

“Fundamentalist, pragmatic, or unconcerned?”: an analysis of consumers’ willingness to disclose information online

Fundamentalist,
pragmatic or
unconcerned

31

Renata Monteiro Martins

Department of Marketing, FGV-EAESP, Sao Paulo, Brazil

Sofia Batista Ferraz

Department of Marketing, FGV-EAESP, Sao Paulo, Brazil and Department of Marketing, Escola Superior de Propaganda e Marketing, Sao Paulo, Brazil, and

André Francisco Alcântara Fagundes

Department of Business, Universidade Federal de Uberlândia, Uberlândia, Brazil

Received 15 June 2023
Revised 21 September 2023
21 November 2023
Accepted 23 November 2023

Abstract

Purpose – This study aims to propose an innovative model that integrates variables and examines the influence of internet usage expertise, perceived risk and attitude toward information control on privacy concerns (PC) and, consequently, in consumers’ willingness to disclose personal information online. The authors also propose to test the mediation role of trust between PCs and willingness to disclose information. Trust is not a predictor of PC but a causal mechanism – considering that the focus is to understand consumers’ attitudes and behavior regarding the virtual environment (not context-specific) (Martin, 2018).

Design/methodology/approach – The authors developed a survey questionnaire based on the constructs that compose the proposed model to collect data from 864 respondents. The survey questionnaire included the following scales: internet usage expertise from Ohanian (1990); perceived risk, attitude toward information control, trust and willingness to disclose personal information online from Malhotra et al. (2004); and PC from Castañeda and Montoro (2007). All items were measured on a Likert seven-point scale (1 = totally disagree; 7 = totally agree). To obtain Westin’s attitudinal categories toward privacy, respondents answered Westin’s three-item privacy index. For data analysis, the authors applied covariance-based structural equation modeling.

Findings – First, the proposed model explains the drivers of consumers’ disposition to provide personal information at a level that surpasses specific contexts (Martin, 2018), bringing the analysis to consumers’ level and considering their general perceptions toward data privacy. Second, the findings provide inputs to propose a better definition of Westin’s attitudinal categories toward privacy, which used to be defined only by individuals’ information privacy perception. Consumers’ perceptions about their abilities in using the internet, the risks, their beliefs toward information control and trust also help to delimitate and distinguish the fundamentalists, the pragmatics and the unconcerned.

© Renata Monteiro Martins, Sofia Batista Ferraz and André Francisco Alcântara Fagundes. Published in *RAUSP Management Journal*. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licenses/by/4.0/legalcode>

The authors thank Professor Stella Moriguchi (Universidade Federal de Uberlândia) for the insightful contributions.

Conflict of Interest Statement: The authors declare that there is no conflict of interest.



Research limitations/implications – Some limitations weigh the theoretical and practical implications of this study. The sample size of pragmatic and unconcerned respondents was substantially smaller than that of fundamentalists. It might be explained by applying Westin’s self-report index to classify the groups according to their score regarding PCs. Most individuals affirm having a great concern for their data privacy but still provide online information for the benefit of personalization – known as the privacy paradox (Zeng et al., 2021). It leads to another limitation of this research, given the lack of measures that classify respondents by considering their actual behavior toward privacy.

Practical implications – PC emerges as an important predictor of consumer trust and willingness to disclose their data online, and trust also influences this disposition. Managers need to implement actions that effectively reduce consumers’ concerns about privacy and increase their trust in the company – e.g. adopting a clear and transparent policy on how the data collected is stored, treated, protected and used to benefit the consumer. Regarding the perception of risk, if managers convince consumers that the data collected on the internet is protected, they tend to be less concerned about privacy.

Social implications – The results suggest different aspects influencing the willingness to disclose personal information online, including different responses considering consumers’ PCs. Through their policies and legislation, the authors understand that governments must be attentive to this aspect, establishing regulations that protect consumers’ data in the virtual environment. In addition to regulatory policies, education campaigns can be carried out for both consumers and managers to raise the discussion about privacy and the availability of information in the online environment, demonstrating the importance of protecting personal data to benefit the government, consumers and organizations.

Originality/value – Although there is increasing research on consumers’ privacy, studies have not considered their attitudinal classifications – high, moderate and low concern – as moderators of willingness to disclose information online. Researchers have also increased attention to the antecedents of PCs and disclosure of information but overlooked possible mechanisms that explain the relationship between them.

Keywords Willingness to disclose information, Privacy concern, Trust, Consumers’ attitudes toward privacy

Paper type Research paper

1. Introduction

About 46% of consumers worldwide feel unable to protect their data. Since 2018, 33% of users have left social media, and 28% left internet service providers. The main reason is a need for more transparency and clarity regarding companies’ policies and data practices (Cisco, 2021).

This concern makes sense as companies like Amazon, Google and Facebook use exclusive identifiers to track users’ online activities and facilitate marketing communication. As a result, individuals constantly face ads for products they would probably buy on different websites they access, even when these Web pages are not interrelated (Marr, 2017; Markman, 2017; Schifferle, 2016). In this sense, consumers become data producers in both voluntary (i.e. subscribing to websites) and involuntary (i.e. cookies) ways (Aloysius, Hoehle & Venkatesh, 2016; Chen, Chiang and Storey, 2012; Chen & Zhang, 2014; Manovich, 2012).

The blur between “choice-choicelessness, empowerment-entrapment, and autonomy-autocracy” has been intensified in the digital age (Dholakia et al., 2021, p. 65). As tracking and mining technologies evolve, legal-political debates on information privacy strengthen (Gandon & Sadeh, 2004; Nissenbaum, 2010). To illustrate, Cambridge Analytica, the political consultancy responsible for Donald Trump’s 2016 successful election, leaked the personal data of up to 87 million Facebook users, leading to a privacy scandal (Ingram, 2018). This episode resulted in many people canceling their accounts and promoting a “Delete Facebook” campaign (Dudley-Nicholson, 2018).

Although debates on data privacy have gained relevance in the last years with the consolidation of e-commerce and social media, changes in individuals’ attitudes toward privacy concern (PC) have been investigated since the 1960s. Westin (1967, 2003), one of the

seminal authors in the privacy field, analyzed the conflict between privacy and tracking in modern society to understand the role that privacy has on people's lives in the face of the advances in surveillance technologies. He conducted about 30 studies sponsored by Equifax Inc. on consumers' information privacy regarding the usage companies from different sectors use from their data (Kumaraguru & Cranor, 2005).

Westin (1967, 2003) identified three groups of individuals (or attitudinal categories toward privacy), classifying them as *fundamentalists* (high PC), *pragmatics* (moderate PC) and *unconcerned* (low PC). From 1961 to 2002, fundamentalists and pragmatics prevailed over unconcerned as people became more aware of the negative consequences of disclosing personal information (Kumaraguru & Cranor, 2005; Westin, 2003). However, even though Westin's (2003) studies show that people are increasingly concerned about their informational privacy, online personalization of products and services provides value for consumers in strengthening business-to-consumer relationships. For example, consumers can receive notifications when a desired product is on sale (Aguirre, Roggeveen, Grewal & Wetzels, 2016; Sutanto, Palme, Tan & Phang, 2013).

In this context, the trade-off between privacy and disclosing personal information online to obtain economic or social benefits has gained the attention of researchers since the 2000s. Literature findings suggest that Internet usage expertise (e.g. Lopez-Nicolas & Molina-Castillo, 2008; Pomfret, Previte & Coote, 2020), perceived risk (e.g. Malhotra, Kim & Agarwal, 2004; Mourey & Waldman, 2020; Park & Jun, 2003), attitude toward information control (e.g. Castañeda & Montoro, 2007; Lin & Liu, 2012; Willis, Jai & Lauderdale, 2021), PC (e.g. Grosso, Castaldo, Li & Larivière, 2020; Kim & Kim, 2018; Lin & Liu, 2012; Malhotra et al., 2004; Phelps, Nowak & Ferrell, 2000; Schoenbachler & Gordon, 2002) and trust in online companies (Swani, Milne & Slepchuk, 2021; Lin & Liu, 2012; Wu, Huang, Yen & Popova, 2012) are antecedents of information disclosure behavior.

This research proposes an innovative model that integrates these variables and examines the influence of internet usage expertise, perceived risk and attitude toward information control on PCs and, consequently, in consumers' willingness to disclose personal information online. We also propose to test the mediation role of trust between PCs and willingness to disclose information. Trust is not a predictor of PC but a mechanism – considering that our focus is to understand consumers' attitudes and behavior regarding the virtual environment (not context-specific) (Martin, 2018). Furthermore, although previous studies have referenced Westin's (1967, 2003) works (Kasper, 2005; Kumaraguru & Cranor, 2005; Margulis, 2003; Moore, 2008; Solove, 2008), this research is the first to consider his proposed typologies (e.g. fundamentalists, pragmatics and unconcerned) as moderators. We assume that these individuals' characteristics present different responses regarding their attitudes toward privacy.

2. Theoretical background and hypotheses

2.1 Privacy concern, trust and consumer willingness to disclose personal information online

Advanced technologies in data collection and mining have transformed the nature of products, production and communication to provide personalization to consumers, allowing companies to identify latent needs and to direct to the products and services regarding their behavior and preferences (Martinez-Lopez, Pla-García, Gázquez-Abad & Rodríguez-Ardura, 2014; Weijo, Hietanen & Matilla, 2014). However, despite the benefits of personalization, there is a growing concern about ethical issues, such as information privacy, security and anonymity (Martin & Murphy, 2017; Michael & Miller, 2013; Pentland, 2013; Zwitter, 2014). Considering that individuals face a “privacy versus personalization” dilemma (Chellappa &

Sin, 2005), this research examines the factors determining consumers' disclosure of personal information.

Consumer willingness to disclose personal information reflects how individuals give their information in exchange for the value of the benefits they receive. It also depends on how they respond to the way companies use their information (Schoenbachler & Gordon, 2002). As most companies adopt data-driven strategies focusing on one-to-one marketing, consumers are even more prone to disclose information due to the value of personalization (Phelps et al., 2000; Xie, Teo & Wan, 2006).

Based on prior literature, our research draws attention to consumers' PCs and trust (on websites and social media platforms in general) as direct antecedents intrinsically related to consumers' willingness to disclose personal information online (Grosso et al., 2020; Lin & Liu, 2012; Sutanto et al., 2013; Urbonavicius, Degutis, Zimaitis, Kaduskeviciute & Skare, 2021).

PCs refer to individuals' apprehension about how their data are collected and used by companies or institutions online to generate information about them (Castañeda & Montoro, 2007). When consumers are concerned about their information privacy, they take caution in disclosing their data, adopting actions to protect themselves (Grosso et al., 2020; Kumaraguru & Cranor, 2005). Individuals are generally concerned about how companies collect their data and analyze and use it for strategy development (Mai, 2016). Even when companies ensure the security of consumers' information (being transparent and clearer about their privacy policies), individuals feel invaded, believing their data are collected involuntarily and without their consent. Thus, consumers highly concerned about privacy are usually reluctant to provide their personal information online (Bandyopadhyay & Bandyopadhyay, 2018; Milne & Culnan, 2004). Then, we hypothesize that:

H1. PC negatively influences consumer willingness to disclose personal information online.

Trust refers to the extent to which individuals believe their data are protected by the ones who collect it. In an online context, trust-building is centered on trust delegation. Consumers delegate their trust to organizations, permitting them to make decisions based on their data, which includes delegating consumers' information to third parties (Grandison & Sloman, 2000). Because trust also involves risks and uncertainty, it is expected that the one being trusted will act accordingly (Siau & Shen, 2003).

PC and trust have similar levels of analysis as both are relational constructs resulting from a combination of dispositions and attitudes toward how companies use consumers' personal information (Martin, 2018). Depending on the context of the analysis, on the one hand, trust can influence PCs. For example, if consumers trust a specific firm, they will be less concerned about the usage that this firm makes of their data (e.g. Grosso et al., 2020; Rohm & Milne, 2004; Urbonavicius et al., 2021). On the other hand, PCs can affect trust. This research analyzes trust and privacy at a general level that transcends particular situations (Martin, 2018). We posit that when individuals have a higher level of PC, they will have a lower disposition to trust that their personal information is secured by online companies (Kehr, Kowatsch, Wentzel & Fleisch, 2015). Thus:

H2. PC negatively influences trust.

Trust, in turn, also predicts consumer willingness to disclose information online. The more consumers believe their information is secure with online companies, the higher will be their disposition to provide their personal information (Kim, Park, Park & Ahn, 2019). Accordingly, we hypothesized:

-
- H3. Trust positively influences consumers' willingness to disclose personal information online. Fundamentalist, pragmatic or unconcerned
- H4. Trust mediates the relationship between PCs and consumers' willingness to disclose personal information online.

2.2 Antecedents of privacy concern

Several antecedents of PC in the online context have been considered in prior research, such as individuals' responses toward privacy notices (Awad & Krishnan, 2006), familiarity with online companies (Castañeda & Montoro, 2007; Schoenbachler & Gordon, 2002) and companies' reputation (Schoenbachler & Gordon, 2002; Xie et al., 2006). However, consumers' responses to these factors might vary according to companies, product categories or brands.

Our research focuses on consumers' cognition and attitudes toward the general context of companies' online data collection, tracking and usage. Thus, alternatively, we propose to investigate consumers' internet usage expertise (Dinev & Hart, 2005; Lopez-Nicolas & Molina-Castillo, 2008; Zhou, 2020), perceived risk (Chang, Shen & Liu, 2016; Lopez-Nicolas & Molina-Castillo, 2008; Malhotra et al., 2004; Youn, 2009) and attitude toward information control (Anic, Škare & Milaković, 2019; Malhotra et al., 2004; Taylor, Davis & Jillapalli, 2009) as antecedents of PC. These constructs reflect consumers' perceptions about their abilities to protect themselves from data privacy violations.

Internet usage expertise refers to the degree to which individuals believe in having self-sufficient abilities to use the internet, such as dealing with basic technical problems (i.e. spam and viruses), making transactions online, knowing how to protect their information and identifying dangerous e-mail messages and websites (Dinev & Hart, 2005). It means that people with higher levels of internet usage expertise have the technical knowledge to cope with internet risks and often customize their browsers to protect themselves from malware and fraud. As they can ensure the safety of their information, they have lower levels of PC (Dinev & Hart, 2005; Lopez-Nicolas & Molina-Castillo, 2008; Zhou, 2020). Thus:

- H5. Internet usage expertise negatively influences PCs.

The perceived risk involves the consumers' subjective feeling that certain events are highly likely to happen, leading to negative consequences. However, this definition is even more complex, as it varies according to the context (Pérez-Cabañero, 2007). The perceived risk is assumed to be one-factor driving information PCs and trust. This study considers the definition proposed by Malhotra et al. (2004), in which perceived risk is related to consumers' expectations of negative events if they provide their personal information to companies online. When individuals perceive risky situations, they often adopt protective behaviors, such as falsifying personal data or searching for information about a certain website related to a high PC (Chang et al., 2016; Malhotra et al., 2004; Youn, 2009). Therefore, we propose the following hypothesis:

- H6. The perceived risk positively influences PCs.

Sometimes, consumers realize that their data are being collected without their consent only when they face ads or personalized products according to their preferences, impacting their desire to control their data (Hoadley, Xu, Lee & Rosson, 2010; Taylor et al., 2009). Information control is a key driver of PC, mainly because its absence leads to greater perceived risks (Malhotra et al., 2004). Consumers with a greater attitude toward information control need to perceive how companies collect their data fairly. Thus, since the attitude toward information control consists of how much individuals wish to decide what

can be known about them, we can state that the higher the attitude toward information control, the higher the PC (Anic et al., 2019; Taylor et al., 2009). It leads to the following hypothesis:

H7. The attitude toward information control positively influences PCs.

2.3 Attitudinal categories toward privacy

Westin (1967, 2003) was one of the leading researchers in the field of PC, providing a deeper understanding of the role of technological advances. From 1961 to 2002, he observed that the way consumers respond to privacy in the face of these advances changed over the years, which led to the development of a PC index.

This index comprises three items and measures consumers' perceptions of how their personal information is collected and used by companies. Based on this index, he classified individuals into three attitudes toward privacy according to the extent to which they agree with each item. The *unconcerned* have a lower level of PC and are more prone to provide their personal information to companies and institutions. The *pragmatics* believe they can benefit themselves by providing their personal information to companies but, at the same time, are concerned about how these companies use their data. The *fundamentalists* have high levels of PCs and hardly provide their personal information. Westin's (2003) studies show that, as the technologies evolve, the number of fundamentalists and pragmatics increases (while the number of unconcerned people decreases).

Westin's (1967, 2003) works have been foundational to several studies (e.g. Kasper, 2005; Kumaraguru & Cranor, 2005; Margulis, 2003; Moore, 2008; Solove, 2008). However, the role of attitudinal categories toward privacy has not been considered a moderator of a model behind consumers' willingness to disclose personal information online. Understanding how this model responds to this moderation can help to explain the differences among these three groups regarding the psychological and behavioral processes toward privacy and provide further insights into this literature.

We posit that moderation occurs in both fundamentalist and unconcerned levels since they represent opposite sides of Westin's privacy index and may affect the strength or direction of the model relationships. On the other hand, it will not occur at the pragmatics level, as we do not expect the model to remain the same in this group. To explore and identify which relationships are stronger or weaker among fundamentalists, pragmatics and unconcerned, our final hypothesis is

H8. Westin's attitudinal categories toward privacy (fundamentalist, unconcerned and pragmatic) moderate the relationships posited in the structural model.

2.4 Research model

After reviewing prior literature and establishing the research hypotheses, we propose an integrated model of consumer willingness to disclose personal information online, considering the moderating role of attitudinal categories toward privacy (Figure 1).

3. Method

3.1 Sample and measures

We developed a survey questionnaire based on the constructs that compose the proposed model to collect data from 864 sampling units (63.7% female, $\bar{X}_{age} = 25.57$; $SD = 6.69$). We considered the minimum dimensions for multivariate analysis, with 10 cases per observable variable (30 variables) (Hair, Black, Babin & Anderson, 2010).

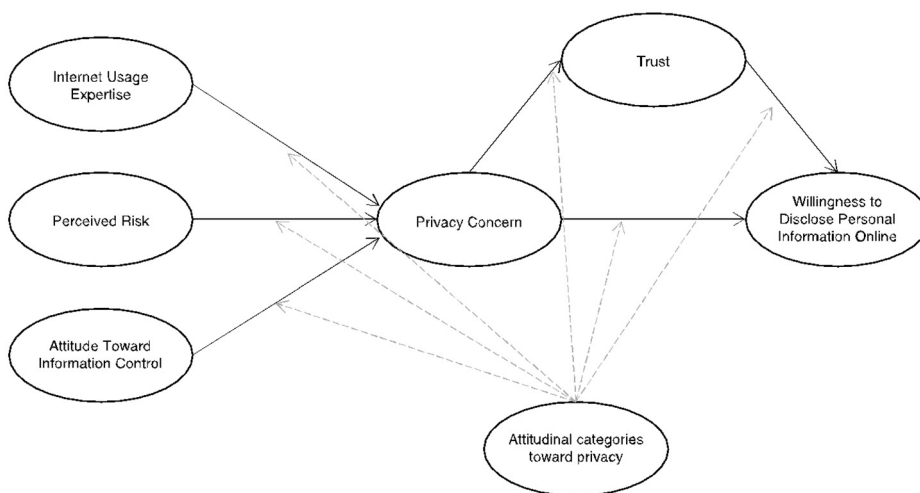


Figure 1.
The proposed
structural model

Source: Figure by authors

We adapted and replicated validated scales from other studies to measure the independent and dependent variables. Four professors who specialized in survey research previously reviewed our data collection instrument. After the first adjustments, a pretest was applied to 21 participants (including undergraduate students, master’s students and professors of a Business course).

The survey questionnaire included the following scales: internet usage expertise from [Ohanian \(1990\)](#); perceived risk, attitude toward information control, trust and willingness to disclose personal information online from [Malhotra et al. \(2004\)](#); and PC from [Castañeda and Montoro \(2007\)](#). All items were measured on a Likert seven-point scale (1 = *totally disagree*; 7 = *totally agree*).

To obtain Westin’s attitudinal categories toward privacy (moderator variable), respondents answered Westin’s three-item privacy index using a seven-point scale according to their level of agreement with the statements. The same procedure was adopted in this study, considering the respondent’s leverage scores regarding the privacy index. Those who scored between 1 and 3 (*totally disagree*, *disagree* and *partially disagree*) were classified as “unconcerned.” Between 5 and 7 (*partially agree*, *agree* and *totally agree*) were classified as “fundamentalists.” Those who scored close to 4 (*neutral*) were classified as “pragmatics.”

3.2 Data analysis

For data analysis, we applied the technique of covariance-based structural equation modeling (SEM-CB), as our model is based on the common variance of data ([Hair, Gabriel & Patel, 2014](#)). We used the statistical software Statistical Package for the Social Sciences (SPSS) 23.0 and Analysis of Moment Structures (AMOS) 22.0 to run the model. All analyses considered a confidence interval of 95%.

4. Results

Initially, we analyzed tolerance and variance of inflation, which indicated no signs of multicollinearity (TOL > 0.20 and VIF < 5.00). We did not need to exclude the missing

values, as the questions in the questionnaire required a mandatory answer to be completed. We also decided not to exclude outliers, considering that the Likert scale measured the variables.

We proceeded with the data analysis with the confirmatory factor analysis. The model suggests a good overall fit ($\chi^2/df = 2.411$; $RMR = 0.078$, $GFI = 0.931$; $NFI = 0.931$, $CFI = 0.958$; $RMSEA = 0.040$; $p < 0.001$). The composite reliability values were greater than 0.70, which is acceptable according to [Hair et al. \(2010\)](#) criteria. However, the dimension of PC toward data collection (PC1) – from the second-order construct of PC – presented an average variance extracted (AVE) lower than 0.50. With the exclusion of the item PC1-4, in which the factorial load was lower than 0.70, we achieved adequate values for convergent validity, considering factorial loads > 0.60 ; $AVE > 0.50$; composite reliability > 0.75 ; and Cronbach's alpha > 0.75 ([Table 1](#)) ([Hair et al., 2010](#)).

The AVE's values were greater than the value squared of the correlation between constructs, indicating discriminant validity according to [Fornell and Larcker's \(1981\)](#) criterion ([Table 2](#)).

We proceeded with the analysis of the structural model ([Figure 2](#)), which presents good indicators of model fit ($\chi^2/df = 3.114$; $RMR = 0.182$; $GFI = 0.914$; $NFI = 0.912$; $CFI = 0.938$; $RMSEA = 0.049$; $p < 0.001$).

The *H1*, *H2*, *H3*, *H5*, *H6* and *H7* were supported ([Table 3](#)). Thus, all the relationships between the model constructs explain consumers' willingness to disclose information online. Internet usage expertise, perceived risk and attitude toward information control predict consumers' PCs. A lower internet usage expertise, a higher perceived risk and a higher attitude toward information control lead to a greater PC. PC, in turn, is negatively related to trust and consumers' willingness to disclose information online, while trust is positively related to the latter. The strongest relationship of the model is the attitude toward information control and PC, followed by PC and trust.

An analysis of the path coefficients and indirect effects ([Table 4](#)) and the results of the Sobel test ($z = -3.01$, $p = 0.000$) supported *H4*, indicating that trust partially mediated the relationship between PCs and willingness to disclose information online.

Finally, we run a multigroup analysis to identify the existence of significant differences in the relationships regarding the moderating effect of Westin's attitudinal categories toward privacy, given by the groups of fundamentalists (1), pragmatics (2) and unconcerned (3). The chi-square distribution test indicated a significant difference between the unconstrained (A) and the constrained model (B) ($\chi^2A - \chi^2B = 30.244$, $df_A - df_B = 14$, $p = 0.007$), supporting *H8* ([Figure 3](#)).

We followed the analysis by comparing the hypotheses across the three groups ([Table 5](#)). The relationship between internet usage expertise and PC is stronger among fundamentalists ($\beta = -0.164$, $p = 0.034$) but nonsignificant among pragmatics ($\beta = -0.217$, n.s.) and unconcerned consumers ($\beta = -0.268$, n.s.). The impact of the perceived risk on PC is also stronger among fundamentalists ($\beta = 0.327$, $p = 0.000$) and nonsignificant for the pragmatics ($\beta = 0.506$, n.s.) and unconcerned ones ($\beta = 0.081$, n.s.). The relationship between attitude toward information control and PC is nonsignificant only for the pragmatics ($\beta = 0.303$, n.s.) and significant for fundamentalists ($\beta = 0.493$, $p = 0.000$) and unconcerned consumers ($\beta = 0.807$, $p = 0.006$) – being stronger for the latter. The same effect occurs in the relationship between PC and willingness to disclose information online, as it is nonsignificant for pragmatics and significant for fundamentalists ($\beta = -0.360$, $p = 0.000$) and the unconcerned ones ($\beta = -0.431$, $p = 0.046$), also being stronger for the latter group. The relationship between PC and trust, and trust and willingness to disclose information online, is significant only for fundamentalists ($\beta_{PC-TRU} = -0.313$, $p = 0.001$;

Construct	Items	Factor loadings	Composite reliability	Cronbach's alpha	AVE
<i>Internet usage expertise (IUE)</i>	IUE1: I think I am experienced	0.760	0.904	0.896	0.655
	IUE2: I think I am an expert	0.659			
	IUE3: I think I am well-informed	0.780			
	IUE4: I think I am qualified	0.929			
	IUE5: I think I am trained	0.891			
<i>Perceived risk (PR)</i>	PR1: In general, it is risky to give my personal information to websites	0.657	0.866	0.861	0.565
	PR2: There is a great chance of having problems giving my personal information to websites	0.799			
	PR3: I have doubts when I provide my personal information to websites	0.726			
	PR4: Giving my personal information on the Internet involves too many unexpected problems	0.854			
	PR5: I do not feel safe giving my personal information to websites	0.706			
<i>Attitude toward information control (AIC)</i>	AIC1: Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used and shared	0.825	0.824	0.815	0.613
	AIC2: Consumer control of personal information lies at the heart of consumer privacy	0.852			
	AIC3: I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction	0.657			
	AIC4: When I provide my personal data to websites, I am not sure who might collect it	0.624			
<i>Privacy concern toward data collection (PC1)</i>	PC1-1: When I surf the Internet, I cannot control the data websites collect on me	0.709	0.758	0.752	0.514
	PC1-3: When I buy online, I cannot control who might collect my personal data	0.806			
	PC1-4*: My data is not safe on the Internet and may be collected by unauthorized people or organizations	–			
	PC1-2: Websites cannot share the information I voluntarily provide to them with other firms without my permission	0.799			
<i>Privacy concern toward data usage (PC2)</i>	PC2-1: Websites cannot share the information they collect about my surfing process with other firms without my permission	0.878	0.871	0.865	0.628
	PC2-2: Websites cannot share the information they collect about my surfing process with other firms without my permission	0.725			
	PC2-3: Websites cannot hand over the information they collect on me to other departments in the organization without my permission	0.762			
	PC2-4: Websites cannot use the information they collect on me for purposes different from that initially authorized	–			

(continued)

Fundamentalist,
pragmatic or
unconcerned

Table 1.
Convergent validity

Table 1.

Construct	Items	Factor loadings	Composite reliability	Cronbach's alpha	AVE
<i>Trust (TRU)</i>	TRU1: Websites are trustworthy in handing over my personal information	0.711	0.870	0.869	0.573
	TRU2: Websites fulfill promises related to the information provided by me	0.783			
	TRU3: I trust that websites keep my best interests in mind when dealing with my personal information	0.780			
	TRU4: Websites in general act as expected regarding the usage of my personal information	0.784			
	TRU5: Websites are always honest with customers when it comes to using their personal information	0.724			
<i>Willingness to disclose personal information (WDI)</i>	WDI1: It does not bother me when websites ask me for my personal information	0.771	0.878	0.867	0.628
	WDI2: I do not think twice when I provide my personal information to websites	0.803			
	WDI3: It does not bother me to give my personal information to so many websites	0.856			
	WDI4: I do not care whether websites collect too much personal information about me	0.733			

Note: *The item PC1-4 was excluded after the average variance extracted (AVE) of the construct PC1 presented a value lower than 0.50
Source: Table by authors

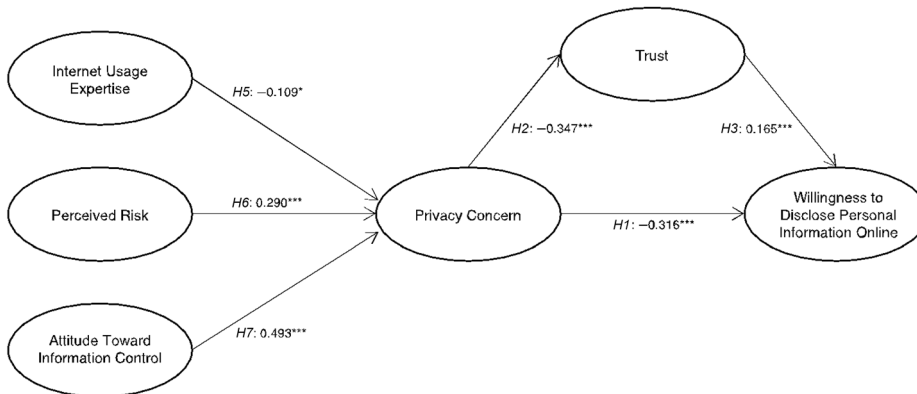
Constructs	IUE	Fornell–Larcker criterion					
		PR	AIC	PC1	PC2	TRU	WDI
IUE	0.655						
PR	0.020	0.565					
AIC	0.001	0.208	0.613				
PC1	0.006	0.061	0.063	0.514			
PC2	0.002	0.030	0.126	0.112	0.628		
TRU	0.005	0.018	0.022	0.065	0.048	0.573	
WDI	0.011	0.135	0.069	0.001	0.034	0.081	0.628
Average	5.457	5.157	6.067	5.435	6.462	3.039	2.184
Standard deviation	1.048	1.348	1.090	1.288	0.981	1.256	1.312

Fundamentalist,
pragmatic or
unconcerned

41

Notes: PC = privacy concern; TRU = trust; WDI = willingness to disclose information online; IUE = internet usage expertise; PR = perceived risk; AIC = attitude toward information control
Source: Table by authors

Table 2.
Discriminant validity



Notes: *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$
Source: Figure by authors

Figure 2.
Structural equation modeling

$\beta_{TRU \rightarrow WDI} = 0.194, p = 0.000$) and nonsignificant for pragmatics ($\beta_{PC \rightarrow TRU} = -0.165, n.s.$; $\beta_{TRU \rightarrow WDI} = 0.118, n.s.$) and unconcerned consumers ($\beta_{PC \rightarrow TRU} = 0.256, n.s.$; $\beta_{TRU \rightarrow WDI} = 0.162, n.s.$).

The determination coefficients (R^2) analysis across the three groups showed that the model is more suitable for pragmatic consumers. PC is explained by 39.6% of its regressions. In comparison, the variation of WDI is predicted by 34.5% of the model.

5. Discussion

Drawing on the literature review of information privacy, we proposed investigating the drivers of consumers' willingness to disclose information online. In addition, to the best of the authors' knowledge, the authors are the first to rescue Westin's attitudinal categories toward privacy (2003) to take them as moderators of a comprehensive model that explains consumers' general information disclosure on the internet.

All hypotheses were supported, showing that consumers' internet usage expertise, perceived risk and attitude toward information control drive PCs. PC affects consumers' willingness to disclose personal information online, and this relationship is mediated by trust.

Considering the antecedents of PCs, the results indicate that internet usage expertise negatively influences PCs, corroborating [Dinev and Hart \(2005\)](#), [Lopez-Nicolas and Molina-Castillo \(2008\)](#) and [Zhou \(2020\)](#). We also observed the positive influence of the perceived risk on PCs, confirming the findings of [Chang et al. \(2016\)](#), [Malhotra et al. \(2004\)](#) and [Youn \(2009\)](#). Finally, corroborating with [Anic et al. \(2019\)](#) and [Taylor et al. \(2009\)](#), the perceived risk positively influences PCs. Our research innovates in analyzing these three constructs simultaneously as antecedents of PC, and they explain 33.9% of the variation of this variable ($R^2 = 0.339$).

Our results indicate that PC significantly and negatively influences willingness to disclose personal information online, corroborating [Bandyopadhyay and Bandyopadhyay \(2018\)](#) and [Milne and Culnan \(2004\)](#). Furthermore, confirming the results of [Keher et al. \(2015\)](#), PC negatively influences trust. Trust positively influences consumers' willingness to disclose personal information online, according to [Kim et al. \(2019\)](#). We also advance by showing that trust mediates the relationship between PCs and consumers' willingness to disclose personal information online.

Notwithstanding, the most innovative aspect of this study is showing that Westin's attitudinal categories toward privacy (fundamentalist, unconcerned and pragmatic) moderate the relationships posited in the structural model proposed. Our results indicated the moderating role of the attitudinal categories toward privacy in all the relationships. However, moderation occurred differently among the three Westin categories. All the six

Hypotheses	Paths	Coeff.	Errors	Std. coeff.	<i>t</i>	<i>p</i> -value	Results
<i>H1</i>	PC → WDI	-1.010	0.220	-0.316	-4.583	0.000	Supported
<i>H2</i>	PC → TRU	-1.000	0.196	-0.347	-5.092	0.000	Supported
<i>H3</i>	TRU → WDI	0.183	0.049	0.165	3.719	0.000	Supported
<i>H5</i>	IUE → PC	-0.051	0.024	-0.109	-2.117	0.034	Supported
<i>H6</i>	PR → PC	0.093	0.020	0.290	4.704	0.000	Supported
<i>H7</i>	AIC → PC	0.192	0.030	0.493	6.376	0.000	Supported

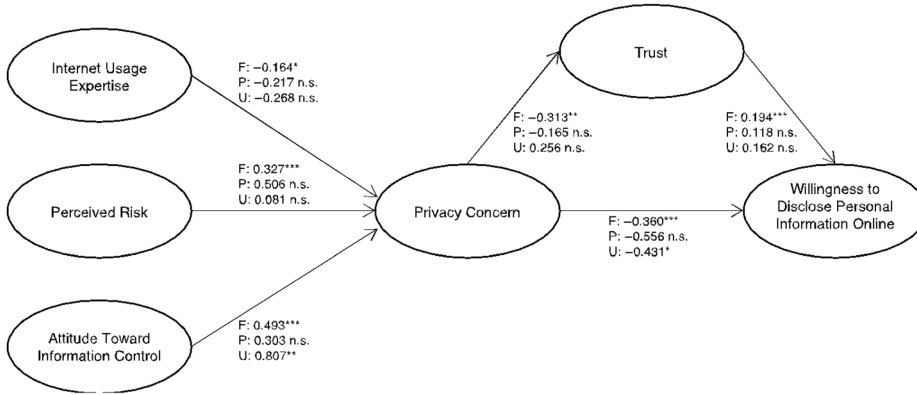
Table 3.
Structural model
estimates

Notes: PC = privacy concern; TRU = trust; WDI = willingness to disclose information online; IUE = internet usage expertise; PR = perceived risk; AIC = attitude toward information control
Source: Table by authors

<i>H4</i>	PC → TRU → WDI	β	Total, direct and indirect effects			<i>p</i> -values	Results
			Standardized error	CI 95% inferior	CI 95% superior		
Total effect		-0.373	0.074	-0.500	-0.212	0.009	Significant
Direct effect		-0.316	0.088	-0.474	-0.137	0.006	Significant
Indirect effect		-0.057	0.021	-0.098	-0.015	0.006	Significant

Table 4.
Mediation analysis

Notes: PC = privacy concern; TRU = trust; WDI = willingness to disclose information online
Source: Table by authors



Notes: F = fundamentalists; P = pragmatics; U = unconcerned; *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$

Source: Figure by authors

Figure 3.
Structural equation
modeling –
multigroup analysis

Group	Paths	Coeff.	Errors	Std. coeff.	<i>t</i>	<i>p</i> -values	Results
Fundamentalists (F)	PC → TRU	-1.800	0.557	-0.313	-3.229	0.001	Significant
	TRU → WDI	0.201	0.056	0.194	3.553	0.000	Significant
	PC → WDI	-2.141	0.643	-0.360	-3.330	0.000	Significant
	IUE → PC	-0.040	0.019	-0.164	-2.123	0.034	Significant
	PR → PC	0.056	0.028	0.327	3.298	0.000	Significant
Pragmatics (P)	AIC → PC	0.111	0.028	0.493	3.920	0.000	Significant
	PC → TRU	-6.375	22.154	-0.165	-0.288	0.774	Nonsignificant
	TRU → WDI	0.181	0.144	0.118	1.264	0.206	Nonsignificant
	PC → WDI	-33.013	112.214	-0.556	-0.294	0.769	Nonsignificant
	IUE → PC	-0.006	0.021	-0.217	-0.291	0.771	Nonsignificant
Unconcerned (U)	PR → PC	0.010	0.033	0.506	0.294	0.769	Nonsignificant
	AIC → PC	0.007	0.023	0.303	0.293	0.770	Nonsignificant
	PC → TRU	0.345	0.249	0.256	1.386	0.166	Nonsignificant
	TRU → WDI	0.201	0.188	0.162	1.074	0.283	Nonsignificant
	PC → WDI	-0.721	0.361	-0.431	-1.998	0.046	Significant
	IUE → PC	-0.188	0.130	-0.268	-1.447	0.148	Nonsignificant
	PR → PC	0.046	0.097	0.081	0.470	0.638	Nonsignificant
	AIC → PC	0.301	0.109	0.807	2.756	0.006	Significant

Notes: PC = privacy concern; TRU = trust; WDI = willingness to disclose information online; IUE = internet usage expertise; RP = perceived risk; AIC = attitude toward information control

Source: table by authors

Table 5.
Structural model
estimates –
multigroup analysis

relationships presented in the model were significant among fundamentalists – those with high levels of PC and who hardly provide their personal information.

Conversely, the pragmatics – who believe they can benefit by providing their personal information to companies but, at the same time, are concerned about how these companies use their data – did not moderate any of the model relationships. In the other extreme of attitude toward privacy, the group of unconcerned ones – those that have lower levels of PC and are more prone to provide their personal information to companies and

institutions – moderates two relationships (attitude toward information control and PC, and PC and willingness to disclose personal information online).

The relationships between internet usage expertise and PC, perceived risk and PC, PC and trust and trust and willingness to disclose information online are stronger among fundamentalists. Thus, the proposed model is more appropriate for those concerned about privacy.

6. Conclusion

Our contributions to the literature on information privacy are threefold. First, our proposed model explains the drivers of consumers' disposition to provide personal information at a level that surpasses specific contexts (Martin, 2018), bringing the analysis to consumers' level and considering their general perceptions toward data privacy. Second, our findings provide inputs to propose a better definition of Westin's attitudinal categories toward privacy, which used to be defined only by individuals' information privacy perception. As mentioned above, consumers' perceptions about their abilities in using the internet, the risks, their beliefs toward information control and trust also help to delimitate and distinguish the fundamentalists, the pragmatics and the unconcerned. Although Westin's studies have been widely referred to in different contexts, our proposed model is innovative in considering Westin's categories as moderators of the aspects influencing willingness to disclose personal information online. Finally, we also show that trust is a mechanism that explains the relationship between PCs and willingness to disclose information online.

PC emerges as an essential predictor of consumer trust and willingness to disclose their data online, and trust also influences this disposition. Managers need to implement actions that effectively reduce consumers' concerns about privacy and increase their trust in the company – for example, adopting a clear and transparent policy on how the data collected is stored, treated, protected and used to benefit the consumer. We also infer from the results that practitioners should be more attentive to consumers who have little experience with the internet since they tend to be more concerned with privacy and avoid contacting companies on the internet. Regarding the perception of risk, if managers convince consumers that the data collected on the internet is protected and will never be used in a way that harms them, they tend to be less concerned about privacy. The same occurs with the attitude toward information control. Managers need to clarify that the information collected will be used to enable benefits for consumers, providing personalized products and offers or even customized promotions. As privacy is a much-discussed topic today, we highlight the importance of companies segmenting their consumers considering their PCs. Those in the pragmatic category need more attention and more effective actions to convince them to make data available online.

In addition to the managerial implications, it is important to think about the political-legal aspect. Our results suggest different aspects influencing the willingness to disclose personal information online, including different responses considering consumers' PCs. Governments must be attentive to this aspect through their policies and legislation, establishing regulations that protect consumers' data in the virtual environment. In addition to regulatory policies, education campaigns can be carried out for both consumers and managers to raise the discussion about privacy and the availability of information in the online environment, demonstrating the importance of protecting personal data to benefit the government, consumers and organizations.

Some limitations weigh the theoretical and practical implications of this study. The sample size of pragmatic and unconcerned respondents was substantially smaller than that of fundamentalists. It might be explained by applying Westin's self-report index to classify

the groups according to their score regarding PCs. Most individuals affirm having a great concern for their data privacy but still provide online information for the benefit of personalization – known as the *privacy paradox* (Zeng, Ye, Li & Yang, 2021). This leads to another limitation of this research, given the lack of measures that classify respondents by considering their actual behavior toward privacy. Finally, the concept of trust is complex, and, in opting to use an unidimensional scale, we are not able to define the type of trust influencing the relationship between PC and willingness to disclose personal information online. In this research, we opted for the Malhotra et al. (2004) trust scale because it relies on the definition of trust as “the degree to which people believe a firm is dependable in protecting consumers’ personal information” (p. 341).

Future research should consider proposing and using behavioral measures associated with Westin’s attitudinal categories of privacy. We also recommend including other variables – such as perceived benefits of disclosing information online – to investigate the role of Westin’s attitudinal categories of privacy on consumers’ trade-off between privacy and personalization. Finally, we suggest cross-cultural studies, as our proposed model might vary according to individualistic versus collectivist cultures.

References

- Aguirre, E., Roggeveen, A. L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. *Journal of Consumer Marketing*, 33(2), 98–110, doi: <https://doi.org/10.1108/JCM-06-2015-1458>.
- Aloysius, J. A., Hoehle, H., & Venkatesh, V. (2016). Exploiting big data for customer and retailer benefits: a study of emerging mobile checkout scenarios. *International Journal of Operations & Production Management*, 36(4), 467–486, doi: <https://doi.org/10.1108/IJOPM-03-2015-0147>.
- Anic, I. D., Škare, V., & Milaković, I. K. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications*, 36, 100868, doi: <https://doi.org/10.1016/j.elerap.2019.100868>.
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13–28, doi: <https://doi.org/10.2307/25148715>.
- Bandyopadhyay, S., & Bandyopadhyay, K. (2018). How consumers in India react to online privacy concerns. *Journal of Competitiveness Studies*, 26(3-4), 183–194, <https://go.gale.com/ps/i.do?id=GALE%7CA588655392&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=23304103&p=AONE&sw=w&userGroupName=anon%7Ee5ddbcb7>
- Castañeda, J. A., & Montoro, F. J. (2007). The effect of internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7(2), 117–141, doi: <https://doi.org/10.1007/s10660-007-9000-y>.
- Chang, S. E., Shen, W. C., & Liu, A. Y. (2016). Why mobile users trust smartphone social networking services? A PLS-SEM approach. *Journal of Business Research*, 69(11), 4890–4895, doi: <https://doi.org/10.1016/j.jbusres.2016.04.048>.
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: an empirical examination of the online consumer’s dilemma. *Information Technology and Management*, 6(2-3), 181–2005, doi: <https://doi.org/10.1007/s10799-005-5879-y>.
- Chen, C. P., & Zhang, C. Y. (2014). Data-intensive applications, challenges, techniques, and technologies: a survey on big data. *Information Sciences*, 275, 314–347, doi: <https://doi.org/10.1016/j.ins.2014.01.015>.
- Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: from big data to big impact. *MIS Quarterly*, 36(4), 1165–1188, doi: <https://doi.org/10.2307/41703503>.

- Cisco. (2021). Consumer privacy survey: Building consumer confidence through transparency and control. Retrieved from www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf
- Dholakia, N., Darmody, A., Zwick, D., Dholakia, R. R., & Firat, A. F. (2021). Consumer choicemaking and choicelessness in hyperdigital marketplaces. *Journal of Macromarketing*, 41(1), 65–74, doi: <https://doi.org/10.1177/0276146720978257>.
- Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7–29, doi: <https://doi.org/10.2753/JEC1086-4415100201>.
- Dudley-Nicholson, J. (2018). Facebook users are deleting their accounts after it was revealed their data was used in the 2016 US election. 20 Match News Corp Australia Network. Retrieved from www.news.com.au/technology/online/social/facebook-users-are-deleting-their-accounts-after-it-was-revealed-their-data-was-used-in-the-2016-us-election/news-story/41a355e6846865ba37525624a98e2fb0
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.
- Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, 3(4), 2–16, doi: <https://doi.org/10.1109/COMST.2000.5340804>.
- Gandon, F. L., & Sadeh, N. M. (2004). Semantic web technologies to reconcile privacy and context awareness. *Journal of Web Semantics*, 1(3), 241–260, doi: <https://doi.org/10.1016/j.websem.2003.07.008>.
- Grosso, M., Castaldo, S., Li, H. A., & Larivière, B. (2020). What information do shoppers share? The effect of personnel-, retailer-, and country-trust on willingness to share information. *Journal of Retailing*, 96(4), 524–547, doi: <https://doi.org/10.1016/j.jretai.2020.08.002>.
- Hair, J. F., Gabriel, M. L., & Patel, V. K. (2014). Modelagem de equações estruturais baseada em covariância (CB-SEM) com o AMOS: Orientações sobre a sua aplicação como uma ferramenta de pesquisa de marketing. *Revista Brasileira de Marketing*, 13(2), 44–55, doi: <https://doi.org/10.5585/remark.v13i2.2718>.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*, 7th Edition, NJ: Prentice Hall.
- Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: the case of the Facebook news feed privacy outcry. *Electronic Commerce Research and Applications*, 9(1), 50–60, doi: <https://doi.org/10.1016/j.eierap.2009.05.001>
- Ingram, D. (2018). Facebook says data leak hits 87 million users, widening privacy scandal. Reuters, 4 April. Retrieved from www.reuters.com/article/us-facebook-privacy-idUSKCN1HB2CM
- Kasper, D. V. S. (2005). The evolution (or devolution) of privacy. *Sociological Forum*, 20(1), 60–92, doi: <https://doi.org/10.1007/s11206-005-1898-z>.
- 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, doi: <https://doi.org/10.1111/isj.12062>.
- Kim, M. S., & Kim, S. (2018). Factors influencing willingness to disclose personal information for personalized recommendations. *Computers in Human Behavior*, 88, 143–152, doi: <https://doi.org/10.1016/j.chb.2018.06.031>.
- Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to disclose personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92, 273–281, doi: <https://doi.org/10.1016/j.chb.2018.11.022>.
- Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: a survey of westin's studies*, Pittsburgh, PA: Institute for Software Research International.

- Lin, S. W., & Liu, Y. C. (2012). The effects of motivations, trust, and privacy concern in social networking. *Service Business*, 6(4), 411–424, doi: <https://doi.org/10.1007/s11628-012-0158-6>.
- Lopez-Nicolas, C., & Molina-Castillo, F. J. (2008). Customer knowledge management and E-Commerce: the role of customer perceived risk. *International Journal of Information Management*, 28(2), 102–113, doi: <https://doi.org/10.1016/j.ijinfomgt.2007.09.001>.
- Mai, J. E. (2016). Big data privacy: the datafication of personal information. *The Information Society*, 32(3), 192–199, doi: <https://doi.org/10.1080/01972243.2016.1153010>.
- 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. Retrieve from www.jstor.org/stable/23015787 doi: <https://doi.org/10.1287/isre.1040.0032>.
- Manovich, L. (2012). Trending: the promises and the challenges of big social data. In M. Gold, (Ed.) *Debates in the digital humanities*, pp. 460–475. Minneapolis, MN: University of MN Press.
- Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, 59(2), 243–261, doi: <https://doi.org/10.1111/1540-4560.00063>.
- Markman, J. (2017). Amazon using AI, big data to accelerate profits. Forbes. 5 June. Retrieved from www.forbes.com/sites/jonmarkman/2017/06/05/amazon-using-ai-big-data-to-accelerate-profits/?sh=2e1981d06d55
- Marr, B. (2017). Want to use big data? Why not start via google, Facebook, amazon, (etc.). Forbes, 14 August. Retrieved from www.forbes.com/sites/bernardmarr/2017/08/14/want-to-use-big-data-why-not-start-via-google-facebook-amazon-etc/?sh=78bf18d3d5db
- Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, 82, 103–116, doi: <https://doi.org/10.1016/j.jbusres.2017.08.034>.
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155, doi: <https://doi.org/10.1007/s11747-016-0495-4>.
- Martinez-Lopez, F. J., Pla-Garcia, C., Gázquez-Abad, J. C., & Rodríguez-Ardura, I. (2014). Utilitarian motivations in online consumption: Dimensional structure and scales. *Electronic Commerce Research and Applications*, 13(3), 188–204, doi: <https://doi.org/10.1016/j.elerap.2014.02.002>.
- Michael, K., & Miller, K. W. (2013). Big data: New opportunities and new challenges. *Computer*, 46(6), 22–24, doi: <https://doi.org/10.1109/MC.2013.196>.
- Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15–29, doi: <https://doi.org/10.1002/dir.20009>.
- Moore, A. (2008). Defining privacy. *Journal of Social Philosophy*, 39(3), 411–428, doi: <https://doi.org/10.1111/j.1467-9833.2008.00433.x>.
- Mourey, J. A., & Waldman, A. E. (2020). Past the privacy paradox: the importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research*, 5(2), 162–180. Retrieved from www.journals.uchicago.edu/doi/abs/10.1086/708034, doi: <https://doi.org/10.1086/708034>.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*, Stanford, CA: Stanford Law Books.
- Ohanian, R. (1990). Construction and validation of a scale to measure celebrity endorsers' perceived expertise, trustworthiness, and attractiveness. *Journal of Advertising*, 19(3), 39–52, doi: <https://doi.org/10.1080/00913367.1990.10673191>.
- Park, C., & Jun, J. K. (2003). A cross-cultural comparison of internet buying behavior: the effects of internet usage, perceived risks, and innovativeness. *International Marketing Review*, 20(5), 534–553, doi: <https://doi.org/10.1108/02651330310498771>.

- Pentland, A. (2013). The Data-Driven society. *Scientific American*, 309(4), 78–83. Retrieved from www.jstor.org/stable/26018109
- Pérez-Cabañero, C. (2007). Perceived risk on goods and service purchases. *EsicMarket*, 129, 193–199.
- Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to disclose personal information. *Journal of Public Policy & Marketing*, 19(1), 27–41, doi: <https://doi.org/10.1509/jppm.19.1.27.16941>.
- Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: socio-demographic and attitudinal influences on privacy and disclosure choices. *Journal of Marketing Management*, 36(5-6), 519–549, doi: <https://doi.org/10.1080/0267257X.2020.1715465>.
- Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: the role. *Of Information Sensitivity and Trust in Reducing Medical Information Privacy Concern*. *Journal of Business Research*, 57(9), 1000–1011, doi: [https://doi.org/10.1016/S0148-2963\(02\)00345-4](https://doi.org/10.1016/S0148-2963(02)00345-4).
- Schifferle, L. W. (2016). Online tracking – more than cookies. Federal Trade Commission: Consumer Information, 23 June. Retrieved from www.consumer.ftc.gov/blog/2016/06/online-tracking-more-cookies
- Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to disclose information in Database-Driven relationship marketing. *Journal of Interactive Marketing*, 16(3), 2–16, doi: <https://doi.org/10.1002/dir.10033>.
- Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM*, 46(4), 91–94, doi: <https://doi.org/10.1145/641205.641211>.
- Solove, D. J. (2008). *Understanding privacy*, Cambridge (MA: Harvard University Press).
- 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. Retrieved from www.jstor.org/stable/43825785 doi: <https://doi.org/10.25300/MISQ/2013/37.4.07>.
- Swani, K., Milne, G. R., & Slepchuk, A. N. (2021). In press). revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: Replication and extension. *Journal of Interactive Marketing*, 56, doi: <https://doi.org/10.1016/j.intmar.2021.03.001>.
- Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: the moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3), 203–223, doi: <https://doi.org/10.1007/s10660-009-9036-2>.
- Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, 136, 76–85, doi: <https://doi.org/10.1016/j.jbusres.2021.07.031>.
- Weiyo, H., Hietanen, J., & Matilla, P. (2014). New insights into online consumption communities and netnography. *Journal of Business Research*, 67(10), 2072–2078, doi: <https://doi.org/10.1016/j.jbusres.2014.04.015>.
- Westin, A. F. (1967). *Privacy and freedom*, New York, NY: Atheneum.
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431–453, doi: <https://doi.org/10.1111/1540-4560.00072>.
- Willis, B., Jai, T., & Lauderdale, M. (2021). Trust and commitment: Effect of applying consumer data rights on US consumers' attitudes toward online retailers in the big data era. *Journal of Consumer Behaviour*, 20(6), 1575–1590, doi: <https://doi.org/10.1002/cb.1968>.
- Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889–897, doi: <https://doi.org/10.1016/j.chb.2011.12.008>.
- Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters*, 17(1), 61–74, doi: <https://doi.org/10.1007/s11002-006-4147-1>.

-
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389–418, doi: <https://doi.org/10.1111/j.1745-6606.2009.01146.x>.
- Zeng, F., Ye, Q., Li, J., & Yang, Z. (2021). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research*, 124, 667–675, doi: <https://doi.org/10.1016/j.jbusres.2020.02.006>.
- Zhou, T. (2020). The effect of information privacy concern on users' social shopping intention. *Online Information Review*, 44(5), doi: <https://doi.org/10.1108/OIR-09-2019-0298>.
- Zwitter, A. (2014). Big data ethics. *Big Data & Society*, 1(2), 1–6, doi: <https://doi.org/10.1177/2053951714559253>.

Author contribution: Renata Monteiro Martins – CRediT roles: Data curation; Formal analysis; Investigation; Methodology; Conceptualization; Software; Visualization; Validation; Roles/Writing – original draft; Writing – review & editing.

The author contributed to the conception and design of the study, acquisition of data, analysis, and interpretation of data, including drafting the article and revising it critically for important intellectual content.

Sofia Batista Ferraz – CRediT roles: Formal analysis; Investigation; Validation; Project administration; Resources; Roles/Writing – original draft; Writing – review & editing.

The author contributed to the analysis and interpretation of data, including drafting the article and revising it critically for important intellectual content.

André Francisco Alcântara Fagundes – CRediT roles: Formal analysis; Roles/Writing – original draft.

The author contributed to reviewing, editing, and revising the article critically for important intellectual content.

Corresponding author

Sofia Batista Ferraz can be contacted at: sofiabf@gmail.com

Associate editor: Otavio Freire

For instructions on how to order reprints of this article, please visit our website:

www.emeraldgrouppublishing.com/licensing/reprints.htm

Or contact us for further details: permissions@emeraldinsight.com