			**321 (100 %)**

In the second round, respondents were randomly presented with one of the three privacy statements while a fourth group was shown no statement at all. We included this no-statement condition to test a confounding effect—namely, that the presence of privacy-related information might trigger and thus increase privacy risks for individuals who would have otherwise remained unconcerned (e.g., Dinev et al., 2015; Keith et al., 2015). Comparing perceived privacy risks between the different groups however showed no reason for concern; those in the no-statement group perceived significantly higher privacy risks than the other groups (4.57 in the no-statement group vs. 3.84, 3.96, and 3.95, $p = .004$). Furthermore, as intended, the different privacy statements affected participants' different response types toward these statements. T-tests confirmed that the mean values for the different response variables were significantly higher in the respective treatment groups compared to the other groups. In the group that received the cognitive statement, the average cognitive response was 4.45 compared to 2.95 for those outside this group ($p < .001$). For the emotional statement, the average emotional response was 4.64 compared to 3.69 for the rest of the participants ($p < .001$). Finally, for the statement without cognitive or emotional appeals, the basic response was 4.88 on average compared to 3.85 in the other groups ($p < .001$). In general, group sizes ranged from 78 to 83. We used a MANOVA to test for differences regarding all study variables that did not depend on group membership and found no significant differences among the groups.

4.3 Measures, Measurement Quality, and Control Variables[2]

Participants' stereotypical thinking was measured as a mean composite index using an established technique that requires individuals to estimate the percentage of group members that possess certain characteristics (e.g., Haslam et al., 1996; Stangor, 2000; Stephan et al., 1993; Zarate, Garcia, Garza, & Hitlan, 2004). A high score on this type of measure indicates that the rater perceives a high degree of group homogeneity. For each characteristic, responses are provided on a 10-point scale ranging from 1 (0-10%) to 10 (90-100%), with higher percentages indicating a higher degree of stereotypical thinking. To ensure the quality of this index measure, we followed the widely recommended procedures for index construction suggested by Diamantopoulos and Winklhofer (2001), as validity procedures for reflective measures do not apply to index measures. First, to ensure that the items used would cover the content of the focal construct (i.e., stereotypical thinking about online companies' handling of user data), we conducted a prestudy among students of our business school ($N = 42$). They were asked in a neutral way how they thought providers of websites and mobile apps would handle users' data. We asked them to spontaneously write down aspects that came to mind and assured them that there were no "right" or "wrong" answers. From this pool of characteristics, we identified 10 dominant themes for which we formulated the final items. Second, we assessed multicollinearity by examining the variance inflation factors (VIFs) among the indicators. No value exceeded 2.7 so all VIFs were well below the recommended threshold of 3.3. Third, we evaluated the

[2] All scales, along with the time of their measurement and the measurement quality, are listed in Appendix C.

external validity of this measure by (1) correlating the indicators with a theoretically related variable, and (2) assessing nomological validity of the whole index (Diamantopoulos & Winklhofer, 2001). We removed one indicator was because it did not correlate at all with misjudgment as a theoretically related variable. Further, as reported in our results section, the overall stereotypical thinking index was significantly related to its outcome variable, confirming the construct's nomological validity.

In order to assess individuals' misjudgments of the provider's activities, we calculated a mean composite index, following prior research on cognitive biases and systematic errors that measured the deviation between users' beliefs about the provider's activities and the known objective values (e.g., Gabrielcik & Fazio, 1984; Hamilton & Gifford, 1976). In particular, we asked the study participants to what extent they thought the provider of the case mobile app would engage in each of nine listed activities related to personal user information (using 7-point Likert scales). Again, we followed the procedures recommended by Diamantopoulos and Winklhofer (2001) to validate our measure. First, to create items that covered the content of the construct's domain, we relied on Culnan's (1993) three dimensions of secondary data use as a framework representing potential activities with regard to user data. Thus, based on this framework and our inside knowledge about our mobile news app, we carefully developed a list of nine items that represented potential activities of the app's provider with respect to personal information. Of these nine activities, the provider actually engaged in only two—the seven other activities represented "incorrect" items. As outlined above, we knew the case provider's true activities and therefore knew that higher ratings on the seven incorrect items would represent greater misjudgment and erroneous beliefs. Second, we calculated VIFs to examine potential multicollinearity issues. Initially, for two items, the VIFs exceeded the recommended thresholds of 3.3 (values of 4.8 and 4.7 respectively). After removing the item associated with the higher VIF that was highly correlated with the second item, all VIFs were below 2.7 and the threshold of 3.3. Third, we tested the construct's external validity by confirming that all remaining indicators were significantly correlated with a theoretically related variable (i.e., privacy risk). In addition, the construct's nomological validity was confirmed by our study, as the overall index showed significant relationships with its hypothesized antecedent and outcome variables as well.

Multi-item reflective measures were used to assess perceived privacy risks and users' responses to privacy statements. We measured perceived privacy risk using the four-item scale provided by Xu et al. (2011). In these items, we replaced "website" with "app", to match our study's focus. To calculate users' privacy risk perceptions, we used the mean value of the four items (e.g., Im & Rai, 2014). To measure users' cognitive, emotional, and basic responses to the privacy statements, we developed three new scales, each consisting of three reflective items. The scale for measuring a cognitive response assessed whether respondents perceived that the provider offered a rational argument for its counter-stereotypic privacy statement. The scale for an emotional response measured the extent to which the provider conveyed a feeling of empathy and a sense of caring about users' privacy. Finally, the scale for users' basic responses to counter-stereotypic information measured whether users felt they were provided with pure stereotype-deviating information without any additional persuasive arguments. To examine the content validity of these scales, we followed the procedure described by MacKenzie, Podsakoff, and Podsakoff (2011). After two iterations involving seven IS researchers and an additional assessment by nonacademic participants, we deemed the scales to be adequate. For each of the three scales, we calculated the mean value of the related items (e.g., Im & Rai, 2014).

To assure the quality of these multi-item reflective measures, we assessed common criteria for scale validity and reliability. Since the three scales to measure users' responses to privacy statements were newly developed, we conducted a quantitative prestudy prior to the main data collection. Therefore, participants were recruited on the campus of a large Western European university (N = 195). The pretest data showed good quality for the newly developed scales for users' responses to the privacy statements. Cronbach's alpha, composite reliability (CR), and the average variance extracted (AVE) all met the recommended thresholds of 0.7, 0.7, and 0.5, respectively (MacKenzie et al., 2011). Regarding discriminant validity, both an exploratory factor analysis (EFA) and the Fornell and Larcker (1981) criterion showed no concerns. For our main data collection, all reflective-item measures showed good quality with respect to the same evaluation criteria. We computed Cronbach's alpha using SPSS, and all values exceeded the recommended threshold of 0.7 (MacKenzie et al., 2011). We further calculated CRs and AVEs using MPlus, and all were above the cutoff values of 0.7 and 0.5 (MacKenzie et al., 2011). To assess discriminant validity, we followed Fornell and Larcker (1981) and compared the square roots of AVEs with the bivariate correlations. We further conducted an EFA to check item loadings and cross-loadings (Appendix D). We identified no concerns about discriminant validity.

We included the following control variables: Internet trust, Internet use, smartphone operating system (OS), age, and gender. First, prior research has shown that trust is central to Internet users' online behaviors (e.g.,

Dinev & Hart, 2006; Lowry, Vance, Moody, Beckman, & Read, 2008). Second, users' privacy risk perceptions are negatively related to their experience using the Internet (Malhotra et al., 2004). Third, the smartphone operating system Android has been associated with higher privacy and security risks than Apple's iOS (e.g., Gruman, 2015). Finally, previous research has documented both age and gender differences regarding risk perceptions in a variety of contexts such as smoking, driving, and online behavior (e.g., Garbarino & Strahilevitz, 2004; Viscusi, 1991).

5 Hypothesis Testing and Results

Table 4 shows the bivariate correlations for all study and control variables. Participants exhibited high levels of stereotypical thinking (M = 7.32, 10-point scale), and their systematic misjudgments were rather strong (M = 5.09, 7-point scale with the low anchor representing no misjudgment). Gender, smartphone OS, and Internet use showed no significant bivariate correlations with other variables at a 5% level, although correlations between gender and trust (p = .053), Internet use and cognitive response (p = .108), and smartphone OS and trust (p = .069) were marginally significant.

Our model structure suggests moderated mediation, meaning that the independent variable's effect on the dependent variable is transmitted by a mediator and that this mediated effect is conditional on the value of a moderator. In other words, moderated mediation is used to explain both how and when an effect occurs (Preacher et al., 2007). We applied standard testing procedures for this model structure, using OLS regressions combined with bootstrapping (e.g., Blohm, Riedl, Füller, & Leimeister, 2016; Cianci, Klein, & Seijts, 2010; Gardner, Gino, & Staats, 2012; Lee, Sambamurthy, Lim, & Wei, 2015). We mean-centered variables to facilitate interpretation and avoid collinearity issues (Aiken & West, 1991).

5.1 Direct Effects and Mediation Analysis

We first regressed misjudgment on stereotypical thinking and the control variables (Models 1a, 1b). Stereotypical thinking had a significant effect on misjudgment (β = .199, p < .001), confirming H1. Next, we regressed perceived privacy risk on misjudgment, stereotypical thinking, and the control variables (Models 2a-c). The coefficient of misjudgment was significant (β = .542, p < .001), confirming H2. Model 2c accounted for 34% of the variance in perceived risk. These regression results are shown in Table 5.

To test for mediation, we followed recommendations that existing tests (multistep approaches, Sobel's test) should be replaced with the bootstrapping procedure developed by Preacher and Hayes (2004), which has become feasible due to the increased processor speeds of today's computers. This method yields superior statistical power because it accounts for non-normal distributions of the product term (i.e., the indirect effect), which are usually skewed (e.g., Preacher & Hayes, 2004; Zhao, Lynch Jr, & Chen, 2010). Thus, to test the indirect effect of stereotypical thinking on perceived privacy risk through misjudgment (H3), we used the PROCESS tool for SPSS (Hayes, 2017). We ran the bootstrapping procedure for mediation models (i.e., Model 4) using 5,000 resamples. As the resulting 95% confidence interval did not contain zero, the indirect effect, which amounted to 0.10, was significant, confirming H3.

Table 4. Summary Statistics and Correlations

		M (*SD*)	Variables									
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	**Age**	36.16 (13.45)										
2	**Gender**	1.52 (.50)	.030									
3	**Android OS**	.75 (.43)	.018	.034								
4	**Internet use**	6.61 (.84)	.062	.089	-.035							
5	**Trust**	3.70 (.94)	-.107	.108	.102	.042						
6	**Stereotypical thinking**	7.32 (1.49)	.137*	.014	.056	-.006	-.256*					
7	**Misjudgment**	5.09 (1.10)	.346*	.021	.027	-.067	-.170*	.266*				
8	**Cognitive response**	3.33 (1.68)	-.024	.003	-.031	.090	.202*	-.152*	-.177*			
9	**Emotional response**	3.92 (1.51)	-.183*	.044	.010	.030	.259*	-.158*	-.386*	.443*		
10	**Basic response**	4.12 (1.68)	-.037	-.002	.045	-.051	-.059	-.044	-.172*	.111*	.292*	
11	**Privacy risk**	4.08 (1.41)	.258*	-.030	.004	-.063	-.136*	.157*	.572*	-.127*	-.394*	-.180*

Note: * significant correlation at 5% level or less.

5.2 Moderating Effects of Users' Responses to Privacy Statements

In this step, we analyzed the moderating role of users' responses to counter-stereotypic privacy statements with regard to the relationship between stereotypical thinking and misjudgment. To test our baseline hypothesis H4a, we regressed misjudgment on the control variables, stereotypical thinking, and individuals' basic response (Model 3). Next, to test the moderator hypotheses associated with increased argument strength (H4b-d), we regressed misjudgment on the control variables, stereotypical thinking as well as cognitive and emotional response respectively (Models 4 and 5a). Table 6 shows the results ofthis analysis.

The results do not support H4a and H4b but provide support for H4c and H4d. Only emotional response had a moderating effect on the link between stereotypical thinking and misjudgment ($\beta = -.109$, $p < .05$), while the other responses did not. Given that the direct effects for the basic and cognitive response on misjudgment were significant in Models 3 and 4, we included these direct links in the regression model for emotional response to see whether its moderating effect would remain stable. Model 5b in Table 6 shows that this was the case. The direct effects for the basic and cognitive response were insignificant in this model while the significant direct and moderating effect of emotional response remained significant. The interaction of stereotypical thinking and emotional response is plotted in Figure 3, which shows the relationships between stereotypical thinking and misjudgment at different levels of emotional response (mean, +/-1 *SD*). As can be seen, the effect of stereotypical thinking on misjudgment was stronger if users did not feel addressed on the emotional level. With stronger emotional responses, the effect of stereotypical thinking on misjudgment decreased.

Table 5. Regression Results for Direct Effects

Dependent variable	Misjudgment		Perceived privacy risk		
	Model 1a	Model 1b	Model 2a	Model 2b	Model 2c
Control variables					
Age	.335***	.313***	.252***	.241***	.071
Gender	.033	.025	-.020	-.024	-.037
Android OS	.031	.015	.009	.000	-.008
Internet use	-.083	-.083	-.072	-.072	-.027
Trust	-.137*	-.086	-.105	-.078	-.031
Independent variables					
Stereotypical thinking		.199***		.104	-.004
Misjudgment					.542***
R^2	.15	.18	.08	.09	.34
***F*-value for R^2 difference**	10.79***	13.90***	5.82***	3.43	113.15***

Notes: Values show standardized regression coefficients. * $p < .05$; ** $p < .01$; *** $p < .001$.

Table 6. Regression Results for Moderator Analysis

Dependent variable	Misjudgment			
	Model 3	Model 4	Model 5a	Model 5b
Control variables				
Age	.308***	.313***	.264***	.265***
Gender	.028	.024	.022	.022
Android OS	.023	.010	.016	.021
Internet use	-.091	-.073	-.068	-.072
Trust	-.099	-.063	-.017	-.030
Independent variables				
Stereotypical thinking (ST)	.190***	.191***	.176**	.173**
Basic response				
Basic response	-.165**			-.083
ST × Basic response	.015			
Cognitive response				
Cognitive response		-.121*		-.002
ST × Cognitive response		-.028		
Emotional response				
Emotional response			-.282***	-.254***
ST × Emotional response			-.109*	-.112*
R^2	.21	.20	.28	.28
***F*-value for R^2 difference**	10.31***	9.56***	14.94***	1.32

Notes: Values show standardized regression coefficients. * $p < .05$; ** $p < .01$; *** $p < .001$.

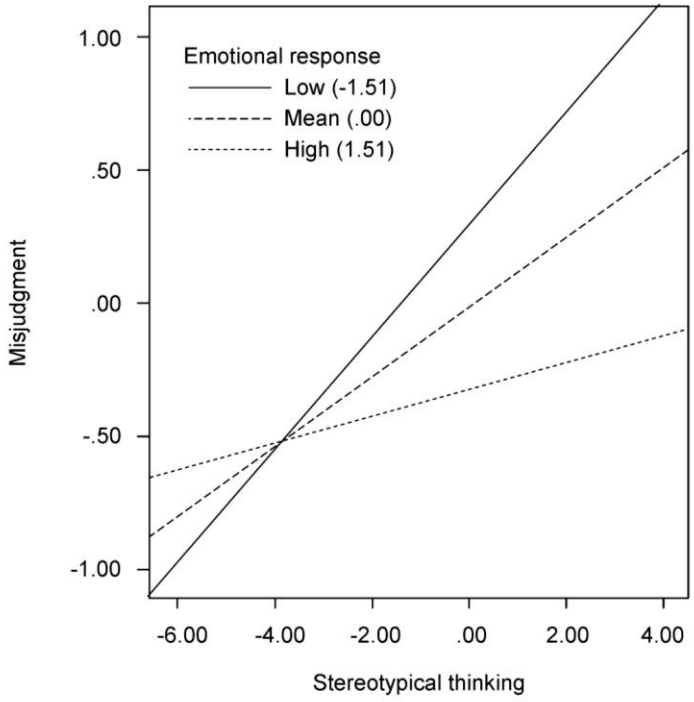

Figure 3. Plot of Interaction Effects

Table 7. Conditional Indirect Effects

Level of emotional response	Indirect effect	SE	LLCI	ULCI
10th percentile: -2.25	.17	.05	.08	.29
25th percentile: -0.92	.13	.04	.06	.20
50th percentile: 0.08	.09	.03	.03	.15
75th percentile: 1.08	.05	.03	-.01	.12
90th percentile: 1.75	.03	.04	-.06	.11

Notes: bootstrap sample size = 5,000; SE: standard error; LLCI & ULCI: lower and upper levels for confidence interval.

Due to the moderating role of emotional response, the final step in our analysis was to assess the overall indirect effect of stereotypical thinking on perceived privacy risk mediated by misjudgment at different levels of emotional response. This analysis provides insights regarding whether and when the detrimental consequences of stereotypical thinking can be entirely muted due to higher emotional responses to privacy statements. To test moderated mediation, we employed the bootstrapping procedure recommended by Preacher et al. (2007) and implemented as part of the PROCESS tool for SPSS (Hayes, 2017), assessing the indirect effect at different levels of the moderator (10th, 25th, 50th, 75th, and 90th percentiles). The results appear in Table 7. As can be seen, the indirect effect was significant for low levels of emotional response but its strength and significance decreased with increasing levels of emotional response. At the 75th percentile of emotional response, the confidence interval included zero, thus the indirect effect was no longer significant and almost completely muted. This indicates that stereotypical thinking will not influence privacy risk perceptions under the condition of a strong emotional response. Given the nonsignificant roles of the other two types of responses (i.e., basic and cognitive), these results partially support H5.

Table 8. Summary of Hypothesis Testing

Hypothesis	Result
H1: Stereotypical thinking → Misjudgment (+)	Support
H2: Misjudgment → Perceived privacy risk (+)	Support
H3: Stereotypical thinking → Misjudgment → Perceived privacy risk (+)	Support
H4a-c: (a) Basic, (b) Cognitive, (c) Emotional response moderates H1	Support for (c)
H4d: H4c's moderating effect is stronger than H4b's	Support
H5: Moderated mediation	Partial support

5.3 Summary of Results

Our results suggest that systematic errors in privacy-related judgments can present a problem for online services. These errors are made by users who apply their stereotypic beliefs to specific online providers in an overgeneralizing manner (H1). The resulting misjudgments lead to an inflation of privacy risk perceptions (H2) and, overall, stereotypical thinking exerts a significant indirect effect on users' perceived risk (H3). We hypothesized that users' responses to stereotype-deviating privacy statements would attenuate the effects of stereotypical thinking (H4a-d + H5). The moderating effect of users' emotional responses supported H4c and H4d and partially supported H5. Table 8 provides an overview of our results.

6 Discussion

The goal of this research was to examine whether Internet users' judgments of online services might be prone to systematic errors that are caused by stereotypical thinking (RQ1), and if so, how such systematic errors can be prevented by a presentation of counter-stereotypic privacy statements (RQ2). Data collected in two steps from a representative sample of smartphone users suggest that stereotypical thinking can indeed lead to systematic judgment errors when users are presented with a mobile app that deviates from their generalized beliefs. We also investigated whether highly accessible counter-stereotypic information can be an effective means of avoiding the detrimental outcomes of stereotypical thinking. According to our results, it can—but the success of such a communication effort depends on how the communication is received by users.

6.1 Research Implications

We believe our research is novel and important because it attempts to extend conceptions regarding the well-studied phenomenon of information privacy in new directions. Thereby, we contribute to extant research in several ways. First, we address the need for information privacy research to better understand how individuals' low-effort thinking and mental shortcuts might play a role when users form beliefs about online services (e.g., Acquisti & Grossklags, 2005; Dinev et al., 2015). In this regard, our study complements the few studies that investigate how information external to individuals is used as a mental shortcut to form their beliefs and attitudes (e.g., Bansal et al., 2015; Lowry et al., 2012; Pan & Zinkhan, 2006; Yang et al., 2006). Our study shows that category-based knowledge that is internal to individuals can serve as a heuristic belief-formation device as well. In particular, we have shown that individuals' judgments of the activities of a provider are prone to systematic errors associated with stereotypical thinking. This contributes to an increasingly important perspective, which does not regard users as systematic information processors who analyze all available information to arrive at a fully informed set of beliefs. Our results suggest that many smartphone users tend to generalize across providers of mobile apps—independently of whether these generalizations are appropriate. When presented with a provider that deviates from their stereotypic beliefs, users are prone to making misjudgments, despite the presence of stereotype-deviating information.

These findings offer a new perspective on the formation of individuals' privacy-related beliefs and can raise awareness regarding users' biases in this context. A central implication for research is that scholars who aim to investigate users' beliefs about the practices of a provider should be aware that such beliefs might not originate from information about the specific research context itself. Instead, users' beliefs about the service under study might be based on their stereotypic beliefs—even when service-specific information is presented that contrasts with the stereotype. Another related implication for research is that studies that include privacy risk perceptions, such as those adopting a privacy-calculus perspective, need to be conscious of the potential for overestimation of risk. Depending on how a particular research context is affected by stereotypic beliefs, participants' privacy risk perceptions may be inflated by systematic judgment errors, as shown in our study.

Prior research on the effects of privacy-related information (e.g., privacy policies, privacy seals) on individuals' beliefs, attitudes, and behaviors has paid only little attention to the possibility that users might take mental shortcuts and engage in heuristic information processing. Based on dual-process-theory and stereotype research, we have proposed a mechanism that takes into account how stereotypical thinking interacts with counter-stereotypic privacy information. In particular, we have focused on testing different versions of such information (in the form of highly accessible, stereotype-incongruent privacy statements) aimed at mitigating the deleterious effects of stereotypical thinking. In our representative sample of smartphone users, we found that communication that conveyed a feeling of empathy or concern presented the only effective tone for attenuating users' application of stereotypic beliefs to a privacy-friendly provider. This is in line with dual-process research suggesting that information that is incongruent with an evoked schema is more effective in activating more systematic processing by an individual (e.g., Goodstein, 1993; Maheswaran & Chaiken, 1991). In our context, empathic communication—i.e., expressing feelings of concern or care toward users—is less congruent with the stereotypic beliefs about a utility-maximizing company and thus should be effective in preventing stereotype application. This result finds additional support in studies that emphasize the benefits of empathy in companies' interactions with customers (e.g., Aggarwal, Castleberry, Shepherd, & Ridnour, 2005; Gerlach, Rödiger, Stock, & Zacharias, 2016; Homburg, Wieseke, & Bornemann, 2009). In contrast, users' stereotypic beliefs could not be overruled by reason-oriented statements (Schumann, von Wangenheim, & Groene, 2014) and pure counter-stereotypic information, which are more congruent with users' assumptions about profit-maximizing firms.

6.2 Practical Implications

Our findings have important implications for providers of Internet-based services and the market for digital services in general. In our study, we observed that many users apply stereotypic beliefs when they assess a new mobile app and might therefore arrive at erroneous conclusions about a provider's dealings with personal user information. This was the case even in the presence of contrasting information that did not include an additional emotional appeal. As a result, users might falsely assume that they will be targeted with personalized advertising, that their locations will be tracked, or that their personal information will be traded with third parties. These findings should be highly alarming for privacy-friendly providers who seek to differentiate themselves by offering privacy protection but suffer unnecessary rejections based on users' erroneous beliefs. From the users' perspective, stereotypical thinking can cause "false negatives": users might quickly reject useful services if they do not recognize that these services deviate from the stereotype in a positive way. As a result, privacy-friendly services may find it more difficult to survive—with the result that more privacy-intrusive services would have greater opportunities to further contribute to media reports regarding the privacy-intrusive practices of the majority of digital services.

Stereotype-deviating privacy statements that aim to attenuate the adverse consequences of stereotypical thinking produced mixed outcomes in our study. We found that the only communication mode that effectively influenced individuals' stereotyping was an emotional, empathy-based approach. Privacy-friendly companies offering mobile apps therefore should make it explicit that they care about users, and not only about their own profits. Specifically, they must communicate in a convincing manner that they understand and are addressing users' fears that their personal information might be mishandled. Our results show that if online companies succeed in doing this, they can effectively prevent Internet users from applying stereotypic beliefs to their specific services in an overgeneralizing manner.

Our study design placed short, privacy-related statements close to the default app description that is presented to users when installing a mobile app. This lowered the effort needed to assess the statement and would seem to be beneficial in light of evidence supporting the effectiveness of prominent and accessible privacy information (Tsai et al., 2011). For privacy-friendly providers, this implies that a brief privacy statement should be added to the app description itself to ensure that it is read even by those who do not usually expend the effort to look for and read lengthy privacy policies (e.g., Tsai et al., 2011).

6.3 Limitations and Future Work

Considering the theme underlying this research—that generalizations should be made with caution—we devote this final section to the limitations of our study. First and foremost, our results provide initial evidence for the presence of systematic errors in privacy-related judgments caused by stereotypical thinking. These findings could benefit from further validation—for instance, by using different samples or different methods (e.g., laboratory experiments). In addition, Dinev et al. (2015) suggest additional heuristics and mental shortcuts, which might operate in the context of privacy. Although the authors admit that these heuristics cannot be assessed in a single study, future research should continue to explore the role of heuristics in individuals' privacy-related beliefs, attitudes, and behaviors.

Furthermore, this study investigates how users' stereotypical thinking about how online providers

handle user information distorts individuals' perceptions of privacy risks. This is similar to studies in psychology investigating the relationship between mental shortcuts and belief distortions (e.g., Gabrielcik & Fazio, 1984; Hamilton & Gifford, 1976). Although extant research provides significant evidence for the important role of perceived privacy risks in shaping users' online behaviors, future studies could include the concept of stereotypical thinking in experimental research designs that study actual behavioral outcomes. Our study presents a significant first step that offers initial evidence that stereotypical thinking indeed has the potential to distort individuals' privacy-related beliefs and behaviors.

Although our study has explored conditions with respect to privacy statements under which stereotype application in a specific situation might be prevented, research on dual-process theories has specified additional factors that might determine whether individuals rely on mental-shortcuts such as stereotypes or enter a more elaborate information processing mode. For instance, prior research has shown that factors like an individual's mood, time constraints, time of day, and the need for cognition affect whether individuals enter a low-effort processing mode (e.g., Bodenhausen, 1990; Dinev et al., 2015). These factors might present boundaries to our findings and future research could explore their role in users' stereotypical thinking in the context of information privacy. We did not control for participants' motivation or capacity to engage in effortful information processing—two central determinants of individuals' mode of processing. Given that our participants comprised a sample of smartphone users that was representative for our country (Germany) in terms of age and gender and given that they were assigned randomly to the different privacy statements, potential variation in motivation and capacity should have been distributed equally across the groups. However, future studies could include individuals' motivation and capacity for information processing in their research models to test the influence of these factors.

We used the context of a real mobile news app to test our hypotheses. This choice of a real scenario reduced the degrees of freedom of our study. Using a hypothetical scenario would have allowed us to vary additional factors, such as the company's practices in terms of how it handles user information. Likewise, it is possible that online companies exist to which people do not apply the salient stereotypic beliefs of this study. Future research could use experimental setups to test the influence of additional factors such as different firm characteristics in this regard (e.g., country of origin, industry sector). Despite our belief that the mobile app case we used is similar to other mobile apps, we encourage future studies to apply the concept of stereotyping to a larger number of companies.

Finally, how and why the stereotype considered in our research develops was not part of our conceptual model. Rather, our model assumed that individuals hold this stereotype to a greater or lesser extent. An interesting avenue for future studies would be to explore the development of such stereotypes in different societies and the role of media reports in this regard. Privacy scandals such as Facebook's recent incident—in which the personal information of millions of users was acquired and used by Cambridge Analytica (see, e.g., Confessore, 2018)—could provide a natural environment to study the development of stereotypes in societies. Such future research could employ the stereotype measure developed in our study.

References

Aaker, J. L., & Williams, P. (1998). Empathy versus pride: The influence of emotional appeals across cultures. *Journal of Consumer Research*, *25*(3), 241-261.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26-33.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442-492.

Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of privacy: Framing, disclosures, and the limits of transparency. Paper presented at the *Proceedings of the Ninth Symposium on Usable Privacy and Security*.

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, *42*(2), 465-A465.

Adler, R. F., Iacobelli, F., & Gutstein, Y. (2016). Are you convinced? A Wizard of Oz study to test emotional vs. rational persuasion strategies in dialogues. *Computers in Human Behavior*, *57*, 75-81.

Aggarwal, P., Castleberry, S. B., Shepherd, C. D., & Ridnour, R. (2005). Salesperson empathy and listening: Impact on relationship outcomes. *Journal of Marketing Theory & Practice*, *13*(3), 16-31.

Aiken, L. S., & West, S. G. (1991). *Multiple regression: Testing and interpreting interactions*. Thousand Oaks, CA: SAGE.

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.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, *31*(5), 661-681.

Arnott, D. (2006). Cognitive biases and decision support systems development: A design science approach. *Information Systems Journal*, *16*(1), 55-78.

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.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, *24*(6), 624-644.

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*(3-4), 245-270.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM*, *48*(4), 101-106.

Berger, B., Matt, C., Steininger, D. M., & Hess, T. (2015). It is not just about competition with "free": Differences between content formats in consumer preferences and willingness to pay. *Journal of Management Information Systems*, *32*(3), 105-128.

Bilkey, W. J., & Nes, E. (1982). Country-of-origin effects on product evaluations. *Journal of International Business Studies*, *13*(1), 89-100.

Blair, I. V. (2002). The malleability of automatic stereotypes and prejudice. *Personality and Social Psychology Review*, *6*(3), 242-261.

Blohm, I., Riedl, C., Füller, J., & Leimeister, J. M. (2016). Rate or trade? Identifying winning ideas in open idea sourcing. *Information Systems Research*, *27*(1), 27-48.

Bodenhausen, G. V. (1990). Stereotypes as judgmental heuristics: Evidence of circadian variations in discrimination. *Psychological Science*, *1*(5), 319-322.

Bodenhausen, G. V., Sheppard, L. A., & Kramer, G. P. (1994). Negative affect and social judgment: The differential impact of anger and sadness. *European Journal of Social Psychology*, *24*(1), 45-62.

Bradley, T. (2013). Study finds most mobile apps put your security and privacy at risk. Retrieved from http://www.pcworld.com/article/2068824

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. *Information Systems Research*, *27*(4), 848-879.

Chaiken, S. (1977). *The use of source versus message cues in persuasion: An information processing analysis*. Amherst, MA: University of Massachusetts Press.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, *39*(5), 752-766.

Chaiken, S., Liberman, A., & Eagly, A. H. (1989). Heuristic and systematic information processing within and beyond the persuasion context. In J. S. Uleman & J. A. Bargh (Eds.), *Unintended thought* (Vol. 212, pp. 212-252). New York: NY: Guilford.

Chaiken, S., & Maheswaran, D. (1994). Heuristic processing can bias systematic processing: Effects of source credibility, argument ambiguity, and task importance on attitude judgment. *Journal of Personality and Social Psychology*, *66*(3), 460-473.

Chaudhuri, A., & Buck, R. (1995). Affect, reason, and persuasion advertising strategies that predict affective and analytic-cognitive responses. *Human Communication Research*, *21*(3), 422-441.

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social psychology* (pp. 73-96). New York, NY: Guilford.

Cianci, A. M., Klein, H. J., & Seijts, G. H. (2010). The effect of negative feedback on tension and subsequent performance: The main and interactive effects of goal content and conscientiousness. *Journal of Applied Psychology*, *95*(4), 618-630.

Confessore, N. (2018). Cambridge Analytica and Facebook: The scandal and the fallout so far. Retrieved from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*(3), 341-363.

Darke, P. R., & Ritchie, R. J. (2007). The defensive consumer: Advertising deception, defensive processing, and distrust. *Journal of Marketing Research*, *44*(1), 114-127.

Dasgupta, N. (2009). Mechanisms underlying the malleability of implicit prejudice and stereotypes. In T. D. Nelson (Ed.), *Handbook of prejudice, stereotyping, and discrimination* (pp. 267-284). New York, NY: Psychology.

Dasgupta, N., & Greenwald, A. G. (2001). On the malleability of automatic attitudes: Combating automatic prejudice with images of admired and disliked individuals. *Journal of Personality and Social Psychology*, *81*(5), 800-814.

Devine, P. G. (1989). Stereotypes and prejudice: Their automatic and controlled components. *Journal of Personality and Social Psychology*, *56*(1), 5-18.

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research*, *38*(2), 269-277.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce: A study of Italy and the United States. *European Journal of Information Systems*, *15*(4), 389-402.

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

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research*, *26*(4), 639-655.

Evans, J. S. B. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. *Annual Review of Psychology*, *59*, 255-278.

Fiske, S. T., Lin, M., & Neuberg, S. (1999). The continuum model. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social psychology* (pp. 231-254). New York, NY: Guilford.

Forgas, J. P. (1995). Mood and judgment: The affect infusion model (AIM). *Psychological Bulletin*, *117*(1), 39-66.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Foroni, F., & Mayr, U. (2005). The power of a story: New, automatic associations from a single

reading of a short scenario. *Psychonomic Bulletin & Review*, *12*(1), 139-144.

Fox, S., & Amichai-Hamburger, Y. (2001). The power of emotional appeals in promoting organizational change programs. *The Academy of Management Executive*, *15*(4), 84-94.

Gabrielcik, A., & Fazio, R. H. (1984). Priming and frequency estimation: A strict test of the availability heuristic. *Personality and Social Psychology Bulletin*, *10*(1), 85-89.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, *57*(7), 768-775.

Gardner, H. K., Gino, F., & Staats, B. R. (2012). Dynamically integrating knowledge in teams: Transforming resources into performance. *Academy of Management Journal*, *55*(4), 998-1022.

Gawronski, B., & Sritharan, R. (2010). Formation, change, and contextualization of mental associations. In B. Gawronski & B. K. Payne (Eds.), *Handbook of implicit social cognition: Measurement, theory, and applications* (pp. 216-240). New York, NY: Guilford.

George, J. F., Duffy, K., & Ahuja, M. (2000). Countering the anchoring and adjustment bias with decision support systems. *Decision Support Systems*, *29*(2), 195-206.

Gerlach, G. I., Rödiger, K., Stock, R. M., & Zacharias, N. A. (2016). Salespersons' empathy as a missing link in the customer orientation-loyalty chain: An investigation of drivers and age differences as a contingency. *Journal of Personal Selling & Sales Management*, *36*(3), 221-239.

Gerlach, J. P., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems*, *24*(1), 33-43.

Goldstein, E. B. (2005). *Cognitive psychology: Connecting mind, research and everyday experience*. Belmont, CA: Thomson Wadsworth.

Goodstein, R. C. (1993). Category-based applications and extensions in advertising: Motivating more extensive ad processing. *Journal of Consumer Research*, *20*(1), 87-99.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *30*(4), 395-410.

Greenwald, A. G., & Banaji, M. R. (1995). Implicit social cognition: Attitudes, self-esteem, and stereotypes. *Psychological Review*, *102*(1), 4-27.

Gruman, G. (2015). iOS still does app privacy better than android. Retrieved from http://www.infoworld.com/article/2993308/privacy/app-privacy-ios-vs-android.html

Hamilton, D. L., & Gifford, R. K. (1976). Illusory correlation in interpersonal perception: A cognitive basis of stereotypic judgments. *Journal of Experimental Social Psychology*, *12*(4), 392-407.

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13-42.

Haslam, S. A., Oakes, P. J., McGarty, C., Turner, J. C., Reynolds, K. J., & Eggins, R. A. (1996). Stereotyping and social influence: The mediation of stereotype applicability and sharedness by the views of in-group and out-group members. *British Journal of Social Psychology*, *35*(3), 369-397.

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford.

Homburg, C., Wieseke, J., & Bornemann, T. (2009). Implementing the marketing concept at the employee-customer interface: The role of customer need knowledge. *Journal of Marketing*, *73*(4), 64-81.

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems*, *48*(2), 407-418.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Im, G., & Rai, A. (2014). IT-enabled coordination for ambidextrous interorganizational relationships. *Information Systems Research*, *25*(1), 72-92.

Judd, C. M., & Park, B. (1993). Definition and assessment of accuracy in social stereotypes. *Psychological Review*, *100*(1), 109-128.

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *American Economic Review*, *93*(5), 1449-1475.

Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive thought* (pp. 49-81). New York, NY: Cambridge University Press.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization-privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369-400.

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, *26*(6), 688-715.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637-667.

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.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems*, *24*(4), 13-45.

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, D. J., Steinfield, C., & Lai, Y.-J. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems*, *44*(4), 1000-1015.

Kim, D. J., Yim, M.-S., Sugumaran, V., & Rao, H. R. (2016). Web assurance seal services, trust and consumers' concerns: An investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems*, *25*(3), 252-273.

Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application*, *4*(2), 63-82.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122-134.

Kovar, S. E., Burke, K. G., & Kovar, B. R. (2000). Consumer responses to the CPA webtrust™ assurance. *Journal of Information Systems*, *14*(1), 17-35.

Lai, C. K., Marini, M., Lehr, S. A., Cerruti, C., Shin, J.-E. L., Joy-Gaba, J. A., . . . Koleva, S. P. (2014). Reducing implicit racial preferences: I. A comparative investigation of 17 interventions. *Journal of Experimental Psychology: General*, *143*(4), 1765-1785.

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, *41*(1), 127-149.

Lee, O.-K., Sambamurthy, V., Lim, K. H., & Wei, K. K. (2015). How does IT ambidexterity impact organizational agility? *Information Systems Research*, *26*(2), 398-417.

Lee, S. M., Choi, J., & Lee, S.-G. (2004). The impact of a third-party assurance seal in customer purchasing intention. *Journal of Internet Commerce*, *3*(2), 33-51.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114-121.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163-200.

Lowry, P. B., Moody, G., Vance, A., Jensen, M., Jenkins, J., & Wells, T. (2012). Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers. *Journal of the American Society for Information Science and Technology*, *63*(4), 755-776.

Lowry, P. B., Vance, A., Moody, G., Beckman, B., & Read, A. (2008). Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce

web sites. *Journal of Management Information Systems*, *24*(4), 199-224.

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-A295.

Macrae, C. N., Milne, A. B., & Bodenhausen, G. V. (1994). Stereotypes as energy-saving devices: A peek inside the cognitive toolbox. *Journal of Personality and Social Psychology*, *66*(1), 37-47.

Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/

Maheswaran, D. (1994). Country of origin as a stereotype: Effects of consumer expertise and attribute strength on product evaluations. *Journal of Consumer Research*, *21*(2), 354-365.

Maheswaran, D., & Chaiken, S. (1991). Promoting systematic processing in low-motivation settings: Effect of incongruent information on processing and judgment. *Journal of Personality and Social Psychology*, *61*(1), 13-25.

Mai, B., Menon, N. M., & Sarkar, S. (2010). No free lunch: Price premium for privacy seal-bearing vendors. *Journal of Management Information Systems*, *27*(2), 189-212.

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.

Marcus, G. E. (2000). Emotions in politics. *Annual Review of Political Science*, *3*(1), 221-250.

Mathews, L. (2017). 70% of mobile apps share your data with third parties. Retrieved from https://www.forbes.com/sites/leemathews/2017/06/13/70-percent-of-mobile-apps-share-your-data-with-third-parties/#67bf00fd1569

Mauldin, E., & Arunachalam, V. (2002). An experimental examination of alternative forms of web assurance for business-to-consumer e-commerce. *Journal of Information Systems*, *16*(S1), 33-54.

McGarty, C., Yzerbyt, V. Y., & Spears, R. (2002). *Stereotypes as explanations: The formation of meaningful beliefs about social groups*. Cambridge, UK: Cambridge University Press.

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business. *Electronic Markets*, *14*(3), 252-266.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155-179.

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15-29.

Mitchell, J. P., Nosek, B. A., & Banaji, M. R. (2003). Contextual variations in implicit evaluation. *Journal of Experimental Psychology: General*, *132*(3), 455-469.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, *19*(1), 54-61.

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs*, *36*(1), 28-49.

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642-660.

Özpolat, K., Gao, G., Jank, W., & Viswanathan, S. (2013). Research note—The value of third-party assurance seals in online retailing: An empirical investigation. *Information Systems Research*, *24*(4), 1100-1111.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331-338.

Park, I., Bhatnagar, A., & Rao, H. R. (2010). Assurance seals, on-line customer satisfaction, and repurchase intention. *International Journal of Electronic Commerce*, *14*(3), 11-34.

Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, *26*(1), 37-65.

Pavlou, P. A., Huigang, L., & Yajiong, X. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105-136.

Pennington, R., Wilcox, H. D., & Grover, V. (2003). The role of system trust in business-to-consumer transactions. *Journal of Management Information Systems*, *20*(3), 197-226.

Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, *59*(4), 327-345.

Peterson, D., Meinert, D., Criswell, J., & Crossland, M. (2007). Consumer trust: Privacy policies and third-party seals. *Journal of Small Business and Enterprise Development*, *14*(4), 654-669.

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion *Advances in experimental social psychology* (Vol. 19, pp. 123-205). Amsterdam: Elsevier.

Petty, R. E., & Wegener, D. T. (1999). The elaboration likelihood model: Current status and controversies. In S. Chaiken & Y. Trope (Eds.), *Dual-process theories in social psychology* (pp. 41-72). New York, NY: Guilford.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539-569.

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior research methods, instruments, & computers*, *36*(4), 717-731.

Preacher, K. J., Rucker, D. D., & Hayes, A. F. (2007). Addressing moderated mediation hypotheses: Theory, methods, and prescriptions. *Multivariate Behavioral Research*, *42*(1), 185-227.

Priester, J. R., & Petty, R. E. (1995). Source attributions and persuasion: Perceived honesty as a determinant of message scrutiny. *Personality and Social Psychology Bulletin*, *21*(6), 637-654.

Ramachandran, V., & Gopal, A. (2010). Managers' judgments of performance in IT services outsourcing. *Journal of Management Information Systems*, *26*(4), 181-218.

Rosselli, F., Skelly, J. J., & Mackie, D. M. (1995). Processing rational and emotional messages: The cognitive and affective mediation of persuasion. *Journal of Experimental Social Psychology*, *31*(2), 163-190.

Rucker, D. D., & Petty, R. E. (2006). Increasing the effectiveness of communications to consumers: Recommendations based on elaboration likelihood and attitude certainty perspectives. *Journal of Public Policy & Marketing*, *25*(1), 39-52.

Sagar, H. A., & Schofield, J. W. (1980). Racial and behavioral cues in black and white children's perceptions of ambiguously aggressive acts. *Journal of Personality and Social Psychology*, *39*(4), 590-598.

Schmid Mast, M., Hall, J. A., & Roter, D. L. (2007). Disentangling physician sex and physician communication style: Their effects on patient satisfaction in a virtual medical visit. *Patient Education and Counseling*, *68*(1), 16-22.

Schneider, D. J. (2005). *The psychology of stereotyping*. New York, NY: Guilford.

Schumann, J. H., von Wangenheim, F., & Groene, N. (2014). Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing*, *78*(1), 59-75.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears: Understanding perceived risk. In R. C. Schwing & W. A. Albers (Eds.), *Societal risk assessment: How safe is safe enough* (pp. 181-216). New York, NY: Plenum.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 980-A927.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167-196.

Stangor, C. (2000). *Stereotypes and prejudice: Essential readings*. Philadelphia, PA: Psychology.

Stephan, W. G., Ageyev, V., Stephan, C. W., Abalakina, M., Stefanenko, T., & Coates-Shrider, L. (1993). Measuring stereotypes: A comparison of methods using Russian and American samples. *Social Psychology Quarterly*, *56*(1), 54-64.

Sujan, M. (1985). Consumer knowledge: Effects on evaluation strategies mediating consumer judgments. *Journal of Consumer Research*, *12*(1), 31-46.

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*(4), 1141-1164.

Taylor, S. E. (1982). The availability bias in social perception and interaction. In D. Kahneman, P. Slovic, & A. Tversky (Eds.), *Judgment under*

uncertainty: Heuristics and biases (pp. 190-200). Cambridge, UK: Cambridge University Press.

Trope, Y., & Thompson, E. P. (1997). Looking for truth in all the wrong places? Asymmetric search of individuating information about stereotyped group members. *Journal of Personality and Social Psychology*, *73*(2), 229-241.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, *5*(2), 207-232.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124-1131.

Vaas, L. (2016). How mobile apps leak user data that's supposedly off-limits. Retrieved from https://nakedsecurity.sophos.com/2016/02/29/how-mobile-apps-leak-user-data-thats-supposedly-off-limits/

Viscusi, W. K. (1991). Age variations in risk perceptions and smoking decisions. *The Review of Economics and Statistics*, *73*(4), 577-588.

Wegener, D. T., Clark, J. K., & Petty, R. E. (2006). Not all stereotyping is created equal: Differential consequences of thoughtful versus non-thoughtful stereotyping. *Journal of Personality and Social Psychology*, *90*(1), 42-59.

Wegener, D. T., & Petty, R. E. (1997). The flexible correction model: The role of naive theories of bias in bias correction *Advances in experimental social psychology* (Vol. 29, pp. 141-208). Amsterdam: Elsevier.

Xie, E., Teo, H.-H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters*, *17*(1), 61-74.

Xu, H., Crossler, R. E., & Bélanger, F. (2012). A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision Support Systems*, *54*(1), 424-433.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). 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. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135-173.

Yang, S. C., Hung, W. C., Sung, K., & Farn, C. K. (2006). Investigating initial trust toward e-tailers from the elaboration likelihood model perspective. *Psychology & Marketing*, *23*(5), 429-445.

Zarate, M. A., Garcia, B., Garza, A. A., & Hitlan, R. T. (2004). Cultural threat and perceived realistic group conflict as dual predictors of prejudice. *Journal of Experimental Social Psychology*, *40*(1), 99-105.

Zhao, X., Lynch Jr, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197-206.

Appendix A

Table A1. Overview of Studies on Privacy-Related Information

Study	Objective	Findings	Treatment of heuristics[a]
Karwatzki, Dytynko, Trenz, & Veit (2017)	Uncover how interactions among individuals' privacy valuation, transparency features, and personalization influence intentions to disclose information	No relationship between transparency information and disclosure intentions	No particular consideration
Kim, Yim, Sugumaran, & Rao (2016)	Find out how consumers in two cultures perceive the roles of trust in e-Channel and the effectiveness of assurance seals in alleviating the concerns about e-transactions and transaction intentions	Effectiveness of assurance seals increases transaction intentions and reduces concerns regarding e-commerce for US but not for South Korean students	No particular consideration
Bansal et al. (2015)	Examine how privacy assurance mechanisms influence trust from an ELM perspective	Several factors serve as peripheral cues that can increase an individual's trust toward a website; these effects are moderated by an individual's privacy concerns	ELM as theoretical foundation
Gerlach et al. (2015)	Investigate the relationship between privacy policies and users' willingness to disclose	Link between policies and disclosure is mediated by perceived privacy risk	No particular consideration
Keith et al. (2015)	Investigate the role of mobile self-efficacy in the context of mobile app trust and information disclosure	A relationship between structural assurance and trusting beliefs and a relationship between self-efficacy and risk information seeking but no effect of such information seeking on trusting beliefs exist	No particular consideration
Adjerid et al. (2013)	Illustrate how privacy notices' effects on disclosure behavior might be biased due to bounded rationality	The effects of privacy statements on individuals' behaviors are subject to bounded rationality	Bounded rationality of individuals can interfere with how privacy notices affect behavior
Özpolat, Gao, Jank, & Viswanathan (2013)	Examine the impact of assurance seals on online transactions	The presence of assurance seals increases the likelihood of purchase conversion at online retailers' websites	No particular consideration
Lowry et al. (2012)	Explore conditions under which privacy assurance is more or less effective from an ELM perspective	Several factors serve as peripheral cues on a website that increase an individual's perceived privacy assurance; the presence of privacy statements serves as such a cue while privacy seals only do so if individuals understand and associate privacy assurance with them	ELM as theoretical foundation
Xu, Teo, Tan, & Agarwal (2012)	Generate insights into the effects of different privacy assurance approaches on context-specific concerns for information privacy	Negative relationship between industry self-regulation and context-specific privacy concerns; positive relationship between industry self-regulation and perceived control; no interaction effect found for industry self-regulation and individual control on perceived control	No particular consideration
Tsai et al. (2011)	Determine whether a more prominent display of privacy information will cause consumers to incorporate privacy	Prominent privacy information affects purchasing behavior	Argue that privacy policy information remains invisible to customers who do

Table A1. Overview of Studies on Privacy-Related Information

	considerations into their online purchasing decisions		not read or understand these policies
Xu et al. (2011)	Explore the link between individual privacy perceptions and institutional privacy assurances	Effectiveness of privacy policies increase control and reduce risk; self-regulation increases control (except for finance websites) but does not reduce risk for any context	No particular consideration
Hu, Wu, Wu, & Zhang (2010)	Examine the effects of third-party web assurance seals on consumers' initial trust in online vendors	Find interaction effects when a seal represents more than one function (privacy and security and transaction integrity)	No particular consideration
Mai, Menon, & Sarkar (2010)	Investigate whether seal-bearing vendors in the B2C context charge a higher price than vendors that do not bear a privacy seal	Privacy seals are associated with higher prices by the vendors	No particular consideration
Park, Bhatnagar, & Rao (2010)	Explore how third-party assurance seals have an impact on online customer satisfaction and repeat-purchase intention	Seal presence affects both satisfaction and repurchase intention significantly; it also moderates the effect of service performance on the two outcome variables; a diminishing sensitivity effect for satisfaction depends on the presence of seals	No particular consideration
Xu et al. (2009)	Explore the role of information delivery mechanisms (pull and push) in the efficacy of three privacy intervention approaches (compensation, industry self-regulation, and government regulation) in influencing individual privacy decision making	Industry self-regulation has a significant negative effect on privacy risk perceptions	No particular consideration
Kim (2008)	Study the impact of culture on trust determinants in computer-mediated commerce transactions	Perceived importance of privacy seals is weakly but significantly associated with trust in South Korea but not in the US	No particular consideration
Kim, Steinfield, et al. (2008)	Explore whether an intervention to educate consumers about the security and privacy dangers of the web, as well as the role of assurance services, influence their perceptions about the relative security and privacy of e-commerce sites they visit	Both awareness and importance of assurance seals increase through an educational intervention	No particular consideration
Kim, Ferrin, & Rao (2008)	Investigate the role of trust and risk in purchasing decisions in an e-commerce context	Beliefs about privacy seals reduce risk perceptions but do not increase trust (as hypothesized)	No particular consideration
Arcand, Nantel, Arles-Dufour, & Vincent (2007)	Study the impact of reading a web site's privacy statement on the perceptions of control over privacy and trust in a cyber merchant	Clicking on a privacy policy has a significant negative effect on perceived control and trust in one study but not in the other; mere presence of a privacy policy increases perceived control but not trust	No particular consideration
Hann et al. (2007)	Investigate the effectiveness of different means to overcome privacy concerns	Privacy policies are valued by users	No particular consideration
Hui, Teo, & Lee (2007)	Find out whether consumers value privacy statements and privacy seals and, if so, whether these statements and seals affect consumer disclosure of personal information	Privacy statements affect information disclosure marginally, but privacy seals do not	No particular consideration
LaRose & Rifon (2007)	Examine the effects of explicit privacy warnings, a clear, conspicuous, and concise presentation of the benefits and	Presence of privacy seals affects disclosure intentions	No particular consideration

Table A1. Overview of Studies on Privacy-Related Information

	risks associated with database information practices stated in a website's privacy policy		
Pavlou et al. (2007)	Understand and prescribe how uncertainty can be mitigated in online exchange relationships	Website informativeness significantly reduces uncertainty	No particular consideration
Peterson, Meinert, Criswell, & Crossland (2007)	Compare the effectiveness of third-party seals with self-reported privacy policy statements with regard to the willingness of potential e-commerce customers to provide web sites with various types of personal information	Strength of privacy protection through a privacy policy as well as privacy seals have an impact on information disclosure	No particular consideration
Awad & Krishnan (2006)	Examine the relationship between information technology features, specifically information transparency features, and consumer willingness to share information for online personalization	Importance of privacy policy is positively related to importance of information transparency and negatively related to willingness to be profiled	No particular consideration
Metzger (2006)	Explore how characteristics of online vendors and consumers interact with website communications to affect consumer behavior online	Contrary to hypothesis: no effect of privacy assurance strength on disclosures	No particular consideration
Pan & Zinkhan (2006)	Explore the impact of privacy statements on individuals' trust in an e-tailer	Individuals tend to read more of a privacy policy when the statement is short and straightforward	State that humans have bounded rationality and therefore are limited in their capacity to process privacy policies
Xie, Teo, & Wan (2006)	Examine the effects of reputation, privacy notices, and rewards on online consumer behavior in volunteering two types of personal information on the Internet	Availability of a secure connection, a privacy statement, and a TRUSTe seal encourages disclosure behavior	No particular consideration
Yang et al. (2006)	Investigate initial website trust formation from an ELM perspective	Privacy seals affect individuals' trust formation through peripheral route processing when product involvement is low or trait anxiety is high.	ELM as theoretical foundation
Berendt, Günther, & Spiekermann (2005)	Investigate the gap between online shoppers' stated preferences and actual disclosure behaviors	The intrusiveness of a privacy policy does not have a statistically significant impact on individuals' disclosure behaviors	No particular consideration
Lee, Choi, & Lee (2004)	Investigate how assurance seals affect potential Internet shoppers' perceived trustworthiness toward Web retailers and perceived risks in the context of online purchasing; also, examine how potential Internet shoppers' perceived transaction risk would affect their intention to purchase from the website	Beliefs about privacy seals reduce risk perceptions and increase trustworthiness perceptions	No particular consideration
McKnight, Kacmar, & Choudhury (2004)	Investigate how trust-building occurs across the early stages of a consumer's web experience	No effects for privacy seals on trust were found	No particular consideration
Pennington et al. (2003)	Explore the role of system trust in B2C transactions	Contrary to hypothesis: no effect of privacy seals on trust	No particular consideration
Belanger, Hiller, & Smith (2002)	Investigate the role of privacy, security, and site attributes with respect to trustworthiness in e-commerce	Importance of privacy policy's contents and the existence of privacy	No particular consideration

Table A1. Overview of Studies on Privacy-Related Information

		seals is lower than importance of security features	
Kimery & McCord (2002)	Investigate relationship between third-party assurance seals, trust, and online purchasing intentions	Contrary to hypothesis: neither a significant effect of attention to seal on trust nor of notice of assurance seal on trust	No particular consideration
Mauldin & Arunachalam (2002)	Investigate the role of web assurance in B2C e-commerce	Contrary to hypothesis: no effect of assurance seals on purchase intent; they found that when product familiarity is low, assurance seals are positively associated with purchase intent	No particular consideration
Miyazaki & Krishnamurthy (2002)	Investigate the effectiveness of assurance seals in raising online firms' privacy standards to acceptable levels and influencing consumers' perceptions of these privacy practices	Privacy seals tend to have an effect on disclosure regarding some information items under the condition of low shopping risk	No particular consideration
Grazioli & Jarvenpaa (2000)	Explore whether experienced Internet consumers are able to detect Internet deceptions	Assurance mechanisms (consisting of different factors; one is an assurance seal) significantly decrease risk but perceived deception moderates this link	No particular consideration
Kovar et al. (2000)	Explore the influence of privacy assurance on individuals' online shopping from an ELM perspective	Noticing a privacy seal affects individuals' expectations and intentions to shop online	ELM as theoretical foundation
Miyazaki & Fernandez (2000)	Assess disclosures of online retailers and compare the prevalence of privacy- and security-related disclosures with a subset of risk perception and online purchase intention data from a consumer survey	Contrary to expectations, no significant correlation was found between privacy-related statements and risk perceptions but there was a significant correlation between privacy-related statements and purchase likelihoods in this category	No particular consideration

[a] No particular consideration means that the model or theory does not include a concept or mechanism that represents heuristic or less elaborate information processing or judgment formation.

Appendix B: Addressing Common Method Bias

We took several steps to address the issue of CMB (e.g., Podsakoff et al., 2012). First, we temporally separated the assessment of stereotypical thinking and the control variables from the assessment of the mediator and the dependent variable to avoid common method variance from cross-sectional data. Second, Podsakoff et al. (2012) elaborate on the conditions when CMB is more likely to be a problem. They argue that this is the case if participants are not able or not motivated to provide accurate responses. Thus, we kept both questionnaires short without including any questions that were not immediately relevant to this study. According to the survey company, each survey only took about five minutes on average. As part of their quality check, the survey company also confirmed that our questionnaires were pleasant and easy to answer. Our high completion rates indicated that answering our questions was not difficult for participants. Third, we measured stereotypical thinking and misjudgment on different scales, which avoids the influence of common scale properties. Fourth, even though our study should not have raised social desirability concerns, we assured respondents that the data would be analyzed anonymously and that there were no "right or wrong" answers. In addition, we asked respondents to answer spontaneously and honestly. For statistical remedies, we followed the marker variable approach recommended by Lindell and Whitney (2001). This approach requires a marker variable that is theoretically unrelated to the study variables to show low correlations with those variables. We assumed that the device used to fill out the survey (smartphone vs. computer), which was self-reported by the participants, would be theoretically unrelated to our study variables. We found no significant correlations among device type and the other variables, and the absolute correlation values were below 0.10. We also observed no significant differences between partial and zero-order correlations. In sum, while we cannot completely rule out the existence of common method variance within our data, these steps provided confidence that it should not be a significant concern in our study.

Appendix C

Table C1. Measurement Information

Construct items (time of measurement; quality of reflective measures)	Source; scale
Trust (t = 1; Cronbach's α = .76; CR = .76; AVE = .52):	Dinev and Hart (2006); 7-point Likert scale
Internet websites are safe environments in which to exchange information with others.	
Internet websites handle personal information submitted by users in a competent fashion.	
Internet websites are reliable environments in which to conduct business transactions.	
Stereotypical thinking (t = 1; not applicable): Please provide your honest and personal opinion: What percentage of all companies providing mobile smartphone apps…	Developed after existing stereotyping scales (e.g., Haslam et al., 1996; Stephan et al., 1993; Zarate et al., 2004); 10-point scale: 0-10%, 10-20%,... 90-100% *excluded from analysis during validation
…collect more user data than they actually need?	
…collect as much user data as they can?	
…try to collect information about their users that is as detailed as possible?	
…conduct increasingly extensive analyses of their users' data?	
…use the knowledge about their users for personalized advertising?	
…sell their collected user data to other companies?	
…share data about their users with other companies?	
…communicate little to nothing about how they handle their users' data?	
…do not clearly communicate how they handle their users' data?	
…provide information about their handling of user data only in their privacy policy?*	
Misjudgment of provider's activities (t = 2; not applicable): Please state how you would judge this app with respect to its provider's behavior.	Self-developed based on knowledge about the provider and Culnan (1993); 7-point Likert scale */**excluded from analysis during validation / as these practices were actually true
I think that the provider would collect information about my location.	
I think that I would have to register with my email address in order to use this app.	
I think that the provider would collect information about my reading habits.**	
I think that the provider would display advertising based on its knowledge about me.	
I think that the provider would offer me paid content based on my usage behavior.	
I think that the provider would try to deduce my hobbies based on my reading behavior.**	
I think that the provider would transfer my personal information to newspaper publishers.	
I think that the provider would resell my personal information.*	
I think that the provider would transfer my personal information to third parties.	
Perceived privacy risk (t = 2; Cronbach's α = .90; CR = .90; AVE = .68):	Xu et al. (2011); 7-point Likert scale
In general, it would be risky to give personal information to the provider of this app.	
There would be high potential for privacy loss associated with giving personal information to this app's provider.	
Personal information could be inappropriately used by this app's provider.	
Providing this app with my personal information would involve many unexpected problems.	
Cognitive response (t = 2; Cronbach's α = .94; CR = .94; AVE = .85):	Self-developed; 7-point Likert scale
The provider of this app provides a reasonable explanation of why its earnings do not depend on the sale of personal user information.	
The provider explains why its revenue does not depend on selling personal information.	
The provider plausibly elucidates why it is not financially reliant on selling personal user information.	
Construct items (time of measurement; quality of reflective measures)	**Source; scale**

Table C1. Measurement Information

Emotional response (t = 2; Cronbach's α = .91; CR = .91; AVE = .76):	
The provider of this app demonstrates empathy for the privacy of its users.	Self-developed; 7-point Likert scale
The provider conveys the feeling of caring about its users' interests with respect to privacy.	
The provider gives users the feeling that it understands their concerns regarding privacy.	
Basic response (t = 2; Cronbach's α = .93; CR = .93; AVE = .82):	
The provider states without further explanation that it will not sell any personal user information.	Self-developed; 7-point Likert scale
Without further explanation, the provider signals that it will not sell personal user information to third parties.	
The provider states without justification that it will not sell personal user information to third parties.	

Appendix D:

Table D1. Item Loadings

Construct	Items	1	2	3	4	5
Trust	TR_1	-.003	.108	-.115	.090	**.811**
	TR_2	-.053	.143	.041	.052	**.815**
	TR_3	-.105	-.025	-.027	.134	**.811**
Privacy risk	PR_1	**.815**	-.113	-.070	-.167	-.091
	PR_2	**.888**	-.077	-.017	-.122	-.052
	PR_3	**.863**	.041	-.133	-.127	-.012
	PR_4	**.858**	-.002	-.047	-.150	-.045
Cognitive response	CR_1	-.046	**.924**	.028	.180	.088
	CR_2	-.035	**.914**	.057	.189	.107
	CR_3	-.051	**.927**	.040	.204	.062
Emotional response	ER_1	-.219	.257	.164	**.839**	.101
	ER_2	-.236	.183	.102	**.850**	.109
	ER_3	-.153	.209	.151	**.856**	.144
Basic response	NR_1	-.070	.059	**.923**	.052	-.052
	NR_2	-.125	.035	**.923**	.152	-.051
	NR_3	-.048	.028	**.925**	.158	-.007

Note: Item loadings were obtained using principal component analysis with Varimax rotation.

About the Authors

Jin P. Gerlach is an assistant professor at Technische Universität Darmstadt, Germany, where he earned his PhD in information systems. Since then, he has conducted research in the fields of IS adoption and use, IS security and privacy, and data-driven service innovations. His work has appeared in journals such as *Journal of Strategic Information Systems, Information Systems Journal,* and *Journal of Product Innovation Management*.

Peter Buxmann is a full professor of information systems at Technische Universität Darmstadt, Germany. He holds a PhD in general management and information systems from Frankfurt University. His main research areas are the digitalization of business and society, methods and applications of artificial intelligence, entrepreneurship and the development of innovative business models, as well as the economics of cybersecurity and privacy. He has published in several journals, such as *Information Systems Research, Journal of Information Technology, Journal of Strategic Information Systems, European Journal of Information Systems, Information Systems Journal,* and *Journal of Product Innovation Management*.

Tamara Dinev is a full professor and chair of the Department of Information Technology and Operations Management (ITOM) and Dean's Research Fellow, College of Business, Florida Atlantic University, Boca Raton, Florida. She received her PhD in theoretical physics in 1997. Following several senior positions in information technology companies, her interests migrated to management information systems research and she joined the Florida Atlantic University ITOM faculty in 2000. Her research interests include information privacy, trust in online vendors, multicultural aspects of information technology usage, and information security. She has published in several journals, including *MIS Quarterly, Information Systems Research, Journal of the Association for Information Systems, European Journal of Information Systems, Journal of Strategic Information Systems, Communications of the ACM, International Journal of Electronic Commerce, Journal of Global Information Management, e-Service Journal*, and *Behaviour and Information Technology*. She has received numerous best paper awards and nominations at major information system conferences.