University of Groningen

Consumers’ privacy calculus

Beke, Frank T.; Eggers, Felix; Verhoef, Peter C.; Wieringa, Jaap E.

Published in:
International Journal of Research in Marketing

DOI:
10.1016/j.ijresmar.2021.05.005

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2022

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):
Beke, F. T., Eggers, F., Verhoef, P. C., & Wieringa, J. E. (2022). Consumers’ privacy calculus: The PRICAL index development and validation. *International Journal of Research in Marketing*, *39*(1), 20-41. https://doi.org/10.1016/j.ijresmar.2021.05.005

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license. More information can be found on the University of Groningen website: https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment.

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Download date: 20-11-2022

International Journal of Research in Marketing 39 (2022) 20–41

Contents lists available at ScienceDirect

International Journal of Research in Marketing

journal homepage: www.elsevier.com/locate/ijresmar

Full length article

Consumers' privacy calculus: The PRICAL index development and validation

Frank T. Beke [b], Felix Eggers [c,*], Peter C. Verhoef [a], Jaap E. Wieringa [a]

[a] Department of Marketing, Faculty Economics and Business, University of Groningen, Nettelbosje 2, 9747 AE Groningen, Netherlands
[b] De Nieuwe Zaak, Hanzeallee 28, 8017 KZ Zwolle, Netherlands
[c] Copenhagen Business School, Department of Marketing, Solbjerg Plads 3, Copenhagen 2000 Denmark

ARTICLE INFO

Article history:
First received on May 01, 2019 and was under review for 6½ months
Available online 6 June 2021

Area Editor: Venkatesh Shankar

Keywords:
Privacy
Privacy calculus
Information collection
Index development

ABSTRACT

Although collecting personal information about consumers is crucial for firms and marketers, understanding of when and why consumers accept or reject information collection remains limited. The authors conceptualize a privacy calculus that represents a consumer's trade–off of the valence and uncertainty of the consequences of the collection, storage, and use of personal information. For example, usage-based car insurance requires drivers to share data on their driving behavior in exchange for a discount (certain benefit) but at the risk of third parties intercepting location data for malicious use (uncertain disadvantage). Building on this conceptualization, the authors develop the privacy calculus (PRICAL) index. They empirically confirm the validity of the items (Study 1) and the index as a whole (Study 2). The PRICAL index is generally applicable and improves the explanation of behavioral intentions (Study 2) and actual behavior (Study 3), compared with currently used constructs (e.g., privacy concern, trust). Overall, the PRICAL index allows managers to understand consumers' acceptance of information collection regarding financial, performance, psychological, security, social, and time-related consequences, which the authors demonstrate using the top five most valuable digital brands (Study 4).

© 2021 Elsevier B.V. All rights reserved.

1. Introduction

Firms increasingly rely on collecting customer-specific personal information (Rust & Huang, 2014) to understand their markets. Recently, legislation, novel technologies, and the notion of corporate digital responsibility have prompted consumers to be more aware of and assert control over the collection of their information (Lobschat et al., 2021). Therefore, understanding consumers' acceptance of information collection has become imperative for firms. Neglecting privacy issues can have significant effects on firm value, as Martin, Borah, and Palmatier (2017) empirically show and recent issues surrounding Facebook data misuse have borne out. This heightened attention to privacy and data protection is present in the academic marketing literature, where privacy and, on a more general level, consumer protection are gaining increased attention (e.g. Bleier, Goldfarb, & Tucker, 2020; Goldfarb, Jin, & Sudhir, 2020; Rafieian & Yoganarasimhan, 2021).

Governments and regulators are also paying more attention to privacy. Although governments across the globe have developed or are developing legislation, a good deal of variation in privacy regulation remains; for example, the European Union and Canada have very strict privacy legislation, whereas the United States and Australia are less stringent (Verhoef,

* Corresponding author.
E-mail addresses: frank@denieuwezaak.nl (F.T. Beke), felix@preferencelab.com (F. Eggers), p.c.verhoef@rug.nl (P.C. Verhoef), j.e.wieringa@rug.nl (J.E. Wieringa).

https://doi.org/10.1016/j.ijresmar.2021.05.005
0167-8116/© 2021 Elsevier B.V. All rights reserved.

Kooge, & Walk, 2016). Within the European Union, the member states have developed Data Projection Directives, which have led to the EU General Data Protection Regulation (GDPR). The EU has two main objectives with GDPR: (1) to protect the data and strengthen privacy rights of EU citizens and (2) to give EU citizens control of their data. As consumers need to provide consent to have their personal information collected GDPR affects all firms and institutions working with data of EU citizens. In this context, privacy, data protection, and understanding when consumers are willing to share personal information have increased in importance for firms.

Although the interest in privacy has only recently surfaced in the marketing literature (e.g., Bleier et al., 2020), some earlier studies in other research fields address privacy and privacy concern, such as information systems, direct/interactive marketing, and public policy and marketing literature (e.g., Markos, Milne, & Peltier, 2017; Peltier, Milne, & Phelps, 2009; for an overview, see Beke, Eggers, & Verhoef, 2018). This research predominantly focuses on privacy concern to understand consumers' decisions (see Table 1 for widely used and validated privacy concern measures). However, although consumers have become increasingly concerned about data privacy, fueled by negative publicity about data breaches, they are also disclosing more information than ever before. One reason for the discrepancy between privacy concern (an attitude) and information disclosure (a behavior) is that existing measures used in literature, such as privacy concern, largely ignore the benefits consumers enjoy from information collection.[1] Moreover, these measures generally do not account for consumers' perceived probability of both positive and negative consequences occurring.

Although many studies have measured privacy concern, measures that incorporate positive and negative consequences of personal information collection are limited. To address this research gap, we follow privacy calculus theory (Li, 2012) and conceptualize consumers' privacy calculus, which involves a consumer's internal trade–off of the negative and positive consequences of the collection of personal information (Dinev & Hart, 2006). Several studies have empirically confirmed that consumers trade off positive and negative consequences of information collection but these studies rely on ad hoc developed measures that focus on a limited number of consequences (Bol et al., 2018; Kehr, Kowatsch, Wentzel, & Fleisch, 2015; Li, Sarathy, & Xu, 2010; Mothersbaugh, Foxx, Beatty, & Wang, 2012; Xu, Teo, Tan, & Agarwal, 2009), study the antecedents without measuring the privacy calculus (Schumann, Von Wangenheim, & Groene, 2014; Sutanto, Palme, Tan, & Phang, 2013), or focus on specific applications only such as location data (Gutierrez, O'Leary, Rana, Dwivedi, & Calle, 2019; Keith, Thompson, Hale, Lowry, & Greer, 2013; Xu et al., 2009). We extend these previous approaches by developing a privacy calculus index that aims to cover a broad range of carefully selected consequences, while accounting for the valence and uncertainty of these consequences, and therefore can be applied in many settings.

Drawing on prior literature and qualitative interviews, we identify which types of consequences should be taken into account from a consumer perspective. Building on this conceptualization, we develop and test our privacy calculus (PRICAL) index, which considers the valence and perceived (i.e., not objective) probability of the relevant consequences of information collection that may occur immediately or in the future. We validate the formative items empirically (Study 1) and confirm the nomological validity and (incremental) predictive validity of the PRICAL index, using both behavioral intentions (Study 2) and actual behavior (Study 3). Finally, we demonstrate how the PRICAL index can be used for diagnostic purposes and provide managerial implications using the five most valuable digital brands in 2019 according to Interbrand (2020) (Study 4).

The empirical results confirm that consumers' acceptance of information collection is driven by both positive and negative consequences; in other words, consumer behavior is consistent with the privacy calculus. The operationalization and measurement of these consequences is an important contribution to the existing literature on privacy concern. Moreover, we provide evidence that consumers take several types of consequences into account, ranging from tangible (e.g., monetary compensation) to less tangible (e.g., feelings). Importantly, by taking a broader perspective on information collection, and looking beyond the negative side, we show that the PRICAL index is superior in predicting consumer decisions to accept information-intensive services than existing measures of privacy concern or trust.

Our study provides an important contribution to the literature on privacy and the measurement of privacy concerns in the information systems literature (Smith, Dinev, & Xu, 2011), as well as to research in marketing and consumer research (e.g., Milne, Pettinico, Hajjat, & Markos, 2017; Mothersbaugh et al., 2012). First, we develop a new scale to measure consumers' privacy calculus. Second, we show that the frequently mentioned discrepancy between privacy concern and actual behavior—or the privacy paradox—occurs partially because of the use of limited measures for privacy concern. Our studies provide relevant insights to firms that collect consumer information, including governmental agencies, policy makers, and nonprofit organizations aiming to understand consumers' privacy and the benefits and costs of sharing personal information. We also contribute to the literature on scale development, as we add a seventh step in the scale development process (Churchill, 1979) by focusing on the managerial use of a scale in marketing. This usage could lead to a stronger diffusion of proposed measurement scales in practice, in which only a few of the many developed marketing scales are actually frequently used (e.g., SERVQUAL; Parasuraman, Zeithaml, & Berry, 1988; Roberts, Kayande, & Stremersch, 2014).

[1] We acknowledge that measures for online service quality (e.g., Parasuraman, Zeithaml, & Malhotra, 2005) do include security/privacy; however, we propose that explaining the acceptance of information collection warrants a measure specifically focused on information collection.

Table 1
Measures for privacy concern.

Construct (Measure)	*Author(s)*	*Dimensions*	*Positive or Negative*	*Uncertainty*	*Context*
Privacy concern (*Concern for Information Privacy*)	Smith et al. (1996)	Collection, unauthorized secondary use, improper access, errors	Concern (negative) about firms' general privacy practices	No	Offline
Privacy concern (*Internet Users' Information Privacy Concern*)	Malhotra et al. (2004)	Collection, control, awareness	Concern (negative) about firms' general privacy practices	No	Online
Privacy concern (*Perceived Privacy Concern*)	Dinev and Hart (2004)	Perceived ability to control, perceived vulnerability	Concern (negative) about firms' general privacy practices	No	Online
Privacy concern (*Internet Privacy Concern*)	Hong and Thong (2013)	Interaction management, information management, awareness	Concern (negative) about firms' general privacy practices	No	Online
Privacy calculus (*PRICAL*)	This research	Financial, performance, time, psychological, social, security	Costs (negative) and benefits (positive) of data-driven offering	Yes	Offline & Online

2. Conceptual model

Prior research explains consumers' propensity to reject or accept information collection in terms of their concern about informational privacy (e.g., Smith, Milberg, & Burke, 1996). However, more recently, consumers have begun to realize that collecting personal information allows firms to better fulfill consumer needs (e.g., via personalized products and services), thus actually benefiting them. Therefore, existing theory on privacy calculus theory poses that consumers internally trade off the positive and negative consequences of firms' collection of personal information (Dinev & Hart, 2006; Laufer & Wolfe, 1977). As the considered positive or negative consequences of information collection are uncertain and might differ between consumers, we argue that taking the valence of these consequences into account is important. Furthermore, in line with social exchange theory (Homans, 1958), these consequences can be both tangible and intangible (Acquisti, Taylor, & Wagman, 2016).

Importantly, even though a privacy calculus is considered the most suitable framework for studying the acceptance of information collection (Acquisti, Brandimarte, & Loewenstein, 2015), an extensive conceptualization of consumers' privacy calculus in the context of their relationships with firms is still missing. In the following sections, we conceptualize our privacy calculus and, building on this conceptualization, provide a definition of privacy calculus that guides our development of a scale to measure it.

2.1. Consequences of information collection

In our conceptualization of the privacy calculus scale, we build on risk theory. Prior work has shown that consumers consider various types of potential consequences or risks when acquiring a product or service from a firm (Bauer, 1960). Risk can be captured using five dimensions: performance, financial, psychological, social, and (physical) safety (Cunningham, 1967). A sixth dimension, time, was later added (Roselius, 1971). These six dimensions capture a large portion of the variance in the overall perceived risk of products and services, and they are conceptually and empirically distinct (Kaplan, Szybillo, & Jacoby, 1974; Murray & Schlacter, 1990; Stone & Grønhaug, 1993). In addition to the negative uncertain consequences (risks) of products and services, these dimensions can also capture positive uncertain consequences (rewards). Taking both positive and negative consequences (net return) into account explains consumers' preferences better (Peter & Ryan, 1976).

Consumers' acceptance of information collection can also be considered risk-taking behavior, with positive and negative consequences that can be immediate (e.g., monetary compensation for subscribing to a newsletter) or more distant in time and risky (e.g., better product recommendations, possible theft of the information) (Acquisti et al., 2016). While prior work has hinted that consumers consider different types of consequences when firms collect, store, and use information (e.g., Milne et al., 2017; Stewart, 2017; White, 2004), an exhaustive conceptualization of these consequences is missing. We take a broad perspective on privacy by suggesting that consumers' privacy calculus can be conceptualized using the same risk-taking dimensions: performance, time, financial, psychological, social, and security.[2] Together, these dimensions capture consumers' internal trade-off of the consequences of information collection. Table 2 shows the dimensions and their effects on willingness to share information, as well as potential negative (risks) and positive (rewards) consequences for consumers. We further elaborate on these dimensions in the following subsections.[3]

2.1.1. Performance risk

The collection of information results in several consequences that affect the performance, or quality, of products and services. This information enables firms to better understand the needs and preferences of individual consumers (Wedel &

[2] In an information setting, we deem the term "security" to be more appropriate than "(physical) safety".

[3] In Appendix 1, we define the dimensions in line with the general definition of the privacy calculus and provide prior literature that addresses consequences related to these dimensions.

Table 2
Dimensions of PRICAL and their effects on data sharing and positive and negative consequences for consumers.

Dimension	Effect of sharing information	Exemplary potential consequences for customers	
		Negative	Positive
Performance	Increased understanding of customers' needs and wants	Personalization that mainly benefits the firm	Consumer's preferences are better met by offerings
Time	Time required for interactions between the firm and customers may in- or decrease	Sharing and reviewing information takes time	Tailored offerings reduce search time; automated checkout procedures saves time
Financial	Insights based on information increases the firm's efficiency	Misuse of information, e.g. by charging higher prices based on income data	Firms may pass on savings to consumers via monetary incentives or lower prices
Psychological	Affects customers' feelings about the firm	Intrusiveness, customers feel that they lose control, or are being watched	Customers feel special
Social	Personal status with family and friends is affected	Embarrassing disclosures, customers are asked to explain why they share their data	Prerequisite for interacting with their social environment (e.g. in social media)
Security	Vulnerability of personal information is affected	Outsiders may intercept personal information	High level protection of personal data

Kannan, 2016) and accordingly tailor their products, services, and communications (Simonson, 2005). While this could benefit consumers, opportunistic firms could also personalize in a way that serves the interest of firms rather than consumers (Frow, Payne, Wilkinson, & Young, 2011).

2.1.2. Time risk

Allowing firms to collect, store, and use consumers' information might reduce or increase the time consumers need to invest to interact or transact with firms. When firms retain consumers' payment details or reuse information to "auto fill in" forms, consumers might save time (Ackerman, Cranor, & Reagle, 1999). Moreover, personalization reduces the amount of time consumers need to spend searching for suitable products or services (Xu, Luo, Carroll, & Rosson, 2011). However, allowing firms to collect information might also cost consumers more time—for example, the time spent providing the additional information in the first place and monitoring how firms store and use the information.

2.1.3. Financial risk

When firms collect, store, and use information, it could result in monetary gains or losses for consumers. Insights drawn from personal information could increase firms' efficiency, and firms might pass on part of the monetary savings to consumers in the form of lower prices (Smith, Gleim, Robinson, Kettinger, & Park, 2014). More directly, information collection can result in monetary savings for individual consumers via monetary incentives (Acquisti, John, & Loewenstein, 2013; Premazzi et al., 2010). In addition, firms might adjust their prices to individual consumers in beneficial or detrimental ways (Acquisti & Varian, 2005). Another potential financial consequence for consumers is the misuse of financial information—for example, unauthorized charges on a consumer's account (Hille, Walsh, & Cleveland, 2015).

2.1.4. Psychological risk

Firms' collection of consumer information affects how consumers feel about the firm, their privacy, and themselves. These psychological consequences are extremely important in the context of privacy (Acquisti et al., 2015). Although a personalized experience might give consumers the feeling that they are special to a firm (Hennig-Thurau, Gwinner, & Gremler, 2002), information collection can also make consumers feel uncomfortable. Consumers might feel firms know too much about them or that they could lose control over their information (Hong & Thong, 2013). Moreover, consumers could perceive the collection of detailed information as intrusive (Aguirre, Mahr, Grewal, de Ruyter, & Wetzels, 2015; Goldfarb & Tucker, 2011). Likewise, when firms monitor consumers' behavior on a daily basis consumers might feel they are being watched (Smith et al., 2014).

2.1.5. Social risk

The collection, storage, and use of information could affect consumers' interpersonal status or their relationships with friends and family. On the one hand, the collection of information could result in embarrassing disclosures (White, 2004), as several high–profile examples have made clear (e.g., Target inadvertently revealing a customer's pregnancy; Corrigan, Craciun, & Powell, 2014). In addition, since privacy has become a widely debated topic, it has been suggested that consumers might suffer from having to explain or justify to their friends and family why they allow firms to collect their information (e.g., the case of sharing data on Facebook to Cambridge Analytica; Goodwin, 1991). On the other hand, the collection and distribution of information is often a prerequisite for consumers to connect and interact with their social environment (e.g., using social media such as Instagram or instant messaging services such as WhatsApp; Jiang, Heng, & Choi, 2013).

2.1.6. Security risk

The collection and storage of information has little bearing on consumers' physical safety (an exception is when location data is used to harm someone physically); rather, the more salient potential consequences relate to the security of consumers' information. ''Security'' implies that consumers are protected from (unknown) outsiders intercepting or accessing information illegally—that is, without proper authorization (Belanger, Hiller, & Smith, 2002). These security-related consequences could affect consumers' decisions to share their information. As captured by measures for privacy concern, consumers might experience situations in which unknown outsiders have access to their personal information. More generally, when firms collect and store information, consumers become susceptible to issues related to flaws in the security of information systems (Hong & Thong, 2013; Smith et al., 1996). Therefore, given that information collection and storage results in consequences that affect the security of consumers' information, it might also affect the privacy calculus and thus acceptance of information collection.

2.2. Perceived probability

As outlined previously, information collection can lead to positive and negative consequences (i.e., effects that differ in valence). In addition, the consequences also differ in their certainty of affecting consumers—for example, because some consequences are more distant in time than others (Acquisti et al., 2015). Perceived risk theory (Bauer, 1960; Conchar, Zinkhan, Peters, & Olavarrieta, 2004) suggests that people take into account the perceived probability that an outcome or consequence will occur. Understanding consumers' privacy calculus therefore requires correcting for the probability of consequences as consumers perceive it; for example, they might consider a potential loss severe (i.e., negative valence) but also highly unlikely (i.e., low probability).

2.3. Definition of privacy calculus

Following our theoretical conceptualization, we define privacy calculus as *a consumer's perception of the valence and probability of performance, time, financial, psychological, social, and security consequences when a firm collects, stores, and uses consumer information related to the products and services they acquire from that firm*. This definition implies that consumers can rate the potential consequences of information collection on the basis of their perceived valence and probability and that each consequence belongs to one of the six dimensions.

3. Index development

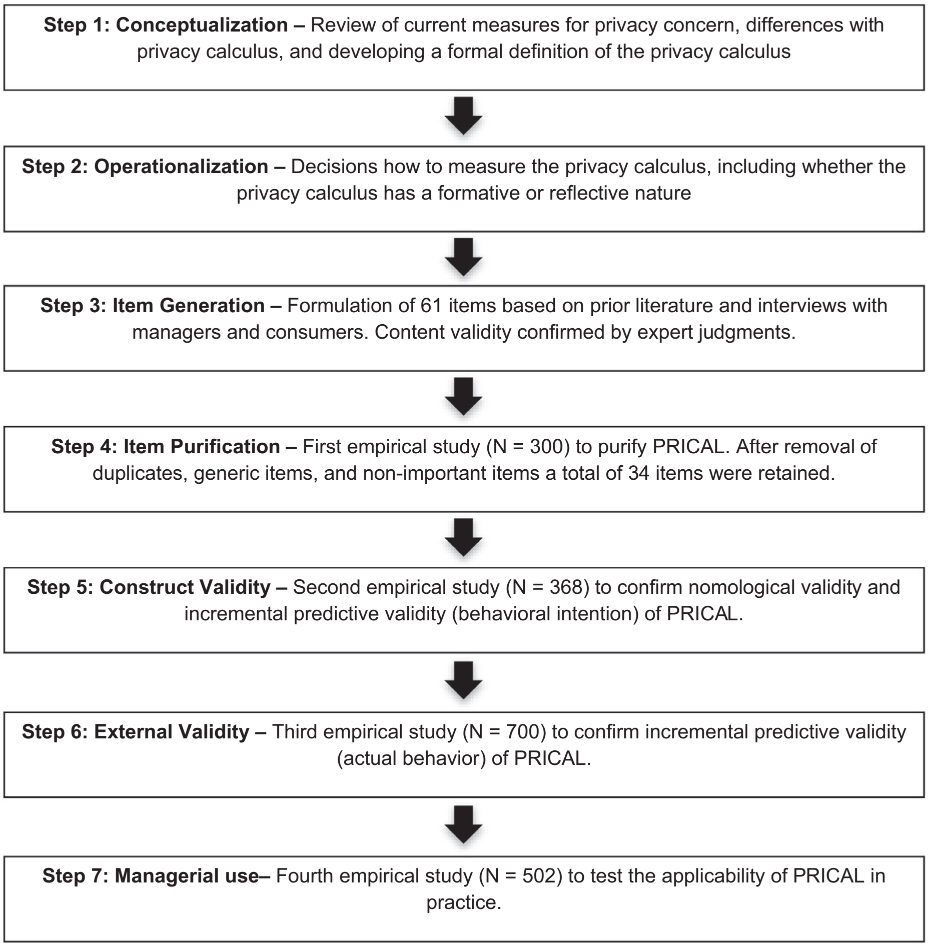
We followed the most prevalent guidelines in developing our PRICAL index (MacKenzie, Podsakoff, & Podsakoff, 2011; Rossiter, 2002) (see Fig. 1), except that we added a step that focuses on the managerial use of our measure in marketing. The marketing field has had an ongoing discussion on increasing the impact of marketing research on practice (e.g., Kohli & Haenlein, 2021; Roberts et al., 2014). By adding the step of testing the applicability of the developed scale in practice, our aim is to show how brands can use the PRICAL index for diagnostic purposes. Specifically, we demonstrate its usefulness in measuring the five most valuable global tech brands in terms of consumer privacy calculus (Interbrand, 2020). Fig. 1 summarizes our procedure.

3.1. Formative construct (Step 2)

The privacy calculus represents a consumer's mental calculation of the consequences of information collection. As shown in Fig. 2, the privacy calculus can be considered a formative–formative (latent) construct, which should be measured using an index or composite variable (Bagozzi, 2011; Hair, Hult, Ringle, Sarstedt, & Thiele, 2017). Each underlying consequence (item) captures a unique element within a particular dimension, and all consequences together cover the entire privacy calculus construct. We assume that the perceived consequences of information collection are unrelated to one another and do not have to occur simultaneously, in line with the formative nature of this calculus (Bagozzi, 2011; Jarvis, MacKenzie, & Podsakoff, 2003). For formative constructs, each item is an essential part of the overall construct (Bagozzi, 2011), such that the definition of the overarching construct and of each dimension determines which items should be included (Borsboom, Mellenbergh, & Van Heerden, 2004) and the formative nature affects how item validity should be assessed.

3.2. Item generation (Step 3)

After our theoretical conceptualization, we conducted a series of interviews with managers and consumers from various industries to get a better initial understanding of the dimensions (for details about the procedure, see Web Appendix 1). The managers we interviewed had varied backgrounds: some worked within the marketing or data department and therefore could provide insight into how collecting data created value for consumers, whereas others were active within the legal team and so provided perspective on the potential negative consequences. For the interviews, we used theoretical sampling; in other words, we conducted interviews until saturation was achieved, such that no new information emerged.



Step 1: Conceptualization – Review of current measures for privacy concern, differences with privacy calculus, and developing a formal definition of the privacy calculus

Step 2: Operationalization – Decisions how to measure the privacy calculus, including whether the privacy calculus has a formative or reflective nature

Step 3: Item Generation – Formulation of 61 items based on prior literature and interviews with managers and consumers. Content validity confirmed by expert judgments.

Step 4: Item Purification – First empirical study (N = 300) to purify PRICAL. After removal of duplicates, generic items, and non-important items a total of 34 items were retained.

Step 5: Construct Validity – Second empirical study (N = 368) to confirm nomological validity and incremental predictive validity (behavioral intention) of PRICAL.

Step 6: External Validity – Third empirical study (N = 700) to confirm incremental predictive validity (actual behavior) of PRICAL.

Step 7: Managerial use– Fourth empirical study (N = 502) to test the applicability of PRICAL in practice.

Fig. 1. Overview of scale development process.

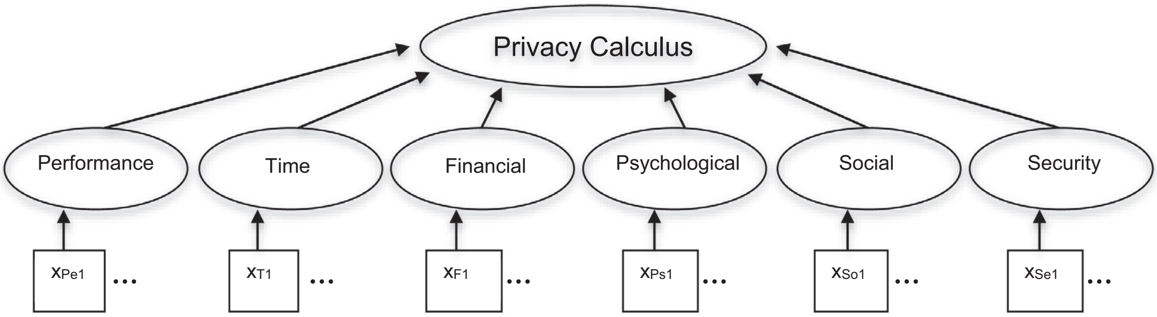


Fig. 2. Privacy calculus as formative-formative (latent) construct.

The interviews confirmed the existence of the distinguished six theoretical dimensions (for a detailed description of these dimensions, see Appendix 1). In addition, the interviews provided the basis for an initial list of consequences of information collection aimed at covering all dimensions. Importantly, while the dimensions we distinguished and definitions are based on prior research (Kaplan et al., 1974; Mitchell, 1999), the initial list of specific items is based on academic as well as practitioner-focused literature (PwC, 2012; Rose, Rehse, & Röber, 2012; World Economic Forum, 2014), as well as our qualitative interviews. Every item is intended to capture a unique consequence and considered part of the internal trade-off consumers make regarding firms' collection of personal information. Our scale allows consumers to determine whether consequences are positive or negative (e.g., some consumers might find personalization beneficial whereas others perceive it as intrusive); thus, we formulated all items to be as neutral as possible. After discussing whether the initial list included all relevant consequences with academic and industry experts, we removed, reformulated or merged several items to arrive at a provisional list of items (Diamantopoulos, 2005; Rossiter, 2002). As a next step, a group of academic experts with the methodological background to understand the conceptual definition of each dimension rated whether the items were representative of the dimension and, therefore, the construct as a whole (MacKenzie et al., 2011; Rossiter, 2002; Zaichkowsky, 1985). Each of the resulting 63 items belonged to one of the six dimensions. Two convenience samples ($N = 20$ and $N = 26$) confirmed the categorization of our items from a consumer's perspective and, after another round of refinements, served as an initial test of whether the items were clear and understandable (Hinkin, 1995). A copy editor further improved the formulation of the items.

3.3. Measurement

First, the scale measures perceived valence on a seven-point bipolar scale ranging from "very positive" (+3) to "very negative" (−3). Next, it measures whether consumers consider a consequence as likely to affect them on a unipolar scale for probability ranging from "very unlikely" (1) to "very likely" (7). Multiplying valence with probability for each consequence (Conchar et al., 2004; Peter & Tarpey, 1975) ensures that consequences deemed neutral or unlikely have little influence. Summing the probability-weighted scores for each consequence within a dimension provides a value for each dimension, and summing the probability–weighted scores for each consequence across dimensions provides the PRICAL index. While the PRICAL index can be used to predict whether consumers will accept or reject the collection of information or, more specifically, a data-driven product or service, another useful purpose of the scale is to diagnose companies' strengths and weaknesses. Managers can derive implications on how to improve data collection (e.g., by increasing the valence of a consequence, by increasing or decreasing the perceived probability of a consequence).

4. Item purification (step 4) —Study 1

With Study 1, we aimed to make the measurement tool more parsimonious by assessing the statistical validity of the items. First, we presented respondents with one of three industries (retailer, telecom operator, or bank) and asked them to indicate the firm with which they were currently transacting. Next, respondents read a scenario in which this specific firm asked permission to collect information necessary for a data-driven offering, such as a personalized service or an enhanced customer relationship management program. Given our goal of explaining consumers' acceptance of information collection, we use willingness to accept (WTA) that their information was collected as the main dependent variable. In the rest of the survey, we used the 61 items to measure the privacy calculus index by requesting the respondents to score the valence and the probability sequentially for each item. Respondents concluded the survey by answering items about their demographics and their use of online services in general.

Throughout the survey, we tried to provide respondents with realistic scenarios by presenting offerings from actual firms and using the name of a firm the respondents identified at the beginning of the survey. To reduce the potential impact of (common) method bias, we used several procedural remedies (MacKenzie & Podsakoff, 2012; Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). By first asking respondents to indicate their WTA and then having them evaluate the items, we minimized the influence of implicit theories and the need for consistency. Moreover, we presented all items in random groups of four on one page, such that the items were mixed across dimensions, to diversify the survey and minimize the risk that respondents would fill out the same response for all items in one category (MacKenzie & Podsakoff, 2012).

4.1. Data

We used a U.S. online panel to invite respondents to our survey (Amazon Mechanical Turk, $N = 300$). Our sample comprised slightly more men than women (56% vs. 44%) and had an average age of 37 years (SD = 11.48), and most respondents had completed at least some type of college education (82%). After confirming all respondents completed the entire survey, we checked our data for (common) method bias, given the repetitive nature of our measure. Harman's single-factor test (Podsakoff et al., 2003) indicated that (common) method bias was not an issue. Moreover, we confirmed that removing the fastest respondents and those with the least variance in their answers had little influence on our results. (We check for common method bias more extensively in Study 4 using the final PRICAL index.)

4.2. Item validity

We used partial least squares structural equation modeling (PLS-SEM) to assess item validity, which is favored over covariance-based SEM when formative items are included and when the aim is to predict or explain a target variable as accurately as possible (Hair et al., 2017; Reinartz, Haenlein, & Henseler, 2009). For our analyses, we used SmartPLS (Ringle, Wende, & Becker, 2015), which determines significance of coefficients, weights, and loadings based on a bootstrapping procedure. When we needed to accommodate a higher-order construct, we used a repeated indicator approach to obtain parameter estimates (Hair, Hult, Ringle, & Sarstedt, 2014).

We assessed item validity using two criteria. First, we assessed the variance inflation factor (VIF) to identify items that correlated highly with multiple other items and could therefore be excluded using a formative approach. To this end, we assessed content validity starting with the item with the highest VIF value (approximately 6), eventually working down to the lowest VIF value (approximately 1). Subsequently, we used the inter-item correlations to identify items that might be considered duplicates and those that might be considered overly generic (i.e., they represent the entire construct). Throughout this process of item purification, we only removed or changed items when it did not affect the conceptual domain of our construct (Bollen & Lennox, 1991; MacKenzie et al., 2011; Rossiter, 2002).

Second, we assessed the relative contribution of each item in explaining variance in the target dimension (i.e., WTA; Bollen & Lennox, 1991). Items with a low or insignificant relative contribution are potentially not an important part of the overall construct (Jarvis et al., 2003; MacKenzie et al., 2011). If an item had a low relative contribution (weight), we assessed the absolute contribution of that item (loading) (Cenfetelli & Bassellier, 2009), as an item with a low relative contribution could still relate to the overall construct. This way, we ensured that removing an item would not affect the conceptual domain. We used the adjusted R^2 as another indication of the importance of individual items, and thus for the inclusion or removal of items (Henseler, Ringle, & Sinkovics, 2009).

In addition to assessing these criteria across all respondents, we also examined them for each scenario separately, because some items might be more relevant in one scenario (i.e., have a higher weight) than in other scenarios. Given our objective of explaining the acceptance of information collection in various contexts, retaining these items is crucial to ensure content validity. Thus, we aimed to remove an item only when it was truly irrelevant in all scenarios.

4.3. Results

We conducted two rounds of item purification (Step 4 in Fig. 1), focusing first on removing duplicates and subsequently on removing items that contributed little to explaining WTA. For formative constructs, it is crucial to ensure that removing items does not compromise content validity (Bollen & Lennox, 1991; Rossiter, 2002). Throughout both rounds, we therefore ensured that removing or reformulating items did not affect the meaning of our construct.

The first round of item purification decreased the number of items from 61 to 43. In some cases, this process made clear that 2 or 3 items represented the same content, and in a few other cases, the items proved to be too generic, resulting in a high correlation with up to 14 other items. We also reformulated several items for which the inter–item correlations suggested they were either too similar within a dimension or too similar to items from another dimension. This similarity suggested they could be duplicates or were not a good representation of the dimension the item should represent.

In the second round, we focused on the relative contribution of each remaining item (indicator weights) and the extent to which each item related to the overall privacy calculus. We used these weights only as guidance; we retained some items despite their insignificant weights to ensure content validity. This resulted in further decreasing the number of items from 43 to 34.

Removing nearly half of the original items is warranted, as many of these items captured the same content. The fact that item purification only slightly decreased the adjusted R^2 (from 0.555 to 0.543) further confirms that the items we removed were less important in explaining the WTA information collection.

5. Construct validity (step 5)—study 2

After confirming item validity, we conducted a second study using an online research panel from the Netherlands to test the validity of the PRICAL index as a whole. As depicted in Fig. 3, we included other constructs that theoretically relate to the privacy calculus (nomological validity) and "rival" constructs that have been used previously to explain the acceptance of information collection (predictive validity) (Jarvis et al., 2003; MacKenzie et al., 2011).

Previous research that addresses antecedents of privacy suggests that multiple factors at the consumer level can influence privacy concern, classified into consumers' characteristics, personal circumstances, and experience of relationship with the firm (e.g., Beke et al., 2018). Building on this classification, we included personality traits as specific consumer characteristics (e.g., Bansal, Zahedi, & Gefen, 2010), privacy violation experiences and information sensitivity as specific consumer personal circumstances surrounding privacy and data (Malhotra et al., 2004), and behavioral loyalty to account for consumers' relationship with the firm (Dick & Basu, 1994). Next, we assessed the incremental predictive validity by comparing the PRICAL index with existing measures for privacy concern and trust.

5.1. Hypotheses on nomological validity

5.1.1. Personality

We expect the privacy calculus to be related to consumers' personality. In terms of the "big five" personality traits, agreeableness has been linked to lower privacy concern (Junglas, Johnson, & Spitzmüller, 2008) and a higher acceptance of new technologies (Devaraj, Easley, & Crant, 2008). Consumers rating high on agreeableness are less skeptical and more likely to agree (McCrae & Costa, 1987). Therefore, we also expect that agreeable consumers are less skeptical about information collection, which should result in a more positive privacy calculus.

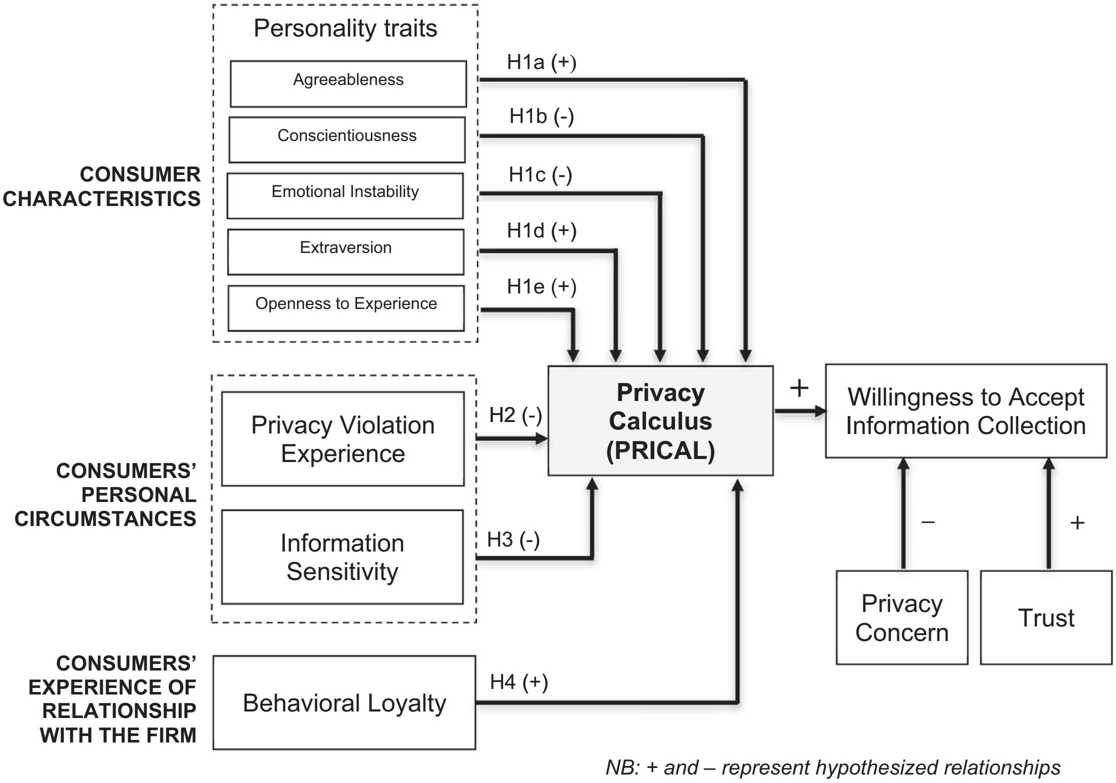


Fig. 3. Overview of nomological network.

H_{1a}. Agreeableness is positively related to the PRICAL index.

Conscientiousness represents the extent to which a person is self-disciplined and careful (McCrae & Costa, 1987). Conscientious consumers are generally more concerned about their privacy (Junglas et al., 2008) and see more risks with regard to privacy (Bansal et al., 2010). We expect consumers rating high on conscientiousness to be more vigilant and thus to consider negative consequences more likely to occur. As a result, consumers rating high on conscientiousness should have a more negative privacy calculus than consumers low on conscientiousness.

H_{1b}. Conscientiousness is negatively related to the PRICAL index.

Emotional instability, or neuroticism, refers to the extent to which consumers feel insecure and their ability to cope with stress (McCrae & Costa, 1987). Prior studies show that emotional instability is positively related to privacy-risk beliefs (Bansal et al., 2010) and privacy concern (Bansal, Zahedi, & Gefen, 2015) and negatively related to technology acceptance (Devaraj et al., 2008). We expect that emotionally unstable consumers are more anxious about information collection and therefore consider the potential negative consequences more likely to occur. Given that we also believe that these consumers are less secure about any potential positive consequences, we expect that emotional instability relates negatively to the privacy calculus.

H_{1c}. Emotional instability is negatively related to the PRICAL index.

Extraversion refers to a person's propensity to be talkative and outgoing (McCrae & Costa, 1987). Extraverted people are less concerned about exposing information to others, and studies show that extraversion relates negatively to privacy risk beliefs (Bansal et al., 2010). Extraverted consumers should be less tentative in sharing information about themselves because they consider information disclosure as not necessarily a negative consequence. Therefore, we expect extraversion to relate positively to the privacy calculus.

H_{1d}. Extraversion is positively related to the PRICAL index.

People who rate high on openness to experience tend to be more imaginative and daring (McCrae & Costa, 1987), regard innovation more positively (Marcati, Guido, & Peluso, 2008), and be more inclined to accept new technologies (Devaraj et al., 2008). These consumers should therefore also be more interested in the potentially positive consequences of information disclosure, suggesting that openness to experience relates positively to the privacy calculus.

H_{1e}. Openness to experience is positively related to the PRICAL index.

5.1.2. Privacy violation experience

We expect that, in addition to consumers' personality traits, consumers' prior experiences will be related to their privacy calculus. Consumers who have directly experienced (negative) outcomes of a behavior usually have a stronger (negative) attitude toward that behavior (Fazio, Powell, & Williams, 1989). Furthermore, in the context of privacy, consumers who have experienced a privacy violation, either directly or indirectly, are more concerned about their privacy (Malhotra, Kim, & Agarwal, 2004). We expect a similar learning effect with respect to the privacy calculus, in the sense that consumers who have experienced a privacy violation more (less) often have a more negative (positive) privacy calculus.

H_2. Privacy violation experience is negatively related to the PRICAL index.

5.1.3. Information sensitivity

Whether consumers are willing to share information or not depends on the sensitivity of the information (Acquisti, John, & Loewenstein, 2012). We define "information sensitivity" as the potential loss or risk for consumers when information is disclosed (Mothersbaugh et al., 2012). For example, consumers generally consider financial and medical information more sensitive than information about online behavior and habits (Phelps, Nowak, & Ferrell, 2000). Information sensitivity should make the potential negative consequences more negative, while also decreasing the appeal of the potential positive consequences. For example, whereas receiving personalized advertisements might be considered positive, consumers are likely to oppose personalization when it relates to "sensitive" information about them (White, 2004). Therefore, we expect that information sensitivity relates to the privacy calculus, in the sense that when firms want to collect sensitive information, consumers' privacy calculus is more negative.

H_3. Information sensitivity is negatively related to the PRICAL index.

5.1.4. Behavioral loyalty

When consumers have been affiliated with a particular firm for a long time (behavioral loyalty), they are generally confident that the firm acts in their best interests and thus will not harm them (Dick & Basu, 1994). Therefore, the perceived probability of negative consequences (risks) should be lower and the privacy calculus more positive. Moreover, as they are also more likely to expect the firm to provide them with beneficial products and services (Kim, Ferrin, & Rao, 2009), consumers will probably hold similar expectations for benefits related to information collection. Therefore, we expect that behavioral loyalty is positively related to the privacy calculus.

H_4. Behavioral loyalty is positively related to the PRICAL index.

5.2. Hypotheses on predictive validity

Researchers have most often explained acceptance of information collection using two alternative constructs. First, as previously stated, many studies use privacy concern to explain the acceptance of information collection. Privacy concerns reflect consumers' attitudes toward and concerns about the disclosure and processing of personal data (Malhotra et al., 2004). The most widely used measurement assesses consumers' concern about information practices based on four reflective dimensions (Smith et al., 1996). Given that these dimensions focus on information practices in general and measure privacy concern as a trait, we chose to adapt the items to measure privacy concern as a context-specific state and thus better represent the specific context of our study. Moreover, as a robustness check, we also include a more recent, abbreviated measure of privacy concern (Dinev & Hart, 2006).

The second way studies explain acceptance of information collection is trust (Bart, Shankar, Sultan, & Urban, 2005; Urban, Amyx, & Lorenzon, 2009). Trust is generally defined as the consumers' confidence in the firms' reliability and integrity (Morgan & Hunt, 1994, p.23). We include a multidimensional measurement for trust from the information systems literature (McKnight, Choudhury, & Kacmar, 2002), which captures trust according to three reflective dimensions (benevolence, integrity, and competence). We also include a more condensed measure of trust as robustness check (Mothersbaugh et al., 2012). To confirm incremental predictive validity, the privacy calculus should be more closely related to the acceptance of information collection than privacy concern and trust.

H_5. The PRICAL index explains more variance in the WTA information collection than (a) privacy concern and (b) trust.

5.3. Design

We presented respondents with a type of firm (telecom operator or insurance company[4]) in which a firm they transacted with asked permission to collect information necessary for a data-driven offering. Other than containing the additional constructs, the setup of the second study and the procedure to reduce the potential impact of (common) method bias were similar to Study 1; that is, after reading the scenario, the respondents first indicated their WTA before disclosing their perceptions.

5.4. Data

We recruited a Dutch sample representative of the Dutch population in terms of gender, age, and education. After confirming all respondents completed the entire survey, we checked our data for outliers and (common) method bias. We removed 32 respondents that could be considered "straight–liners"—that is, respondents whose variance in answers was below 0.5. We used the remaining sample ($N = 368$) to assess nomological and predictive validity.

5.5. Results

Following the confirmation of the validity of the other multi-item measurements (i.e., privacy concern and trust), we used SmartPLS (Ringle et al., 2015) to reconfirm the validity of items of the PRICAL index. Thereafter, we confirmed discriminant validity of the PRICAL index by comparing the item correlations within the privacy calculus with the item correlations for constructs other than the privacy calculus (Klein & Rai, 2009). In addition, bivariate correlations confirmed that the privacy calculus is related, but not identical, to privacy concern ($\rho = -0.372$) and trust ($\rho = 0.476$) (MacKenzie et al., 2011). In line with recent guidelines with regard to formative constructs (Nunnally & Bernstein, 1994), we used correlations based on summated scores to assess nomological and predictive validity. We assessed nomological and predictive validity using PLS-SEM by applying a two-step approach, in which we first calculated the latent variable scores, which we then used to test our nomological network (Hair et al., 2014).

5.5.1. Nomological validity

As Table 3 shows, the bivariate correlations and coefficients from PLS-SEM are in line with most of our hypotheses. The results are consistent across scenarios, and the coefficients are robust to changes in the nomological network.

The relationship between consumers' personality and their privacy calculus is for the most part consistent with our expectations. Consumers rating high on agreeableness have a more positive privacy calculus ($\beta = 0.139$, $p = 0.023$). When consumers score high on conscientiousness, their privacy calculus becomes more negative ($\beta = -0.154$, $p = 0.016$). Extraversion is positively related to the privacy calculus ($\beta = 0.207$, $p < 0.001$). Emotional instability ($\beta = 0.044$, $p = 0.443$) and openness to experience ($\beta = -0.011$, $p = 0.858$) are not significantly related to the privacy calculus, despite showing correct parameter signs. We thus find support for H_{1a}, H_{1b}, and H_{1d}.

Our data show that having directly experienced more privacy violations is unrelated to the privacy calculus ($\beta = 0.018$, $p = 0.752$). We also measured the occurrence of an indirect privacy violations (e.g., someone has heard of a case) and found that the number of indirect privacy violations is negatively related to the privacy calculus and marginally significant ($\beta = -0.117$, $p = 0.052$), providing partial support for H_2. In line with our expectations, the privacy calculus is more negative when consumers consider the information firms collect as sensitive ($\beta = -0.367$, $p < 0.001$), in support of $H_{3.}$

Or results show that the privacy calculus is not significantly related to behavioral loyalty (i.e., the number of years a customer is loyal to a firm; $\beta = -0.002$, $p = 0.965$), which does not support H_4. Apparently, being a customer for a long time does not necessarily imply that the customer expects positive or less negative consequences.

In summary, although three constructs (emotional instability, openness to new experience, and behavioral loyalty) were unrelated to the privacy calculus, we confirm the majority of the hypotheses of our nomological network. Therefore, we conclude that our privacy calculus has good nomological validity.

5.5.2. Predictive validity

Table 4 indicates that the privacy calculus is more consistently related to consumers' WTA than privacy concern or trust (Nunnally & Bernstein, 1994). The bivariate correlation of the summated scores for the privacy calculus and WTA is significantly larger than the correlation between WTA and privacy concern ($Z = 4.33$, $p < 0.001$) or trust ($Z = 4.68$, $p < 0.001$). Likewise, the privacy calculus explains more variance (36.7%) than privacy concern (7.4%) and trust (12.2%) when regressing WTA on each construct with control variables.

While these results are based on a summated approach, which assumes equal importance of all items and dimensions, Table 4 also shows that when the impact of every individual item is weighted using PLS–SEM (Henseler et al., 2014), the explanatory power of the privacy calculus increases further relative to privacy concern and trust. These results also hold when using alternative measures for privacy concern (Dinev & Hart, 2006) or trust (Mothersbaugh et al., 2012) and are

[4] We also included one social media scenario that was based on actual use rather than intentions. Because all respondents used social media (i.e., shared information with social media platforms), we observed no variation in accepting the information collection. We therefore discarded this scenario from the analysis.

Table 3
Nomological validity.

Hypothesis	*Correlation* ρ	*PLS-SEM Coefficient* β	*Supported?*
$H_{1a:}$ Agreeableness → PRICAL (+)	0.148**	0.139*	Yes
H_{1b}: Conscientiousness → PRICAL (−)	−0.122**	−0.154*	Yes
H_{1c}: Emotional Instability → PRICAL (−)	−0.082 ^{ns}	−0.044 ^{ns}	No
$H_{1d:}$ Extraversion → PRICAL (+)	0.253**	0.207**	Yes
H_{1e}: Openness to experience → PRICAL (+)	0.133**	−0.011 ^{ns}	No
H_2: Privacy violation experience → PRICAL (−)			Partly
- Direct	−0.091 ^{ns}	0.018 ^{ns}	
- Indirect	−0.168**	−0.117^{+}	
H_3: Information sensitivity → PRICAL (−)	−0.367**	−0.367**	Yes
H_4: Behavioral loyalty → PRICAL (+)	0.005 ^{ns}	−0.002 ^{ns}	No

** $p < 0.01$.
* $p < 0.05$.
$^{+}$ $p < 0.10$.

Table 4
Predictive validity.

Willingness to Accept	*Correlation*ρ	*OLS Adj.*R^2	*PLS-SEM Adj.*R^2
PRICAL (Our study)	0.603*	0.367	0.378
Privacy concern (Smith et al., 1996)	−0.359*	0.074	0.006
Trust (McKnight et al., 2002)	0.336*	0.122	0.003

* $p < 0.01$.

not driven by the choice of measurement model (formative vs. reflective) (Klein & Rai, 2009). Therefore, we accept H_5 and confirm that the privacy calculus explains more variance in the WTA information collection than privacy concern and trust.

6. External validity (step 6) —study 3

The privacy paradox may refer to not only the aforementioned discrepancy between attitudes (privacy concern) and behavior, but also a discrepancy between behavioral intentions and actual behavior with regard to privacy (Norberg, Horne, & Horne, 2007). To confirm predictive validity based on actual behavior, we linked the privacy calculus to an actual decision regarding the acceptance of information collection. We cooperated with a Dutch insurance company that planned to introduce a new type of car insurance based on collecting information about consumers' driving behavior (usage-based insurance). Before the car insurance was rolled out to the public, we performed a pilot study on a sample of current customers in which we were able to distinguish between customers where were willing to adopt the usage-based insurance and a segment who rejected this data collection. These two segments were invited to fill out a survey containing the PRICAL index and several other constructs. The setup of the survey was similar to Study 1.

6.1. Data

In total, 699 current customers indicated they would be willing to switch to usage-based insurance, and 616 of them completed our survey. Of the customers who refused to switch, 225 were initially willing to fill out the survey, and 84 respondents completed the entire survey. Thus, in total our sample consisted of 700 respondents (616 accepters and 84 nonaccepters).

Before assessing the extent to which the PRICAL index could explain the acceptance of information collection, we used a standard Heckman (1979) two–step approach to assess whether opening the email containing the invitation would result in a sample selection bias. The inverse Mills' ratio was not significantly related to the acceptance of information collection.

6.2. Results

We used the PRICAL index to assess how well it predicts the acceptance of information collection (as well as its rival constructs). To this end, we actually study the adoption of the usage-based insurance, which we use as a proxy for WTA. The mean values for the privacy calculus were consistent with the acceptance of information collection; that is, the PRICAL index for accepters was on average positive (μ = 57.68, SD = 95.354), whereas it was on average negative for nonaccepters (μ = −132.08, SD = 130.980). Consistently, the majority of the accepters had a positive privacy calculus (458 of 616, 74%), whereas the majority of nonaccepters had a negative privacy calculus (74 of 84, 88%).

We used a binary logistic regression model to confirm incremental predictive validity (Table 5). In addition to a model with only control variables (model 1), we compared the incremental predictive validity of trust (model 2), privacy concern

Table 5
Acceptance of information collection (binary logit).

Predictor	*Model 1* *β*	*Model 2* *β*	*Model 3* *β*	*Model 4* *β*	*Model 5* *β*
Constant	0.322	−0.843	5.791	4.641	4.134
Trust	–	0.532^{**}	–	0.339^{**}	–
Privacy Concern	–	–	-1.080^{**}	-0.980^{**}	–
Privacy Calculus	–	–	–	–	0.019^{**}
Controls					
Innovativeness	0.275^{**}	0.266^{**}	0.363^{**}	0.356^{**}	0.365^{**}
Involvement	0.226	0.051	0.248^{+}	0.142	−0.116
Number of Products	0.026	−0.005	−0.046	−0.069	−0.083
Years customer	−0.006	−0.005	0.003	0.007	0.035
Age	-0.019^{+}	-0.027^{*}	-0.029^{*}	-0.037^{**}	-0.059^{**}
−2LL	470.148	437.190	364.599	354.890	275.145
AIC	482.148	451.190	378.599	370.890	289.145
Nagelkerke-R^2	0.071	0.160	0.341	0.363	0.538

Results based on all respondents that could be matched with customers from the firm's database (*N* = 662).
** $p < 0.01$.
* $p < 0.05$.
$^{+}$ $p < 0.10$.

(model 3), trust and privacy concern (model 4), and the privacy calculus (model 5). The results show that all three constructs are significantly related to the acceptance of information collection. In terms of model fit (−2 log-likelihood, Akaike information criterion, and Nagelkerke R^2), the privacy calculus is best at explaining the acceptance of information collection. The within-sample classification shows that only the privacy calculus is able to correctly classify nonaccepters as such, as both trust and privacy concern classified all respondents as accepters according to these models.[5]

7. Managerial diagnostics (step 7) —study 4

Whereas the previous studies' objective was to develop the PRICAL index and assess its validity, Study 4 focuses on the managerial use of the index and how it can be used for diagnostic purposes, focusing on the most valuable digital brands. Study 4 also assesses common method bias more extensively.

7.1. Data and procedure

We recruited 502 consumers representative of the United States in terms of gender, age, and ethnicity using Prolific (Peer, Brandimarte, Samat, & Acquisti, 2017). At the beginning of the questionnaire, we presented the five most valuable US technology brands in 2019 according to Interbrand (2020; we did not consider IBM and Intel, as these firms focus primarily on business customers). We chose to test our scale using technology brands because of their importance in today's digital society (Verhoef & Bijmolt, 2019) and the fact that customer data are of essential importance for these brands (Wedel & Kannan, 2016; Wieringa et al., 2021). We asked respondents to indicate which of the presented companies' products or services they had used within the past 12 months. We then randomly selected from those brands and adjusted the remaining survey items to the selected brand. The brands (and number of respondents allocated to the brand) were as follows: Apple (100), Google (98), Amazon (101), Microsoft (102), and Facebook (101). The five subsamples' demographics differ significantly only in gender (*p* = 0.001): while the proportions of female to male customers are balanced for Apple, Google, and Amazon, Microsoft is used more by male customers (61.3%) and Facebook more by women (67%). We consider these as structural differences in the firms' target groups.

In the survey, we asked respondents how willing they were to disclose 17 pieces of data related to basic information (e.g., name, gender, email address), behavioral information (e.g., media habits, shopping behavior), financial information (e.g., income, credit card information), and health information (health data, medical history). We followed Gupta, Iyer, and Weisskirch (2009) to develop a formative dependent variable related to willingness to share information (WTS; see Appendix 2 for details). The scale ranged from 1 ("not at all willing to disclose") to 7 ("gladly willing to disclose"). Next, we presented unrelated marker variables (Lindell & Whitney, 2001; Williams, Hartman, & Cavazotte, 2010) that are theoretically unrelated to the other variables of the study (i.e., environmental consciousness and health consciousness; Baumgartner & Steenkamp, 2001). We measured each of these items on seven-point scales ("strongly disagree" to "strongly agree"). Finally, we included all items related to PRICAL. Respondents required a median (mean) time to finish the survey of 8.7 minutes (9.9 minutes).

[5] We also estimated models in which we included PRICAL, privacy concern, and trust simultaneously as predictors. Although the Nagelkerke R^2 slightly increases, the additional explanatory power of adding these other measures is limited, further confirming that PRICAL is the strongest measure for explaining WTA.

7.2. Results

7.2.1. Common method bias

Before comparing the brands in terms of WTS and the PRICAL index, we evaluated common method bias. Specifically, the Harman single-factor test shows that a single unrotated factor accounts for only 21.2% of the variance in the data, indicating that method bias is not an issue. Podsakoff et al. (2003) caution that a Harman single-factor test is not sufficient; therefore, we also calculated VIF. As we used formative scales in this study, we performed a full collinearity test in PLS and found a maximum inner factor level VIF of 2.805 (of PSYCH on TIME). This score stays under 3.3 and therefore does not indicate common method bias (Kock, 2015). Finally, we included the marker variable in the PLS model and checked partial correlations with the latent variables. We obtain a maximum correlation of 0.103 (between the marker and PSYCH), which is below 0.3, further suggesting that the model is free of method bias (Lindell & Whitney, 2001). Differences in parameter estimates when including versus excluding the marker variable are negligible (mean absolute deviation of 0.007 with an average effect magnitude of 0.140).

7.2.2. Brand diagnostics[6]

Overall, we observed a strong and significant correlation between WTS and the PRICAL index (r = 0.550, $p < 0.001$; for a full correlation matrix, see Web Appendix 2). Table 6 shows descriptive statistics of WTS, the PRICAL score, and the scores on each privacy dimension. We scale WTS in this study as a sum across the 17 items. The mean WTS is 57.9, which corresponds to an average of 3.4 on a 7-point scale. On average, consumers are most likely to share their gender (average rating 5.4) and least likely to provide financial information (average rating 2.0). Regarding the PRICAL index, we see that, on average, consequences relating to security or psychological consequences are rated as most negative, while performance consequences are rated as positive.

Among the five brands, consumers are most likely to share personal information with Amazon and least likely with Facebook. The PRICAL index leads to the same implication, which again confirms the predictive validity. In fact, Amazon scores best and Facebook worst on each of the PRICAL dimensions, except for social consequences. The scores of Amazon and Facebook differ significantly on all dimensions ($p < 0.01$), with the exception of the social dimension ($p > 0.10$). Zooming in on the social dimension, consumers value and give a high probability that they can connect with friends and family on Facebook (valence = 1.4, probability = 4.5) but dislike the negative consequences (e.g., that friends and family become aware of which products the consumer is interested in; valence = −1.2, probability = 4.1). Amazon only offers limited opportunities to connect (e.g., via wish lists), which users value less (valence = −0.4) or are less likely to use (probability = 2.1). Yet Amazon users equally fear that family and friends might become aware of the products the consumer is interested in (valence = −1.5, probability = 2.6). We report the top items for Amazon and Facebook in Appendix 3.

The five items that contribute most negatively to the PRICAL index (negative valence and high probability) of Amazon all relate to the security dimension. Four of these items also contribute negatively to Facebook's score, in fact, with more negative valence and higher probability. The fifth most negative item relates to the psychological consequence: respondents reported that they felt like Facebook controls the collection, storage, and usage of personal information.

Items that affect data sharing more positively for Amazon relate to time savings ("I can find the right product or service faster", "The process of completing transactions is partly automated"), performance consequences ("Amazon makes less errors when I interact with them", "I have access to free additional services or content"), and financial consequences ("Amazon is able to keep their prices low"). While Facebook users also perceive these consequences as positive and likely, yet to a lesser extent, the item they reported as most positively contributing is that they can "connect with friends and family".

The analyses of Amazon and Facebook are exemplary, showcasing that the PRICAL score not only offers valid results but also serves diagnostic purposes in identifying brands' strengths and weaknesses with regard to their privacy reputation. Specifically, it allows managers to identify influential dimensions, competitive advantages and disadvantages, and ways to improve them (e.g., increase their perceived valence, make consequences more or less likely).

So far we have focused only on Amazon and Facebook. We now briefly discuss the results for Google. While for all other brands a higher (or less negative) PRICAL score leads to a greater willingness to share information, for Google we observed a relatively low PRICAL score (−1.7 compared to the average) but a willingness to share information similar to that of Apple (Google: 58.8 vs. Apple: 58.4; +0.9 compared to the average). Google's dominant position in the search engine market (a market share of around 87% in 2020; Statista 2020)[7] and the importance of search engines overall (Brynjolfsson, Collis, & Eggers, 2019) could explain this result: many consumers rely on search engines and Google seems the only option for searching online, which may force them to share personal data despite potential concerns on the measured privacy dimensions.

[6] We also conducted a latent segmentation of the consumers on their PRICAL dimension scores and identified three segments: one segment shows negative scores across all dimensions, another only positive scores, and the final segment is more balanced. This type of segmentation outcome is typical for this kind of data (e.g., Konus, Neslin, & Verhoef, 2008). The results of this analysis are available upon request from the authors.

[7] https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/.

Table 6
Comparison of digital brands.

	Significant differences (p-value, ANOVA)	Overall mean across brands	Means per brand (Difference to the overall mean across brands in parentheses)				
			Amazon (n = 101)	Google (n = 98)	Apple (n = 100)	Microsoft (n = 102)	Facebook (n = 101)
WTS	0.015	57.9	66.1 (+8.1)	58.8 (+0.9)	58.4 (+0.5)	55.3 (−2.7)	51.1 (−6.9)
PRICAL	0.013	−88.4	−64.4 (+24.0)	−90.1 (−1.7)	−68.6 (+19.8)	−85.3 (+3.1)	−133.5 (−45.1)
Dimensions							
Financial	0.177	2.0	4.1 (+2.1)	2.7 (+0.7)	2.8 (+0.8)	2.9 (+0.9)	−2.6 (−4.6)
Performance	0.203	14.1	19.2 (+5.1)	13.6 (−0.6)	15.0 (+0.9)	16.4 (+2.3)	6.4 (−7.7)
Psychological	0.053	−26.3	−21.4 (+4.8)	−27.1 (−0.9)	−22.4 (+3.9)	−23.0 (+3.3)	−37.3 (−11.1)
Security	0.014	−65.3	−57.2 (+8.1)	−68.7 (−3.4)	−57.5 (+7.8)	−66.9 (−1.7)	−76.0 (−10.8)
Social	0.535	−6.4	−7.7 (−1.3)	−6.2 (+0.1)	−4.0 (+2.3)	−8.8 (−2.5)	−5.0 (+1.4)
Time	0.001	−6.6	−1.4 (+5.2)	−4.3 (+2.3)	−2.6 (+4.1)	−6.0 (+0.7)	−19.0 (−12.3)

8. Conclusion

8.1. Summary

Firms' growing reliance on consumers' approval of information collection has made it imperative to understand when and why consumers accept the collection of personal information. While the privacy paradox suggests that consumers are unaffected by their attitudes (i.e., privacy concern), we believe this discrepancy is partly due to extant scales' omission of positive consequences. In reality, consumers not only focus on the negative consequences but internally trade off these "costs" against the benefits of information collection. Moreover, as these consequences are not always immediate or certain, measurement of consumers' privacy calculus should take into account the perceived probability of these consequences occurring. In this study, we develop the PRICAL index to measure the privacy calculus, taking into consideration benefits and costs of products and services that are contingent on information collection, while accounting for the uncertainty of these consequences. We consider the privacy calculus a formative construct, which we measure using a multidimensional index consisting of 34 items related to six conceptually distinct dimensions. These six dimensions have so far not been theoretically conceptualized and measured in a privacy context, as privacy conceptualizations and scales typically focus on privacy concern solely or on a limited number of privacy attributes (i.e., control). As the (potential) consequences of information collection vary widely, all PRICAL items (as listed in Appendix 4) are necessary to understand consumers' privacy calculus across various contexts. Consumers may perceive some items or consequences as less relevant in certain contexts, so correcting for the perceived probability is critical to account for these differences.

Our study contributes to the privacy literature by showing that our multidimensional measure accounting for privacy benefits and costs is better suited to predict consumer decisions to accept information-intensive services than looking at privacy concern or trust. More specifically, the PRICAL explains the variance in consumers' willingness to let a bank collect and use detailed payment information (Study 1: 70.5%), consumers' acceptance of the collection of information on their purchases by an offline retailer (Study 1: 67.2%), consumers' willingness to let a telecom provider collect information about their location (Study 1: 42%; Study 2: 57.6%), and consumers' willingness to allow an insurance company to collect driving behavior (Study 2: 43.5%). In addition to explaining these behavioral intentions, the PRICAL index also explains consumers' actual acceptance of information collection (Study 3).

Managerially, we show how the PRICAL index can serve diagnostic purposes. This finding is important given that collecting personal information has become an integral part of many products (e.g., digital assistants, cars like Tesla) and (digital) services (e.g., Verhoef et al., 2017).

Moreover, by focusing on the managerial applicability of the PRICAL index, we also contribute to the marketing scale development literature. This literature mainly focuses on content, convergent, discriminant, and construct validity (e.g., Churchill, 1979). Although we ensure that the PRICAL index scores well on these requirements, we go further by adding the managerial applicability of a scale, which demonstrates that a scale can be used in practice. Specifically, we measure how five top technology brands perform on the PRICAL index. In Web Appendix 3, we provide detailed managerial guidelines for administering the PRICAL survey in practice and communicating the results.

8.2. Limitations and future research

While the PRICAL index predicts and explains the acceptance of information collection rather well, expectedly, a large part of variation remains unexplained. Thus, while the PRICAL index is an improvement over existing measures, it cannot explain all behavioral aspects of consumer decision making or heuristics; that is, it cannot resolve the privacy paradox entirely (Adjerid, Peer, & Acquisti, 2018). Another related limitation is that behavior consistent with the PRICAL index can only be expected when consumers are making a conscious decision about the information collection. Thus, when consumers are unaware that they have a choice, when information is collected without consumers realizing it, or when behavior is habitual (Vance, Jenkins, Anderson, Bjornn, & Kirwan, 2018), their PRICAL index and their actual behavior could differ. Likewise, when consumers have no suitable alternatives, their decision making and privacy calculus could diverge. In those situations, the PRICAL index is less suitable for explaining WTA information collection. In this regard, the PRICAL index might benefit from being integrated into a larger framework to explain and predict data sharing, such as the theory of reasoned action (Fishbein & Ajzen, 1975). In this framework, the PRICAL could account for the attitude toward the behavior that could predict the intention to share personal information, in addition to subjective norms (e.g., perceived social pressure) and motivation to comply. Another concern regarding our study is that we did not explicitly include timing of the consequences in our calculation of the PRICAL index; instead we take a theoretical risk perspective and include it implicitly via the perceived probabilities, supported by our interviews. Future extensions of PRICAL could consider incorporating this aspect more explicitly.

We have used a variety of scenarios and contexts throughout the process of developing the PRICAL index. Moreover, we assessed under which circumstances the PRICAL index is best able to predict the acceptance of information collection. However, the number of applications is still limited. Future research could expand the applicability of the PRICAL index by testing it in more scenarios. In line with this, the managers that were involved in administering the PRICAL survey suggested to derive benchmarks across industries and applications (see Web Appendix 3). Furthermore, we focused on WTA information sharing only. Future research could also study other consequences—for example, privacy responses (e.g., opting in versus opting out) and granting permissions for permission-based marketing initiatives (Krafft, Arden, & Verhoef, 2017). Future researchers could also study more general measures, such as opinions concerning privacy legislation like GDPR.

In Study 3 we used adoption of the usage-based insurance as a proxy for WTA, but we acknowledge that adoption of new products is not driven solely by privacy (Arts, Frambach, & Bijmolt, 2011). Future research could study an actual measure for WTA and/or investigate multiple adoptions of information-based services and products. This research also only examined main effects of the PRICAL index. By broadening this area of study to additional contexts, researchers can also apply the PRICAL index to analyze moderating effects. Specifically, they could look at factors such as riskiness of the product or service.

Yet another limitation is that our study analyzes data of multiple countries (United States vs. the Netherlands) but does not provide a full analysis of country differences. Our study shows that the impact of the dimensions in the same research application (Telecom; Studies 1 and 2) is similar, but in different countries, it can differ substantially. Existing research already suggests that the effect of privacy concerns on willingness to share data is moderated by culture (Schumacher, Eggers, Verhoef, & Maas, 2020). In the context of the PRICAL index, research could focus on understanding cultural effects or the effect of external events and media coverage on, for example, the valence or probability of the dimensions. Moreover, researchers could study the moderating effects of culture, as well as legislation, on the effects of the PRICAL index on data sharing.

Overall, we believe that privacy should gain more attention in marketing given the enormous developments in data science and artificial intelligence (e.g., Huang & Rust, 2021; Wedel & Kannan, 2016). The ongoing digital transformation (Verhoef & Bijmolt, 2019), which has been accelerated by the COVID-19 pandemic, has induced an even stronger focus on data and thus privacy. It would specifically be interesting to investigate how the stronger usage of digital solutions affect the PRICAL index and its underlying dimensions. It would also be fruitful to observe how firms other than those researched herein score on the PRICAL index and how these scores develop over time. Finally, investigating how specific actions of firms can influence the PRICAL index using natural experiments would provide relevant insights.

Acknowledgments

The authors acknowledge the Customer Insight Center from the University of Groningen for funding. They are grateful for receiving valuable comments from participants of EMAC in Oslo, the Marketing Science Conference in Shanghai, seminar participants at IESEG Business School Lille, EDHEC Business School Lille, and University of Stavanger.

Appendix 1. Definitions of dimensions

Dimension	*Definition* *"The potential consequences for consumers resulting from the collection, storage, and usage of information by firms that relate to ..."*	*Based on*
Performance	*... the quality of products or services, or the match between products and services and the needs of consumers.*	Simonson (2005); Lacey et al. (2007); Frow et al. (2011); Wedel and Kannan (2016);
Time	*... the amount of time or effort needed for consumers when dealing with the firm.*	Ackerman et al. (1999); Smith et al. (2014)
Financial	*... the monetary gains and losses when dealing with the firm.*	Acquisti and Varian (2005); Premazzi et al. (2010); Hille et al. (2015)
Psychological	*... consumers' feelings with regard to the firm, their personal information, and their own lives in general.*	Edwards et al. (2002); White (2004); Hong and Thong (2013) Smith et al. (2014)
Social	*... consumers' interpersonal status and relationships with friends and family.*	White (2004); Jiang et al. (2013)
Security	*... the unintended disclosure or exchange of information, or the unauthorized use of information by (unknown) third parties.*	Smith et al. (1996); Malhotra et al. (2004); Hong and Thong (2013)

Appendix 2. Willingness to share (WTS) items

- Name
- Email address
- Income
- Date of birth
- Home address
- Work address
- Work phone number
- Home phone number
- Credit card details
- Financial information
- Driving behavior
- Shopping behavior
- Consumption behavior
- Gender
- Location data
- Social media profiles
- Media habits

Appendix 3

Appendix 3.1. Amazon top items

Item (shortened)	**Prob.**	**Val.**	**Score**
Most negative			
[SEC] My personal information ends up with other firms	5.4	−2.1	−11.3
[SEC] My personal information will become accidently publicly available	4.4	−2.5	−10.8
[SEC] I receive unrequested communication	4.7	−2.1	−9.9
[SEC] My personal information is visible for other people	4.9	−1.9	−9.5
[SEC] My personal information will be used for identity fraud	3.9	−2.4	−9.3

Amazon top items (*continued*)

Item (shortened)	Prob.	Val.	Score
Most positive			
[PERF] I have access to free additional services or content	3.5	1.0	3.5
[FIN] Amazon is able to keep their prices low	3.4	1.0	3.5
[PERF] Amazon makes less errors when I interact with them	3.7	1.2	4.6
[TIME] The process of completing transactions is partly automated	5.4	1.2	6.3
[TIME] I can find the right product or service faster	4.7	1.5	7.1

Appendix 3.2. Facebook top items

Item (shortened)	Prob.	Val.	Score
Most negative			
[SEC] My personal information ends up with other firms	6.1	−2.3	−14.1
[SEC] My personal information will become accidently publicly available	5.2	−2.6	−13.8
[SEC] My personal information will be used for identity fraud	4.8	−2.6	−12.3
[SEC] I receive unrequested communication	5.5	−2.2	−12.3
[PSYCH] It feels like Facebook controls the collection, storage, and usage of my personal information	5.8	−2.0	−11.8
Most positive			
[PERF] Facebook makes less errors when I interact with them	3.4	0.5	1.6
[TIME] The process of completing transactions is partly automated	4.2	0.4	1.9
[PERF] Products and or Services of Facebook are adapted to my personal preferences	5.4	0.4	2.0
[TIME] I can find the right product or service faster	4.0	0.9	3.7
[SOC] I can connect with friends and family	4.5	1.4	6.1

Appendix 4

NOTE: All items start with "*When [Your Firm] collects information about me* ..."

Appendix 4:. Final item list of the PRICAL index

Financial
... I receive monetary compensation
... I have access to monetary savings (i.e. discounts)
... *[Your Firm]* is able to keep their prices low (e.g. due to more efficiency, customer insights)
... *[Your Firm]* adapts it's prices to my personal profile
... *[Your Firm]* is able to generate additional revenues
... *[Your Firm]* charges additional money from my credit card or bank card
Performance
... products and/or services of [*Your Firm*] are adapted to my personal preferences
... I am denied certain services and/or products
... [*Your Firm*] makes less errors when I interact or transact with them
... I receive better service than other customers
... I receive information or feedback giving insight in my own behavior or decisions
... I have access to free (additional) services or content
... I receive communication (e.g. advertisements) that is tailored to my personal needs or preferences
Psychological

(*continued on next page*)

Final item list of the PRICAL index (*continued*)

Financial
... it feels like [*Your Firm*] knows a lot about me
... it feels like [*Your Firm*] follows my behavior
... it feels like [*Your Firm*] controls the collection, storage, and usage of my personal information
... my relationship with [*Your Firm*] becomes closer
... [*Your Firm*] makes me feel special
... I have the possibility to express myself
Social
... I can connect with friends and family
... I have to explain to my family and friends why I shared personal information
... my family and friends receive communication (e.g. advertisements) that is adapted to my personal needs
... family and friends become aware which products or services I am interested in
Security
... my personal information ends up with other firms or organizations
... my personal information will be used for (identity) fraud
... my personal information will become (accidently) publicly available
... it depends on the stability of information systems whether my information is kept safe
... my personal information is visible for other people, like employees
... I receive unrequested communication
Time
... I can find the right product or service faster
... the process of completing transaction is (partly) automated
... I have to actively provide additional information (e.g., via forms)
... I have to take the time to protect my (online) identity
... I have to take the time to monitor how [*Your Firm*] handles my information

Appendix E. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijresmar.2021.05.005.

References

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. *ACM Conference on Electronic Commerce*, 1–8. https://doi.org/10.1145/336992.336995.

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

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research, 49*(2), 160–174.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth?. *Journal of Legal Studies, 42*(2), 249–274.

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442.

Acquisti, A., & Varian, H. R. (2005). Conditioning prices on purchase history. *Marketing Science, 24*(3), 367–381. https://doi.org/10.1287/mksc.l040.0103.

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly, 42*(2), 465–488.

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005.

Arts, J. W. C., Frambach, R. T., & Bijmolt, T. H. A. (2011). Generalizations on consumer innovation adoption: A meta-analysis on drivers of intention and behavior. *International Journal of Research in Marketing, 28*(2), 134–144. https://doi.org/10.1016/j.ijresmar.2010.11.002.

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS Quarterly, 35*(2), 261–292.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). he impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010.

Bansal, G., Zahedi, F. M., & Gefen, D. (2015). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69*(4), 133–152.

Bauer, R. A. (1960). Consumer behavior as risk taking. In R. S. Hancock (Ed.), *Dynamic marketing for a changing world* (pp. 389–398). Chicago: American Marketing Association.

Baumgartner, H., & Steenkamp, J.-B. E. M. (2001). Response styles marketing research: A cross-national investigation. *Journal of Marketing Research, 38*(2), 143–156.

Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer informational privacy: Current knowledge and research directions. *Foundations and Trends in Marketing, 11*(1), 1–71. https://doi.org/10.1561/1700000057.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*, 245–270.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing, 37*(3), 466–480.

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

Bollen, K. A., & Lennox, R. (1991). Conventional wisdom on measurement: A structural equation perspective. *Psychological Bulletin, 110*(2), 305–314. https://doi.org/10.1037/0033-2909.110.2.305.

Borsboom, D., Mellenbergh, G. J., & Van Heerden, J. (2004). The concept of validity. *Psychological Review, 111*(4), 1061–1071. https://doi.org/10.1037/0033-295X.111.4.1061.

Brynjolfsson, E., Collis, A., & Eggers, F. (2019). Using massive online choice experiments to measure changes in well-being. *Proceedings of the National Academy of Sciences, 116*(15), 7250–7255.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of the formative measurement in information systems research. *MIS Quarterly, 33*(4), 689–707.

Churchill, G. A. Jr., (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16*(1), 64–73.

Conchar, M. P., Zinkhan, G. M., Peters, C., & Olavarrieta, S. (2004). An integrated framework for the conceptualization of consumers' perceived-risk processing. *Journal of the Academy of Marketing Science, 32*(4), 418–436. https://doi.org/10.1177/0092070304267551.

Corrigan, H. B., Craciun, G., & Powell, A. M. (2014). How does target know so much about its customers? Utilizing customer analytics to make marketing decisions. *Marketing Education Review, 24*(2), 159–166.

Cunningham, S. M. (1967). The major dimensions of perceived risk. In D. F. Cox (Ed.), *Risk taking and information handling in consumer behavior* (pp. 82–108). Boston: Harvard University Press.

Devaraj, S., Easley, R. F., & Crant, J. M. (2008). Personality matter? Relating the five-factor model to technology acceptance. *Information Systems Research, 19* (1), 93–105. https://doi.org/10.1287/isre.l070.0153.

Diamantopoulos, A. (2005). The C-OAR-SE procedure for scale development in marketing: A comment. *International Journal of Research in Marketing, 22*(1), 1–9. https://doi.org/10.1016/j.ijresmar.2003.08.002.

Dick, A. S., & Basu, K. (1994). Customer loyalty: Toward an integrated conceptual framework. *Journal of the Academy of Marketing Science, 22*(2), 99–113. https://doi.org/10.1177/0092070394222001.

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

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

Edwards, Steven M., Li, Hairong, & Lee, Joo-Hyun (2002). Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of advertising, 31*(3), 83–95.

Fazio, R. H., Powell, M. C., & Williams, C. J. (1989). The role of attitude accessibility in the attitude-to-behavior process. *Journal of Consumer Research, 16*(3), 280–288.

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

Frow, P., Payne, A., Wilkinson, I. F., & Young, L. (2011). Customer management and CRM: Addressing the dark side. *Journal of Services Marketing, 25*(2), 79–89. https://doi.org/10.1108/08876041111119804.

Goldfarb, A., Jin, G., & Sudhir, K. (2020). Introduction to the special issue on consumer protection. *Marketing Science, 39*(1), 1–284.

Goldfarb, A., & Tucker, C. E. (2011). Online display advertising: Targeting and obtrusiveness. *Marketing Science, 30*(3), 389–404. https://doi.org/10.1287/mksc.1100.0583.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing, 10*(1), 149–166.

Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2009). Willingness to disclose personal information online and its effect on ensuring and protecting privacy: A two country study. In AMICS 2009 Proceedings.

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior, 95*, 295–306. https://doi.org/10.1016/j.chb.2018.09.015.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks (CA): SAGE Publications.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science, 45*(5), 616–632. https://doi.org/10.1007/s11747-017-0517-x.

Heckman, J. (1979). Sample selection bias as a specification error. *Econometrica, 47*(1), 153–161.

Hennig-Thurau, T., Gwinner, K. P., & Gremler, D. D. (2002). Understanding relationship marketing outcomes: An integration of relational benefits and relationship quality. *Journal of Service Research, 4*(3), 230–247. https://doi.org/10.1177/1094670502004003006.

Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M., & Calantone, R. J. (2014). Common beliefs and reality about PLS: Comments on Ronkko and Evermann (2013). *Organizational Research Methods, 17*(2), 182–209. https://doi.org/10.1177/1094428114526928.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20*, 177–191. https://doi.org/10.1016/0167-8116(92)90003-4.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30* (May), 1–19. https://doi.org/10.1016/j.intmar.2014.10.001.

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management, 21*(5). https://doi.org/10.1016/0149-2063(95)90050-0.

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

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

Huang, M.-H., & Rust, R. T. (2021). Engaged to a robot? The role of AI in service. *Journal of Service Research, 24*(1), 30–41. https://doi.org/10.1177/1094670520902266.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199–218.

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Research Note - Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579–595. https://doi.org/10.1287/isre.1120.0441.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29.

Kaplan, L. B., Szybillo, G. J., & Jacoby, J. (1974). Components of perceived risk in product purchase. *Journal of Applied Psychology, 59*(3), 287–291.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635. https://doi.org/10.1111/isj.12062.

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

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2009). Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration. *Information Systems Research, 20*(2), 237–257. https://doi.org/10.1287/isre.1080.0188.

Klein, R., & Rai, A. (2009). Interfirm strategic information flows in logistics supply chain relationships. *MIS Quarterly, 33*(4), 735–762.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of E-Collaboration, 11*(4), 1–10.

Kohli, A. K., & Haenlein, M. (2021). Factors affecting the study of important marketing issues: Implications and recommendations. *International Journal of Research in Marketing, 38*(1), 1–11. https://doi.org/10.1016/j.ijresmar.2020.02.009.

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns — Why do customers (not) grant permissions? *Journal of Interactive Marketing, 39*(August), 39–54. https://doi.org/10.1016/j.intmar.2017.03.001.

Lacey, Russell, Suh, Jaebeom, & Morgan, Robert M. (2007). Differential effects of preferential treatment levels on relational outcomes. *Journal of service research, 9*(3), 241–256.

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

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), 62–71. https://doi.org/10.1080/08874417.2010.11645450.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010.

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. https://doi.org/10.1037//0021-9010.86.1.114.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research, 122*, 875–888.

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of Retailing, 88*(4), 542–555. https://doi.org/10.1016/j.jretai.2012.08.001.

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). https://doi.org/10.2307/23044045.

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

Marcati, A., Guido, G., & Peluso, A. M. (2008). The role of SME entrepreneurs' innovativeness and personality in the adoption of innovations. *Research Policy, 37*(9), 1579–1590. https://doi.org/10.1016/j.respol.2008.06.004.

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information sensitivity and willingness to provide continua: A comparative privacy study of the United States and Brazil. *Journal of Public Policy & Marketing, 36*(1), 79–96.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58.

McCrae, R. R., & Costa, P. T. Jr., (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology, 52*(1), 81–90. https://doi.org/10.1037/0022-3514.52.1.81.

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

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs, 51*(1), 133–161. https://doi.org/10.1111/joca.12111.

Mitchell, V.-W. (1999). Consumer perceived risk: Conceptualisations and models. *European Journal of Marketing, 33*(1/2), 163–195. https://doi.org/10.1108/03090569910249229.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20–38.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76–98. https://doi.org/10.1177/1094670511424924.

Murray, K. B., & Schlacter, J. L. (1990). The impact of services versus goods on consumers' assessment of perceived risk and variability. *Journal of the Academy of Marketing Science, 18*(1), 51–65. https://doi.org/10.1007/BF02729762.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–127.

Nunnally, J. C., & Bernstein, I. H. (1994). *The assessment of reliability. Psychometric Theory, 3*(1), 248–292.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multi-item scale for measuring consumer perceptions of service quality. *Journal of Retailing, 64*(1), 12–40.

Parasuraman, A., Zeithaml, V. A., & Malhotra, A. (2005). E-S-QUAL: A multiple-item scale for assessing electronic service quality. *Journal of Service Research, 7*(3), 213–233. https://doi.org/10.1177/1094670504271156.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology, 70*, 153–163. https://doi.org/10.1016/j.jesp.2017.01.006.

Peltier, J. W., Milne, G. R., & Phelps, J. E. (2009). Information privacy research: Framework for integrating multiple publics, information channels, and responses. *Journal of Interactive Marketing, 23*(2), 191–205. https://doi.org/10.1016/j.intmar.2009.02.007.

Peter, J. P., & Ryan, M. J. (1976). An investigation of perceived risk at the brand level. *Journal of Marketing Research, 13*(2), 184–188.

Peter, J. P., & Tarpey, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research, 2*(1), 29–37.

Phelps, J. E., Nowak, G. J., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27–41.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Premazzi, K., Castaldo, S., Grosso, M., Raman, P., Brudvig, S., & Hofacker, C. F. (2010). Customer information sharing with e-vendors: The roles of incentives and trust. *International Journal of Electronic Commerce, 14*(3). https://doi.org/10.2753/JEC1086-4415140304.

PwC. (2012). Consumer privacy: What are consumers willing to share? In The speed of life: Consumer intelligence series. Retrieved from https://www.pwc.com/sg/en/tice/assets/ticenews201208/consumerintelligence201208.pdf (accessed on May 14, 2021).

Rafieian, O., & Yoganarasimhan, H. (2021). Targeting and privacy in mobile advertising. *Marketing Science, 40*(2), 193–394.

Reinartz, W. J., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing, 26*(4), 332–344. https://doi.org/10.1016/j.ijresmar.2009.08.001.

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

Roberts, J. H., Kayande, U., & Stremersch, S. (2014). From academic research to marketing practice: Some further thoughts. *International Journal of Research in Marketing, 31*(2), 144–146.

Rose, J., Rehse, O., & Röber, B. (2012). The value of our digital identity. Retrieved from https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf, accessed on May 14, 2021.

Roselius, T. (1971). Consumer rankings of risk reduction methods. *Journal of Marketing, 35*(1), 56–61.

Rossiter, J. R. (2002). The C-OAR-SE procedure for scale development in marketing. *International Journal of Research in Marketing, 19*(4), 305–335.

Rust, R. T., & Huang, M.-H. (2014). The service revolution and the transformation of marketing science. *Marketing Science, 33*(2), 206–221.

Schumacher, C., Eggers, F., Verhoef P.C. and Maas, P. (2020), The Effects of Cultural Differences on Consumers' Willingness to Share Personal Information, Working Paper, U. of St. Gallen.

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.

Simonson, I. (2005). Determinants of customers' responses to customized offers: Conceptual framework and research propositions. *Journal of Marketing, 69*(1), 32–45. https://doi.org/10.1509/jmkg.69.1.32.55512.

Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinairy review. *MIS Quarterly, 35*(4), 989–1015.

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

Smith, J. S., Gleim, M. R., Robinson, S. G., Kettinger, W. J., & Park, S.-H. (2014). Using an old dog for new tricks: A regulatory focus perspective on consumer acceptance of RFID applications. *Journal of Service Research, 17*(1), 85–101. https://doi.org/10.1177/1094670513501394.

Stewart, D. A. (2017). A comment on privacy. *Journal of the Academy of Marketing Science, 45*(2), 156–159.

Stone, R. N., & Grønhaug, K. (1993). Perceived risk: Further considerations for the marketing discipline. *European Journal of Marketing, 27*(3), 39–50.

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.

Urban, G. L., Amyx, C., & Lorenzon, A. (2009). Online trust: state of the art, new frontiers, and research potential. *Journal of Interactive Marketing, 23*(2), 179–190. https://doi.org/10.1016/j.intmar.2009.03.001.

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly, 42*(2), 355–380. https://doi.org/10.25300/MISQ/2018/14124.

Verhoef, P. C., & Bijmolt, T. H. A. (2019). Marketing perspectives on digital business models: A framework and overview of the special issue. *International Journal of Research in Marketing, 36*(3), 341–349.

Verhoef, P. C., Kooge, E., & Walk, N. (2016). *Creating value with big data analytics: Making smarter marketing decisions*. Routledge.

Verhoef, P. C., Stephen, A. T., Kannan, P., Luo, X., Abhishek, V., Andrews, M., ... Zhang, Y. (2017). Consumer connectivity in a complex, technology-enabled, and mobile-oriented world with smart products. *Journal of Interactive Marketing, 40*, 1–8.

Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing, 80*(6), 97–121. https://doi.org/10.1509/jm.15.0413.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology, 14*(1–2), 41–51.

Wieringa, J. E., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2021). Data analytics in a privacy-concerned world. *Journal of Business Research., 122*, 915–925. https://doi.org/10.1016/j.jbusres.2019.05.005.

Williams, L. J., Hartman, N., & Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive CFA marker technique. *Organizational Research Methods, 13*(3), 477–514.

World Economic Forum. (2014). Rethinking personal data: A new lens for strengthening trust. Retrieved from http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf, accessed on May 14, 2021.

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

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). https://doi.org/10.2753/MIS0742-1222260305.

Zaichkowsky, J. L. (1985). Measuring the involvement construct. *Journal of Consumer Research, 12*(3), 341–352.

Web references

Interbrand (2020). Best Global Brands 2019. accessed: 28 August 2020, https://www.interbrand.com/best-brands/best-global-brands/2019/ranking/.