



Article

# Structural Heterogeneity in the Privacy Calculus Across Perceived Privacy Control Groups: Evidence from E-Commerce Information Disclosure

Mohamed Oubal <sup>1,\*</sup> , Abdelouahab El Boukhari <sup>2</sup> , Hicham Faouzi <sup>3</sup> and Slimane Ed-Dafali <sup>4,\*</sup>

<sup>1</sup> ESSEM Business School, Casablanca 20140, Morocco

<sup>2</sup> Faculty of Legal, Economic, and Social Sciences, Cadi Ayyad University, Marrakech 40000, Morocco; a.elboukhari@uca.ac.ma

<sup>3</sup> National School of Business and Management, Ibn Tofail University, University Campus, Kenitra 14000, Morocco; hicham.faouzi@uit.ac.ma

<sup>4</sup> Ecole Nationale de Commerce et de Gestion, Chouaib Doukkali University, El Jadida 24000, Morocco

\* Correspondence: oubalmohamed@gmail.com (M.O.); ed-dafali.s@ucd.ac.ma (S.E.-D.)

## Abstract

Consumer self-disclosure remains a central question in digital markets, as e-commerce participation increasingly depends on voluntary personal information sharing. Despite extensive application of privacy calculus theory, empirical findings regarding privacy concerns, trust, and perceived risk remain inconsistent, suggesting that the structural relationships underlying privacy trade-offs may vary across consumers and contexts. This study examines how privacy concerns, perceived benefits, perceived risk, and trust relate to perceived risk and personal information disclosure intention in e-commerce, and whether these structural relationships differ between consumers with higher and lower perceived privacy control (PPC). Survey data from 743 online consumers were analyzed using partial least squares structural equation modeling and multigroup comparisons between consumers with high and low perceived privacy control. Findings show privacy concerns do not directly inhibit disclosure intention; instead, they are strongly associated with perceived risk, which is negatively associated with disclosure intention. The results reveal a separation between benefit and risk appraisal: perceived benefits motivate disclosure intention but do not significantly reduce perceived risk. The multigroup results reveal significant structural differences between the relatively high- and low-PPC groups. In the relatively high-PPC group, the relationship between perceived benefits and disclosure intention is stronger, as is the negative relationship between trust and perceived risk. In the relatively low-PPC group, perceived risk exerts a stronger inhibiting effect, while trust assumes a compensatory role, helping consumers navigate limited agency. By identifying structural heterogeneity in the privacy calculus across PPC groups, this study explains variations in disclosure decisions and clarifies inconsistent findings in prior research.

**Keywords:** privacy calculus; privacy concerns; perceived privacy control; personal information disclosure; e-commerce; emerging markets; trust



Academic Editors:

Muhammad Aljukhadar, Mohamad Amir Merhabi, Yaozhi Zhang and Sandreen Hitti

Received: 11 August 2026

Revised: 1 September 2026

Accepted: 1 September 2026

Published: 8 September 2026

**Copyright:** © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

## 1. Introduction

The rapid expansion of digital platforms and e-commerce has transformed personal data into a key resource of the digital economy [1]. Online services increasingly rely on the collection and analysis of user information to deliver personalized experiences, optimize

transactions, and improve service efficiency. Personal data enable recommendation systems, targeted marketing, and customized services that enhance the value of digital interactions for both firms and consumers [2]. Consequently, participation in many online services now requires users to disclose personal information (PI) such as identity details, contact information, or payment data. In this environment, voluntary disclosure of PI has become a central mechanism enabling digital economic exchanges [3,4]. While these practices create value for firms and users, they also raise concerns regarding privacy, data governance, and the potential misuse of PI.

Morocco provides a particularly relevant empirical setting for examining privacy-related disclosure in e-commerce [5,6]. The ANRT's 2024–2025 national ICT survey reports 3.7 million additional online buyers between 2019 and 2024, representing a 65% increase [6]. This rapid expansion of digital commerce is accompanied by growing concerns about security and personal information exposure. Visa's Stay Secure Study 2025 found that 56% of Moroccan respondents had reduced their use of digital payments because of news about cyberfraud, including data breaches, email scams, and phishing [7]. More recently, Visa's 2026 Stay Secure Study reported that 30% of surveyed Moroccan consumers had experienced a financial scam during the previous 12 months, while 64% indicated that real-time alerts for suspicious transactions would make them feel more secure when paying online [8]. Kaspersky also reported identifying on the dark web more than 2.1 million compromised credentials associated with Moroccan users or digital resources [9]. These indicators highlight the coexistence of rapidly expanding digital commerce with persistent security and privacy-related vulnerabilities, reinforcing the importance of understanding how consumers evaluate risk, trust, and control when deciding whether to disclose personal information online.

Privacy has traditionally been understood as the individual's ability to regulate the boundaries between the private self and interactions with others [10]. In digital environments, this boundary management becomes particularly complex because PI can be easily collected, stored, and reused by organizations. Communication privacy management theory suggests that individuals constantly seek a balance between disclosing information and protecting their private sphere [11]. This tension is especially salient in e-commerce, where firms rely heavily on personal data to deliver personalized products and services. At the same time, individuals increasingly perceive risks associated with the collection and use of their data. Farooq et al. [12] report that many users perceive their PI as increasingly insecure and express concerns about the misuse of their data, particularly regarding platforms collecting and using PI without their knowledge across MENA countries, including Morocco. Despite these concerns, individuals continue to share PI when interacting with digital platforms.

This apparent contradiction between expressed privacy concerns and actual disclosure behavior has been widely discussed in the literature as the privacy paradox [13]. To explain this phenomenon, many studies rely on the privacy calculus framework, later operationalized through the Privacy Calculus Model (PCM) [14], which conceptualizes disclosure decisions as the outcome of a cognitive evaluation of expected benefits and perceived risks. According to this perspective, individuals are willing to disclose PI when the perceived benefits of disclosure outweigh the perceived risks associated with potential privacy loss [4]. In this sense, individuals may accept a certain degree of privacy loss in exchange for utilitarian or experiential benefits derived from digital services [3]. Such evaluations are not static; they evolve as individuals acquire new information and reassess the balance between perceived risks and benefits, which helps explain the continued relevance of this framework in a context marked by the rapid expansion of digital technologies and online services [15,16].

Beyond this benefit–risk evaluation, several additional factors influence how individuals make disclosure decisions. Prior research has highlighted the importance of perceived benefits, perceived risk, privacy concerns, and trust in shaping individuals’ willingness to disclose PI in online environments [17,18]. Within this decision process, perceived privacy control (PPC) has received increasing attention. PPC refers to individuals’ belief that they can manage how their PI is collected, used, or shared [19]. When individuals perceive greater control over their PI, they may feel less vulnerable to potential misuse and therefore evaluate disclosure decisions differently [20]. However, PPC has predominantly been examined as an antecedent of privacy-related outcomes, while comparatively limited attention has been paid to whether the structural relationships among the core mechanisms of the privacy calculus differ across consumers reporting relatively high and low PPC. Addressing this issue is important because inconsistent findings regarding privacy concerns, perceived risk, perceived benefits, and trust may reflect not only contextual differences but also variation in the extent to which consumers perceive control over their personal information.

The current literature gap is further accentuated by the contextual concentration of empirical evidence. Existing reviews and meta-analyses show that privacy-related disclosure findings are sensitive to contextual moderators such as country, cultural background, and platform type [21,22]. Consequently, relatively little is known about the antecedents of individuals’ self-disclosure decisions in emerging digital economies, particularly in the Middle East and North Africa (MENA) region. This gap is important because cultural attitudes toward privacy, trust in institutions, and digital literacy may vary across institutional and socio-cultural environments [5]. Morocco provides a relevant setting to explore these dynamics, as it has experienced substantial growth in internet penetration, mobile connectivity, and online commerce [5,6]. Although the country has established a formal personal data protection framework through Law No. 09-08 and the National Commission for the Protection of Personal Data, privacy governance and consumer awareness continue to evolve alongside digital commerce [5]. These characteristics make Morocco a theoretically relevant empirical context for examining privacy-related disclosure decisions in a rapidly developing MENA digital economy.

This gap motivates the present study because understanding whether the relative importance of risks, benefits, and trust differs between consumers reporting relatively high and low PPC can help explain why privacy-calculus relationships have produced heterogeneous findings across prior studies. Examining this issue in Morocco is particularly relevant given the simultaneous expansion of e-commerce and the growing exposure of consumers to digital security and privacy risks, providing an opportunity to assess whether privacy-calculus relationships differ across consumers reporting different levels of perceived informational agency in an emerging digital market. Accordingly, this study addresses the following research question: *To what extent do privacy concerns, perceived benefits, perceived risk, and trust explain personal information disclosure intention in e-commerce, and how do these relationships differ between consumers with higher and lower perceived privacy control?*

The purpose of this study is therefore to examine how global information privacy concern, perceived benefits, perceived risk, and trust relate to perceived risk and personal information disclosure intention in e-commerce, and whether these structural relationships differ between consumers with higher and lower PPC. To address this objective, survey data from 743 Moroccan online consumers are analyzed using partial least squares structural equation modeling (PLS-SEM), followed by the Measurement Invariance of Composite Models (MICOM) procedure and multigroup analysis (MGA). PLS-SEM enables the simultaneous assessment of the theoretically specified relationships among latent constructs,

while MICOM establishes whether sufficient measurement invariance exists for meaningful group comparisons. MGA then allows the structural path coefficients to be compared directly between consumers with high and low PPC. Together, these procedures provide an appropriate analytical framework for examining whether the structural path coefficients differ between the relatively high- and low-PPC groups.

This study makes three main contributions to the privacy calculus literature. First, it extends the role of perceived privacy control beyond its conventional treatment as an antecedent of privacy-related perceptions by examining structural heterogeneity in privacy-calculus relationships across relatively high- and low-PPC consumers. Second, it provides a more differentiated account of the privacy calculus by showing that the relative importance of these mechanisms varies between consumers reporting comparatively higher and lower levels of PPC. The multigroup results reveal distinct configurations: benefit-driven disclosure is more pronounced among consumers reporting higher PPC, whereas risk-related mechanisms carry greater weight among those reporting lower PPC, with trust assuming different roles depending on the group. Third, the study extends the empirical scope of privacy calculus research to Morocco, an underrepresented North African and MENA e-commerce context, thereby providing evidence from an institutional and digital environment that remains insufficiently represented in the literature.

## 2. Literature Review and Hypothesis Development

### 2.1. Global Information Privacy Concern

Privacy concerns are conceptualized in the literature as broad, data-oriented apprehensions reflecting individuals' general unease about how organizations collect, use, and share personal data [4,18,23]. Rather than being reducible to perceived risk or simple emotional anxiety, they represent a stable cognitive disposition that informs how individuals interpret and evaluate potential risks in specific online transactions. These concerns are primarily directed at specific data-related practices in e-commerce, such as profiling, cross-site tracking, payment processing, or third-party data sharing, rather than at operational issues such as transaction failure or product quality inconsistencies [24,25].

Early empirical research placed privacy concerns within a broader benefit–risk–trust triad. Liu et al. [25] show that privacy-related beliefs influence trust in e-commerce websites, while Kim et al. [26] argue that trust mitigates perceived risk and facilitates behavioral engagement. These findings highlight that privacy concerns do not operate in isolation but interact with trust and risk within digital decision-making processes. Dinev and Hart [27] consolidated these perspectives into an extended PCM, which treats privacy concerns and perceived risk as interrelated inhibitors of intention: both exert a negative effect on online transaction intention, whereas perceived benefits and trust play a positive role.

Recent literature reviews further cement this centrality in e-commerce settings, albeit with significant variability and context dependency. In their multilevel meta-analysis, Maseeh et al. [21] reported a robust negative association between privacy concerns and both attitudes toward e-commerce platforms and actual usage behavior, while highlighting substantial heterogeneity in effect sizes across studies and contexts. In their comprehensive systematic review, Kolotylo-Kulkarni et al. [28] identified perceived benefits, perceived risk, trust, and privacy concerns as increasingly recurrent antecedents of disclosure decisions. They noted, however, that prior research rarely separates data-specific concerns from overall risk, and the underlying conditions where trust may compensate for high levels of concern are not specified. Bandara et al. [24] add to this picture by proposing a taxonomy showing that consumers differentiate between concerns related to data collection, secondary use, surveillance and loss of control, and by arguing that these dimensions are activated differently depending on the platform and the institutional context.

The relationship between privacy concerns and perceived risk has been theoretically and empirically established across multiple frameworks. Kehr et al. [29] and Malhotra et al. [17] position privacy concerns as a key driver of perceived risk in online transactions, arguing that individuals with heightened concerns about data-related practices are more likely to interpret disclosure requests as risky. Their findings demonstrate that privacy concerns exert a positive effect on perceived risk, which in turn negatively influences disclosure intention. This mechanism reflects a cognitive amplification process: stable privacy concerns, shaped by cumulative prior experiences and awareness, serve as interpretive lenses through which consumers evaluate specific transaction contexts. When confronted with a disclosure decision in e-commerce, individuals with higher privacy concerns are predisposed to appraise the situation as riskier, even when the objective characteristics of the transaction remain constant [30].

With respect to consequences, prior research shows that privacy concerns significantly influence individuals' disclosure intention in online environments. Meta-analytic evidence indicates that higher concern levels are associated with lower e-commerce usage, greater reluctance to disclose PI, and stronger adoption of privacy-protective behaviors, such as providing incomplete or inaccurate data or avoiding certain transactions [21]. Olivero and Lunt [31] further demonstrate that when consumers become more aware of online data collection and profiling, they tend to renegotiate the terms of exchange, demanding more control or explicit compensation for disclosure and may withhold or distort the information provided. Privacy concerns therefore influence both whether consumers disclose information and how they disclose when they decide to transact. Based on the foregoing, we propose the following hypotheses:

**H1.** *Global information privacy concern regarding e-commerce websites positively influences consumers' perceived risk related to personal information disclosure intention.*

**H2.** *Global information privacy concern regarding e-commerce websites negatively influences consumers' intention to disclose personal information.*

## 2.2. Perceived Benefits

Perceived benefits refer to individuals' evaluation of the value they expect to derive from disclosing PI. They represent the anticipated gains or gratifications associated with information disclosure [32], and can be understood as the expected return of disclosure [33]. In this sense, perceived benefits capture the potential advantages individuals believe may result from providing their data, whether framed as the potential gains of information disclosure [22] or as consumers' assessment of what they stand to gain from engaging in digital interactions [34,35]. Perceived benefits encompass both functional and psychological gains associated with information disclosure. According to Ryu and Park [36], the positive outcomes of PI disclosure generally fall into two main categories: financial rewards, such as targeted discounts, and functional advantages, which provide users with customized services, interactivity, and highly relevant, just-in-time information. Furthermore, these benefits are not purely functional but may also involve enjoyment, social interaction, and emotional value [37]. Empirically, perceived benefits have a consistent and highly significant positive impact on an individual's intention to disclose PI across various digital contexts, including mobile applications, e-commerce, and social networking sites. For instance, Wang et al. [38] demonstrated that perceived benefits are positively related to the intention to disclose PI. A meta-analysis synthesizing results from 48 studies found that perceived benefit was the strongest positive factor influencing online information disclosure intention [22].

From a privacy calculus perspective, disclosure decisions reflect a trade-off between benefits and perceived risks [39]. Perceived benefits are therefore a core component of this framework, capturing the motivational value that can encourage disclosure when expected gains outweigh potential losses. In e-commerce, where transactions require personal data and occur without physical verification, this evaluation becomes especially salient. Furthermore, individuals also consider the degree of control they retain as information crosses personal boundaries, since risk and control jointly shape whether disclosure is judged worthwhile [19]. Empirically, perceived benefits tend to exert a stronger influence on disclosure intentions than perceived risks [38]. This asymmetry can be explained through several mechanisms such as economic incentives and convenience that may directly lower perceived risks [40]. In some cases, individuals focus almost entirely on benefits, particularly when immediate gratification is involved [41], and the gains from disclosure may even compensate for the loss of privacy, encouraging data sharing despite potential risks [27]. Therefore, we hypothesize that:

**H3.** *Perceived benefits positively influence consumers' intention to disclose personal information.*

**H4.** *Perceived benefits negatively influence consumers' perceived risk related to personal information disclosure intention.*

### 2.3. Perceived Risks

The Internet is widely characterized as a risk-laden environment in which users must make decisions under uncertainty, with prior research describing everyday online actions as inherently risky [27]. At a broad level, perceived risk refers to the subjective belief that an event may lead to unwanted or negative consequences [42]. In the online context, this captures users' concerns about potential losses resulting from sharing PI, including uncertainty about what might happen to their data [30,43,44]. Such losses may take various forms, including economic harm, misuse of payment information, identity theft, or unauthorized sharing of personal details with third parties [5,44]. In e-commerce specifically, where PI must be disclosed to complete transactions, perceived risk reflects the possibility that such disclosure may lead to misuse, unauthorized access, or loss of control over personal data. When disclosing information online, users mentally weigh the likelihood that their data could be exploited against the expected benefits of participating [45]. Perceived risks are thus not objective facts but subjective assessments of the likelihood and severity of potential losses, often linked to fears of opportunistic behavior by service providers or online sellers.

In privacy calculus, consumers weigh the potential benefits of sharing data against possible costs, such as privacy invasion or financial loss [44,46]. Perceived risks are repeatedly identified as strong inhibitors of the intention to disclose data, with higher levels thereof associated with a greater likelihood of refusing to share information or engaging in privacy-protective behaviors [44,46]. Empirical studies in e-commerce contexts consistently indicate that higher levels of perceived risk are associated with lower intention to share PI and engage in online transactions. Building on these findings, this study hypothesizes that:

**H5.** *Perceived risk negatively influences consumers' intention to disclose personal information.*

### 2.4. Trust in E-Commerce Websites

Trust is commonly defined as the intention to accept vulnerability based on positive expectations regarding another party's behavior [47]. In e-commerce contexts, it reflects consumers' belief that an e-commerce website is reliable, competent, and will not misuse their PI [17]. Because online transactions involve uncertainty and limited control, trust func-

tions as a psychological mechanism that reduces perceived risk and facilitates engagement in digital interactions [42,48].

Trust is widely recognized as a central condition for consumers' intention to share personal data in e-commerce environments. When consumers trust an e-commerce website, they are more inclined to agree to provide PI such as contact details, demographic information, or payment details [37,49]. In this context, trust is often conceptualized as a form of "trusting intention," that is, a person's intention to rely on another party and to deliberately accept a situation of vulnerability toward that party [50]. Disclosing PI online is therefore not a neutral act; it is a trust-related behavior in which the consumer allows the vendor to access and use data that could potentially be misused.

A large body of empirical work consistently shows that higher levels of trust are associated with a greater intention to disclose PI in online transactions, suggesting that when consumers trust an e-commerce website, they are more likely to engage in self-disclosure [51,52]. This vulnerability is particularly evident when consumers provide shipping addresses, which exposes them to potential privacy intrusions, or credit card details, creating a risk of financial fraud. Beyond its direct effect on disclosure, trust also serves as a risk-reducing mechanism: when consumers believe that an e-commerce website is reliable, they tend to perceive lower levels of privacy risk [5,26,42]. Conversely, when consumers perceive online vendors as opportunistic or unpredictable, their trust diminishes, which heightens perceived risk and in turn lowers their intention to share personal data or engage in e-commerce activities [5,53]. In line with this, we hypothesize that:

**H6.** *Trust in e-commerce websites negatively influences consumers' perceived risk related to personal information disclosure.*

**H7.** *Trust in e-commerce websites positively influences consumers' intention to disclose personal information.*

### 2.5. Structural Heterogeneity Across PPC Groups

Privacy scholarship has long placed control at the center of informational privacy. Westin [54] (p. 7) defined privacy as the ability of individuals to control "when, how, and to what extent" information about them is shared, while Altman [10] (p. 18) described it as "the selective control of access to the self," emphasizing the flexible management of personal boundaries. Building on these foundations, Xu et al. [19] note that privacy is often defined through the notion of control, or that control is treated as a key determinant of privacy concerns. This view was further refined by Xu et al. [55], who distinguish between personal control and proxy control, meaning that control may be exercised either directly by individuals or indirectly through external organizations acting on their behalf.

At the individual level, PPC is shaped by situational cues such as the transparency of privacy information, the optionality of data requested, the interface design, and the options available to manage personal data. In this research, PPC refers to perceived control over the disclosure and use of PI, reflecting the influence consumers feel they have over data held by online merchants and their ability to limit how this information is accessed or disseminated. Malhotra et al. [17] note that mechanisms enhancing this sense of control, such as fair data-handling procedures or privacy setting options, shape consumers' evaluations of justice and fairness without creating control by themselves.

Early measurement approaches incorporated control as a dimension of privacy concern itself [23], but subsequent research treats PPC as a related yet distinct belief reflecting individuals' perceived agency over personal data flows [56]. To date, PPC has been examined primarily as an antecedent: Rodríguez-Priego et al. [57] show that it lowers

privacy concerns and reinforces trusting beliefs, while Tao et al. [58] found that it reduces privacy concerns indirectly through trust in e-commerce websites. However, whether the structural relationships within the PCM differ according to consumers' perceived level of privacy control remains insufficiently examined. Rather than focusing solely on differences in construct levels, the present study examines whether the relative strength of the core privacy-calculus relationships varies according to perceived privacy control. Consumers reporting higher PPC may place greater weight on perceived benefits and online vendor trustworthiness because they experience a stronger sense of informational agency. Conversely, consumers reporting lower PPC may exhibit stronger risk-related relationships because they perceive less ability to manage the potential consequences of information disclosure.

**H8a.** *The relationship between global information privacy concern and intention to disclose personal information is stronger in the lower-PPC group than in the higher-PPC group.*

**H8b.** *The relationship between global information privacy concern and perceived risk is stronger in the lower-PPC group than in the higher-PPC group.*

The role of perceived benefits may likewise differ according to consumers' perceived level of privacy control. Consumers with higher PPC may perceive greater ability to manage their disclosed information and consequently experience lower privacy risk [59]. In such conditions, perceived benefits may become more influential in disclosure decisions, providing a theoretical basis for expecting the relationship between perceived benefits and disclosure intention to be stronger in the higher-PPC group. Similarly, a stronger sense of control may make benefit-related considerations more salient, providing a theoretical basis for expecting differences in the relationship between perceived benefits and perceived risk according to PPC levels [38].

**H8c.** *The relationship between perceived benefits and intention to disclose personal information is stronger in the higher-PPC group than in the lower-PPC group.*

**H8d.** *The relationship between perceived benefits and perceived risk is stronger in the higher-PPC group than in the lower-PPC group.*

Higher PPC is also associated with greater intention to disclose PI [30,46,60]. When individuals feel able to influence how their information is handled, they tend to perceive potential risks as less threatening and are more inclined to accept disclosure-related risks [20], reducing uncertainty and perceived vulnerability. Accordingly, the negative relationship between perceived risk and disclosure intention is expected to be more pronounced among consumers reporting lower PPC than among those reporting higher PPC.

**H8e.** *The relationship between perceived risk and intention to disclose personal information is stronger in the lower-PPC group than in the higher-PPC group.*

Finally, the structural role of trust may also differ according to consumers' perceived level of control over how their PI is collected and used. Transparency regarding data-related practices, clear privacy notices, and user-friendly consent mechanisms provide control cues that reinforce trust and facilitate intention to share PI [27,60]. These mechanisms provide a theoretical basis for expecting the trust-to-intention relationship to differ according to consumers' perceived level of privacy control. Similarly, safeguards such as access controls, contractual protections, and privacy technologies amplify the risk-reducing function of trust

by signaling that opportunistic misuse of data is limited [30,46,57], suggesting potential structural differences according to PPC levels.

**H8f.** *The relationship between trust in e-commerce websites and intention to disclose personal information is stronger in the higher-PPC group than in the lower-PPC group.*

**H8g.** *The relationship between trust in e-commerce websites and perceived risk is stronger in the higher-PPC group than in the lower-PPC group.*

To synthesize the key studies informing the proposed model and clarify how the present research builds on prior work, Table 1 summarizes the focus, methodological approach, and main findings of selected studies reviewed above.

**Table 1.** Summary of selected studies on privacy calculus and information disclosure.

| Authors              | Focus of the Paper                                                                                                                                                                                | Methodology                                                                                                                                                                                            | Main Findings                                                                                                                                                                                                                                                   |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Malhotra et al. [17] | Information privacy concerns and their relationships with trusting beliefs, risk beliefs, and intention to disclose personal information online                                                   | Two field surveys with 742 household respondents; scale development/validation and causal-model testing using structural equation modeling.                                                            | Information privacy concerns reduce trusting beliefs and increase risk beliefs. In turn, trusting beliefs positively influence behavioral intention to disclose, whereas risk beliefs negatively influence it.                                                  |
| Dinev and Hart [27]  | Extended privacy calculus for willingness to provide personal information in e-commerce transactions, integrating privacy risk, Internet privacy concerns, trust, and personal Internet interest. | Survey of 369 respondents; structural equation modeling using LISREL.                                                                                                                                  | Internet privacy concerns inhibit e-commerce transactions, while the cumulative influence of Internet trust and personal Internet interest can outweigh privacy risk perceptions in disclosure decisions, supporting an extended privacy calculus model.        |
| Kehr et al. [29]     | Extends the privacy calculus by distinguishing dispositional factors from situation-specific privacy assessments and by examining the role of affect in disclosure decisions.                     | Experimental study using 2 × 2 cross-sectional online experiment manipulating information sensitivity and affect; $n = 414$ (186 U.S., 228 Swiss participants); covariance-based SEM using Mplus 6.12. | General privacy concerns increase perceived risk, whereas institutional trust increases perceived benefits. These situation-specific risk–benefit assessments mediate their effects on disclosure intention, while positive affect reduces perceived risk.      |
| Wang et al. [38]     | Privacy-calculus determinants of intention to disclose personal information through mobile applications.                                                                                          | Online survey; 347 responses collected, 327 retained; PLS-SEM.                                                                                                                                         | Self-presentation and personalized services increase perceived benefits, while perceived severity increases and perceived control reduces perceived risks. Benefits increase and risks reduce disclosure intention, with benefits exerting the stronger effect. |

Table 1. Cont.

| Authors                       | Focus of the Paper                                                                                                                                                       | Methodology                                                                                                                                                                  | Main Findings                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maseeh et al. [21]            | Antecedents and outcomes of privacy concerns in e-commerce and sources of heterogeneity across studies.                                                                  | Multilevel meta-analysis of 184 articles.                                                                                                                                    | Risk perceptions increase privacy concerns, whereas perceived benefits and trust reduce them. Privacy concerns negatively affect e-commerce usage, and these relationships vary across methodological and contextual conditions.                                                                                                  |
| Kolotylo-Kulkarni et al. [28] | Systematic synthesis of information disclosure in e-commerce, including its conceptualization, determinants, moderators, outcomes, theoretical foundations, and methods. | Systematic literature review of 62 eligible papers (1998–June 2020); PRISMA-guided search across eight databases and backward citation analysis; inductive content analysis. | Disclosure is conceptualized in multiple ways, notably as intention and actual behavior. Determinants cluster into consumer, online-platform, information, and contextual factors. Evidence on moderators is limited, particularly for contextual moderation; the authors propose an integrated model and future research agenda. |
| Wang et al. [22]              | Factors influencing online information-disclosure intention and the moderating roles of cultural background and platform type.                                           | Meta-analysis of 48 independent empirical studies.                                                                                                                           | Perceived benefit, trust, subjective norm, and perceived behavioral control positively affect disclosure intention, whereas perceived privacy risk and privacy concern negatively affect it. Cultural background and platform type moderate relationships between antecedents and disclosure intention.                           |
| Jadil et al. [5]              | Antecedents and consequences of online trust in the Moroccan e-commerce context.                                                                                         | Online survey of 414 experienced Moroccan online buyers; PLS-SEM using SmartPLS 3.                                                                                           | Online trust reduces perceived risk and positively affects attitude and purchase intention. Perceived risk negatively affects attitude but has no significant direct effect on purchase intention.                                                                                                                                |
| Rodríguez-Priego et al. [57]  | Determinants of online self-disclosure, with emphasis on perceived customer care, perceived control, privacy concern, and trust.                                         | Online survey of 426 Spanish Amazon customers; variance-based structural equation modeling.                                                                                  | Perceived customer care increases perceived control and trust. Perceived control is positively related to trust and negatively related to privacy concerns, while trust mediates the effects of perceived customer care and privacy concern on self-disclosure.                                                                   |

Table 1. Cont.

| Authors         | Focus of the Paper                                                                                                                                             | Methodology                                                                                          | Main Findings                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tao et al. [58] | Why perceived privacy control has inconsistent effects on privacy concerns in e-commerce, focusing on trust, Internet privacy experience, and risk propensity. | Online survey of 625 Chinese consumers; empirical testing of mediation and moderation relationships. | Trust in e-commerce partially mediates the effect of perceived privacy control on privacy concerns. Internet privacy experience strengthens the PPC–trust relationship, while Internet privacy experience and risk propensity weaken the trust–privacy concern relationship. |

Source: Authors' elaboration.

Taken together, these hypotheses predict that the structural configuration of the privacy calculus differs according to consumers' perceived level of privacy control. By comparing the corresponding structural coefficients between PPC-based consumer segments, this study examines heterogeneity within the PCM and contributes to a more differentiated understanding of disclosure behavior in e-commerce environments.

### 3. Materials and Methods

This study adopts a post-positivist epistemological stance, as it seeks to test theoretically derived relationships among latent constructs using quantitative survey data and statistical modeling.

#### 3.1. Survey Development and Measurement Instrument

The research model includes six reflective constructs measured using established scales adapted to the context of online privacy. Global Information Privacy Concern (GIPC) was measured using six items from Malhotra et al. [17], Perceived Benefits (PB) using three items from Dinev et al. [61] and Kehr et al. [29], Perceived Risk (PR) and Trust (TR) using three items each adapted from Dinev and Hart [27]. Intention to disclose PI (INT) was assessed using Campbell's [49] three-item scale. PPC was measured through four items adapted from Al-Jabri et al. [35] and Dinev et al. [61]. A translation and back-translation procedure involving bilingual experts ensured linguistic accuracy. The questionnaire was reviewed by three PhD researchers and pre-tested with 17 online consumers, resulting in minor refinements to wording and clarity. To minimize potential common method bias, several procedural measures were implemented during questionnaire design and administration. The study relied on established measurement scales, while expert review was used to improve item clarity and reduce ambiguity. The measures of the study constructs were presented in separate questionnaire sections to provide proximal and psychological separation between predictor and criterion variables and reduce respondents' ability to infer the hypothesized relationships. In addition, participation was voluntary, respondents were assured of anonymity and confidentiality, and no personally identifiable information was collected, thereby helping to reduce evaluation apprehension and socially desirable responding. All items were rated on a five-point Likert scale (1 = strongly disagree; 5 = strongly agree). The complete measurement items are provided in Appendix A (Table A1).

### 3.2. Data Collection and Sampling

To empirically test the research model, a quantitative cross-sectional survey design was adopted. This design is appropriate for examining individuals' privacy perceptions and behavioral intentions at a specific point in time and for analyzing structural relationships among latent constructs. Eligible participants were required to have completed at least one online purchase involving personal data disclosure within the previous twelve months.

A non-probability sampling approach was employed, combining convenience sampling and snowball sampling. Convenience sampling facilitated access to active online consumers, while snowball sampling enabled broader reach across Moroccan digital networks. This approach facilitated access to eligible active online consumers but, as a non-probability sampling strategy, does not provide a statistically representative sample of the broader Moroccan population. The final sample comprised 743 valid responses, exceeding the minimum sample-size threshold indicated by the ten-times rule for PLS-SEM [62].

Data were collected between 21 December 2025, and 17 May 2026, using a structured questionnaire administered through Google Forms and disseminated via email and social media platforms. The online format ensured consistency with the digital behavior under investigation and allowed respondents to participate within their natural e-commerce environment. Clear instructions were provided, and participants were encouraged to reflect on recent purchase experiences to improve response accuracy and minimize recall bias.

Anti-duplication procedures were implemented to safeguard data integrity. Participation was voluntary; respondents provided informed consent, were assured of anonymity and confidentiality, and no personally identifiable information was collected. The study complied with institutional and national ethical guidelines for online research. Of the 807 responses initially received, 743 valid cases remained after excluding incomplete entries. The demographic composition and key characteristics of the respondents are presented in Table 2.

### 3.3. Data Analysis

Normality was assessed using skewness and kurtosis statistics, with all values falling within accepted thresholds [63]. Common method bias (CMB) was assessed using two complementary statistical procedures. Harman's single-factor test showed that the first factor accounted for 21.30% of the total variance, well below the 50% threshold, while all full-collinearity VIF values were below the conservative threshold of 3.3 [64]. These results suggest that CMB was unlikely to represent a substantial threat to the estimated relationships. Although the data showed acceptable univariate normality, PLS-SEM was selected due to its suitability for prediction-oriented models, its robustness in complex causal structures, and its flexibility when exploring group differences through non-parametric procedures. SmartPLS 4.1 was used, and significance was assessed using bias-corrected and accelerated (BCa) bootstrapping with 5000 subsamples.

The measurement model assessment included convergent validity (outer loadings and AVE), internal consistency reliability (Cronbach's alpha, composite reliability, rho\_A), and discriminant validity (Fornell-Larcker criterion and HTMT ratios). The structural model was then examined through path coefficients, explanatory power ( $R^2$  and adjusted  $R^2$ ), predictive relevance ( $Q^2$ ), and effect sizes ( $f^2$ ). Collinearity among predictors in the structural model was assessed using VIF values, all of which fell within recommended thresholds.

Potential endogeneity in the structural model was assessed as an additional robustness check using the Gaussian copula approach [65]. Specifically, copula terms were estimated

for the TR → PR, TR → INT, and PR → INT relationships, and their statistical significance was evaluated using bootstrapping.

**Table 2.** Sample characteristics.

| Respondent's Profile              |                      | N   | %      |
|-----------------------------------|----------------------|-----|--------|
| Gender                            | Female               | 319 | 42.93% |
|                                   | Male                 | 424 | 57.07% |
| Age                               | 18–24                | 257 | 34.58% |
|                                   | 25–34                | 357 | 48.04% |
|                                   | 35–44                | 65  | 8.75%  |
|                                   | 45–54                | 22  | 2.96%  |
|                                   | 55–64                | 22  | 2.96%  |
|                                   | 65 or older          | 20  | 2.69%  |
| Highest education level           | High school          | 67  | 9.01%  |
|                                   | Some college/Diploma | 160 | 21.53% |
|                                   | College/Bachelor     | 277 | 37.28% |
|                                   | Master/Doctorate     | 239 | 32.17% |
| Experience with Internet use      | Less than 2 years    | 85  | 11.44% |
|                                   | 2–5 years            | 132 | 17.77% |
|                                   | More than 5 years    | 526 | 70.79% |
| Experience with Internet shopping | Less than 2 years    | 179 | 24.09% |
|                                   | 2–5 years            | 209 | 28.13% |
|                                   | More than 5 years    | 355 | 47.78% |

Source: Authors' elaboration.

Structural heterogeneity according to PPC was examined using multigroup analysis (MGA). Prior to this analysis, the Measurement Invariance of Composite Models (MICOM) procedure [66] was applied to assess configural invariance, compositional invariance, and the equality of means and variances across groups. The sample was divided into high- and low-PPC groups using a median split. The multigroup approach was selected to examine structural heterogeneity in the privacy calculus between consumers assigned to different PPC segments [62,66,67]. However, because PPC is inherently continuous, dichotomization entails information loss. PPC scores were calculated as the mean of the four PPC indicators, and the empirical median of 2.75 was used as the cutoff. Participants with PPC scores above the median were assigned to the high-PPC group ( $n = 336$ ), whereas those with scores equal to or below the median were assigned to the low-PPC group ( $n = 407$ ). Group comparisons were then performed using Henseler's MGA and permutation tests, which are recommended non-parametric procedures for assessing path coefficient differences in PLS-SEM multigroup analysis [62,66].

## 4. Results

### 4.1. Measurement Model Assessment

The evaluation of the measurement model constitutes the initial stage of PLS-SEM analysis and aims to establish the reliability and validity of the constructs before assessing the structural relationships [62]. Accordingly, the measurement model was evaluated based

on indicator reliability, internal consistency reliability, convergent validity, and discriminant validity.

The reflective measurement model met all the required reliability and validity criteria. First, indicator reliability was established, as all measurement items exhibited outer loadings above the recommended threshold of 0.70 [62,68]. As reported in Table 3, the outer loadings ranged from 0.796 to 0.910, confirming satisfactory indicator reliability.

**Table 3.** Construct reliability and convergent validity analysis.

| Constructs | Items       | Outer Loadings | $\alpha$ | CR    | rho_A | AVE   |
|------------|-------------|----------------|----------|-------|-------|-------|
| GIPC       | GIPC1–GIPC6 | 0.796–0.861    | 0.907    | 0.928 | 0.909 | 0.684 |
| INT        | INT1–INT3   | 0.858–0.863    | 0.826    | 0.896 | 0.828 | 0.742 |
| PB         | PB1–PB3     | 0.831–0.883    | 0.815    | 0.890 | 0.820 | 0.730 |
| PR         | PR1–PR3     | 0.864–0.883    | 0.840    | 0.904 | 0.841 | 0.758 |
| TR         | TR1–TR3     | 0.854–0.871    | 0.827    | 0.896 | 0.831 | 0.742 |
| PPC        | PPC1–PPC4   | 0.825–0.910    | 0.903    | 0.930 | 0.950 | 0.768 |

Source: Authors' compilation. GIPC = Global Information Privacy Concern; INT = Intention to disclose personal information; PB = perceived benefits; PR = perceived risks; TR = trust in e-commerce websites; PPC = perceived privacy control.

Second, internal consistency reliability and convergent validity were assessed. Internal consistency was established using Cronbach's alpha ( $\alpha$ ), composite reliability (CR), and rho\_A, with all values exceeding the recommended threshold of 0.70 [62]. Convergent validity was also established, as all average variance extracted (AVE) values exceeded the recommended threshold of 0.50, indicating that each construct accounted for more than half of the variance in its indicators [62]. The detailed reliability and convergent validity results are presented in Table 3.

Finally, discriminant validity was verified using both the Fornell–Larcker criterion and the Heterotrait–Monotrait Ratio (HTMT). Satisfactory discriminant validity was confirmed as the square root of the AVE for each construct was greater than its highest correlation with any other construct (Table 4), in line with the Fornell–Larcker criterion.

**Table 4.** Discriminant validity results.

| Construct | Fornell–Larcker Criterion |        |       |        |       | Heterotrait–Monotrait (HTMT) |       |       |       |    |
|-----------|---------------------------|--------|-------|--------|-------|------------------------------|-------|-------|-------|----|
|           | GIPC                      | INT    | PB    | PR     | TR    | GIPC                         | INT   | PB    | PR    | TR |
| GIPC      | 0.827                     |        |       |        |       |                              |       |       |       |    |
| INT       | −0.073                    | 0.861  |       |        |       | 0.086                        |       |       |       |    |
| PB        | 0.046                     | 0.348  | 0.855 |        |       | 0.054                        | 0.422 |       |       |    |
| PR        | 0.542                     | −0.250 | 0.020 | 0.871  |       | 0.619                        | 0.300 | 0.033 |       |    |
| TR        | 0.042                     | 0.253  | 0.048 | −0.237 | 0.861 | 0.049                        | 0.303 | 0.058 | 0.283 |    |

Source: Authors' compilation. GIPC = Global Information Privacy Concern; INT = Intention to disclose personal information; PB = perceived benefits; PR = perceived risks; TR = trust in e-commerce websites.

Moreover, all HTMT values reported in Table 4 were below the conservative threshold of 0.85 [68], indicating that the latent constructs were empirically distinct [62]. Overall, the measurement model demonstrated satisfactory indicator reliability, internal consistency,

tency reliability, convergent validity, and discriminant validity, supporting the subsequent assessment of the structural model.

#### 4.2. Structural Model Assessment

Following the confirmation of satisfactory reliability and validity metrics for the measurement model across the full sample, the subsequent stage involved assessing the structural model's results. This assessment was conducted on the full dataset, focusing on the significance of the hypothesized relationships, explanatory power, and predictive relevance of the model.

Collinearity was first examined to ensure that the structural paths were not biased by redundancy among the predictors. All inner VIF values were comfortably below the conservative threshold of 3 [62,69], ranging from 1.004 to 1.565. More specifically, the VIFs for the paths predicting disclosure intention (GIPC, PR, TR and PB) ranged between 1.004 and 1.565, while those for the predictors of perceived risk (GIPC, TR and PB) were all 1.004. These values indicate the absence of problematic multicollinearity and confirm that each construct contributes distinct information to the explanation of the endogenous variables. This initial diagnostic step ensures the robustness of the subsequently derived path coefficient estimations.

As summarized in the analysis of the full sample (Table 5), the results provided strong support for the majority of the hypothesized direct effects. For behavioral intention, perceived risk exerted a significant negative effect ( $\beta = -0.229, p < 0.001$ ), whereas trust showed a positive and significant effect ( $\beta = 0.181, p < 0.001$ ). Perceived benefits emerged as the strongest predictor of disclosure intention ( $\beta = 0.343, p < 0.001$ ). In contrast, GIPC did not display a significant direct effect on disclosure intention ( $\beta = 0.027, p = 0.496$ ). Turning to perceived risk, GIPC had a substantial positive impact ( $\beta = 0.552, p < 0.001$ ), while trust reduced perceived risk ( $\beta = -0.260, p < 0.001$ ). Perceived benefits did not significantly influence perceived risk ( $\beta = 0.007, p = 0.810$ ). Overall, these coefficients provide strong support for the central mechanisms of the PCM, with risk, trust and benefits shaping intention, and GIPC and trust shaping risk.

**Table 5.** Results of structural model assessment.

| Hypothesis | Path       | $\beta$    | SD    | <i>t</i> Values | 95% CI           | Decision  | $f^2$ | VIF   |
|------------|------------|------------|-------|-----------------|------------------|-----------|-------|-------|
| H1         | GIPC → PR  | 0.552 ***  | 0.026 | 21.368          | [0.499; 0.601]   | Supported | 0.476 | 1.004 |
| H2         | GIPC → INT | 0.027      | 0.039 | 0.681           | [−0.050; 0.103]  | Rejected  | 0.001 | 1.481 |
| H3         | PB → INT   | 0.343 ***  | 0.031 | 11.062          | [0.280; 0.402]   | Supported | 0.150 | 1.004 |
| H4         | PB → PR    | 0.007      | 0.030 | 0.241           | [−0.050; 0.066]  | Rejected  | 0.000 | 1.004 |
| H5         | PR → INT   | −0.229 *** | 0.040 | 5.668           | [−0.308; −0.151] | Supported | 0.043 | 1.565 |
| H6         | TR → PR    | −0.260 *** | 0.029 | 9.106           | [−0.315; −0.202] | Supported | 0.106 | 1.004 |
| H7         | TR → INT   | 0.181 ***  | 0.034 | 5.264           | [0.112; 0.247]   | Supported | 0.038 | 1.110 |

Source: Authors' compilation. Note: \*\*\*  $p < 0.001$ ; GIPC = Global Information Privacy Concern; INT = Intention to disclose personal information; PB = perceived benefits; PR = perceived risks; TR = trust in e-commerce websites.

The effect sizes were then examined to gauge the substantive importance of each predictor. For INT, PB displayed a moderate effect ( $f^2 = 0.150$ ), confirming its central role in driving intention. The effects of PR ( $f^2 = 0.043$ ) and TR ( $f^2 = 0.038$ ) were small but meaningful, whereas GIPC had a negligible contribution to INT ( $f^2 = 0.001$ ), consistent with its non-significant path. For PR, GIPC showed a large effect ( $f^2 = 0.476$ ), indicating that global privacy concerns are the primary driver of risk perceptions, while trust exerted a small effect ( $f^2 = 0.106$ ). PB exhibited no notable effect on PR ( $f^2 = 0.000$ ). Taken together,

these effect sizes highlight a clear hierarchy among predictors, with PB and GIPC emerging as the most influential constructs in their respective equations.

Finally, the explanatory and predictive power of the model were assessed. The adjusted coefficient of determination ( $R^2$ ) was 0.358 for disclosure intention, indicating that the set of predictors explains approximately 36% of the variance in intention, which constitutes a satisfactory level of explanatory power in this research context. Perceived risk was also adequately explained, with adjusted  $R^2 = 0.216$ , reflecting the strong influence of GIPC and trust. The predictive relevance, assessed using  $Q^2$  statistics, further confirmed the model's predictive relevance, with  $Q^2 = 0.179$  for disclosure intention and  $Q^2 = 0.354$  for perceived risk, both exceeding zero. These values indicate predictive relevance for both endogenous constructs.

As an additional robustness check, potential endogeneity involving trust, perceived risk, and disclosure intention was assessed using the Gaussian copula approach. The copula terms for  $TR \rightarrow INT$  and  $PR \rightarrow INT$  were nonsignificant, indicating no evidence of endogeneity for these relationships. In contrast, the copula term associated with  $TR \rightarrow PR$  was significant ( $\beta = -0.254$ ,  $p = 0.028$ ), indicating a localized endogeneity concern for this path. This result remained significant when the  $TR \rightarrow PR$  copula was estimated separately. As noted by Hair et al. [62] and Hult et al. [65], endogeneity is primarily a concern in explanatory analyses where unbiased coefficient estimation is critical, whereas it is less problematic when the primary objective is prediction. Given the prediction-oriented nature of the present PLS-SEM analysis, this localized endogeneity concern does not invalidate the model's predictive assessment, although the  $TR \rightarrow PR$  coefficient should still be interpreted cautiously.

#### 4.3. Multigroup Analysis (MGA)

Before conducting the multigroup analysis, measurement invariance was assessed using the Measurement Invariance of Composite Models (MICOM) procedure [62,66]. Configural invariance was confirmed, as the measurement models were specified identically across the high and low perceived control groups. Compositional invariance was also supported, with all correlation values between composite scores ranging from 0.998 to 1.000 and non-significant permutation tests ( $p > 0.05$ ). These results establish partial measurement invariance, which is sufficient for meaningful multigroup comparisons of structural relationships. The detailed results of the MICOM procedure are reported in Table 6. The final step examined equality of composite means and variances. While equality of variances was supported for all constructs, equality of means was not fully achieved for trust ( $p = 0.017$ ), indicating that full measurement invariance was not established. Nevertheless, partial measurement invariance is adequate for MGA, allowing structural path differences to be interpreted as substantive group effects rather than measurement artifacts.

Following the confirmation of partial measurement invariance (PMI), multigroup analysis was conducted to determine whether the structural path coefficients differed between the PPC-based consumer segments. Group differences were evaluated using Henseler's MGA (significant when  $p < 0.05$  or  $p > 0.95$ ) and the permutation test (significant when  $p < 0.05$ ). A path difference was considered statistically significant only when both procedures indicated significance. Hypothesis support additionally required the observed group difference to be consistent with the hypothesized direction. The detailed multigroup analysis results are presented in Table 7.

**Table 6.** MICOM procedure results.

| Constructs | Step 1                | Step 2                   |                |       |     |        | Step 3a         |       |       | Step 3b          |                 |       |       |
|------------|-----------------------|--------------------------|----------------|-------|-----|--------|-----------------|-------|-------|------------------|-----------------|-------|-------|
|            | Configural Invariance | Compositional Invariance |                |       |     |        | Equal Means?    |       |       | Equal Variances? |                 |       |       |
|            |                       | (c = 1)                  | 95% CI         | p     | PMI | OD *   | 95% CI          | p     | Equal | OD *             | 95% CI          | p     | Equal |
| GIPC       | Yes                   | 1.000                    | [0.999; 1.000] | 0.274 | Yes | 0.096  | [−0.157; 0.149] | 0.205 | Yes   | −0.135           | [−0.151; 0.158] | 0.086 | Yes   |
| INT        | Yes                   | 0.999                    | [0.998; 1.000] | 0.749 | Yes | −0.033 | [−0.141; 0.151] | 0.669 | Yes   | 0.020            | [0.003; 0.148]  | 0.809 | Yes   |
| PB         | Yes                   | 0.999                    | [0.996; 1.000] | 0.996 | Yes | −0.133 | [−0.140; 0.142] | 0.062 | Yes   | 0.022            | [0.001; 0.163]  | 0.782 | Yes   |
| PR         | Yes                   | 1.000                    | [0.999; 1.000] | 0.576 | Yes | −0.094 | [−0.139; 0.143] | 0.202 | Yes   | 0.007            | [0.002; 0.155]  | 0.942 | Yes   |
| TR         | Yes                   | 0.998                    | [0.994; 1.000] | 0.620 | Yes | 0.187  | [−0.164; 0.144] | 0.017 | No    | 0.067            | [−0.003; 0.158] | 0.404 | Yes   |

Source: Authors' compilation. Note: \* OD = Original difference; GIPC = Global Information Privacy Concern; INT = Intention to disclose personal information; PB = perceived benefits; PR = perceived risks; TR = trust in e-commerce websites.

**Table 7.** Multigroup analysis results.

| Hypothesis | Path       | High Control | Low Control | Difference | Henseler's MGA | Permutation Test | Decision                      |
|------------|------------|--------------|-------------|------------|----------------|------------------|-------------------------------|
| H8a        | GIPC → INT | 0.093        | 0.003       | 0.090      | 0.122          | 0.245            | Rejected                      |
| H8b        | GIPC → PR  | 0.462        | 0.636       | −0.173     | 1.000          | 0.001            | Supported                     |
| H8c        | PB → INT   | 0.578        | 0.151       | 0.427      | 0.000          | 0.000            | Supported                     |
| H8d        | PB → PR    | −0.028       | 0.039       | −0.068     | 0.873          | 0.127            | Rejected                      |
| H8e        | PR → INT   | −0.139       | −0.310      | 0.171      | 0.018          | 0.018            | Supported                     |
| H8f        | TR → INT   | 0.108        | 0.252       | −0.144     | 0.987          | 0.013            | Rejected (opposite direction) |
| H8g        | TR → PR    | −0.427       | −0.100      | −0.326     | 1.000          | 0.000            | Supported                     |

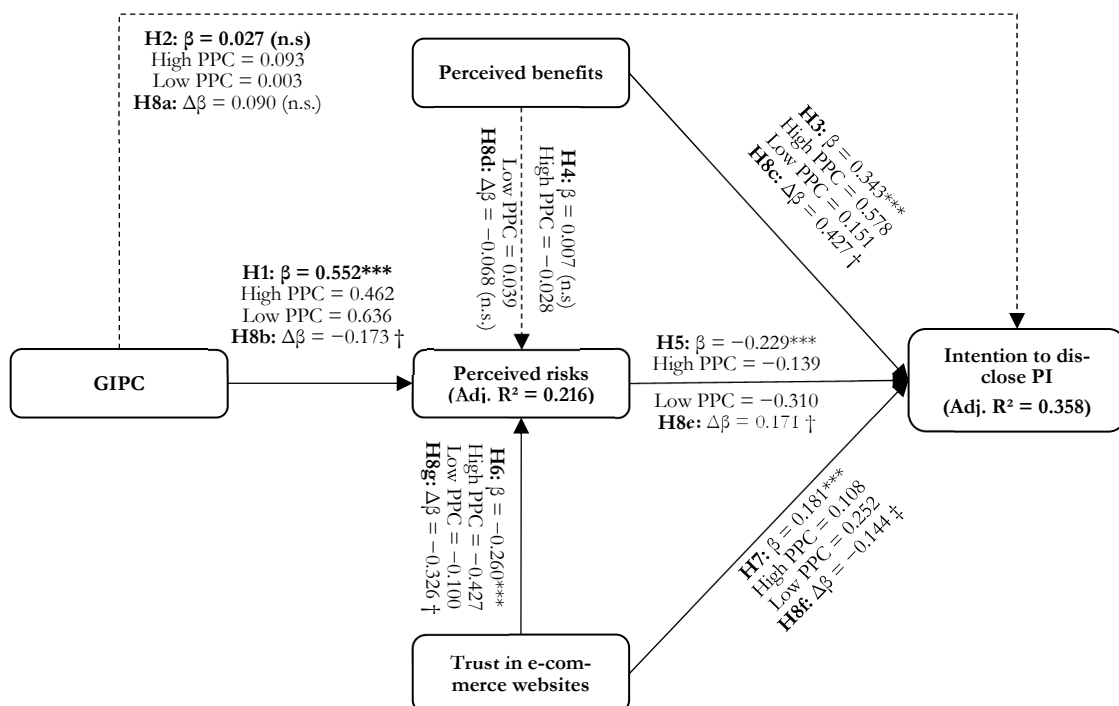
Source: Authors' compilation. GIPC = Global Information Privacy Concern; INT = Intention to disclose personal information; PB = perceived benefits; PR = perceived risks; TR = trust in e-commerce websites; Difference =  $\beta_{\text{High PPC}} - \beta_{\text{Low PPC}}$ . A between-group difference was considered statistically significant only when both Henseler's MGA and permutation testing indicated significance.

The multigroup analysis examined whether the structural relationships in the model differed between the higher- and lower-PPC groups. For consistency, the *p*-values reported in the following discussion correspond to the permutation test. The path between privacy concerns and disclosure intention did not significantly differ across groups ( $\Delta\beta = 0.090$ ,  $p = 0.245$ ), indicating no statistically significant difference between the two PPC groups in the relationship between GIPC and disclosure intention. In contrast, several significant group differences emerged. The negative impact of perceived risk on intention was significantly stronger among individuals with low perceived control ( $\beta = -0.310$ ) than among those with high perceived control ( $\beta = -0.139$ ;  $p = 0.018$ ), indicating that the negative relationship between perceived risk and disclosure intention is stronger in the lower-PPC group. Trust displayed an unexpected pattern: its positive effect on intention was stronger in the low-control group ( $\beta = 0.252$ ) than in the high-control group ( $\beta = 0.108$ ;  $p = 0.013$ ), suggesting that trust plays a comparatively stronger role in disclosure intention in the lower-PPC group. By contrast, perceived benefits exerted a substantially stronger positive influence on intention among high-control individuals ( $\beta = 0.578$ ) compared to low-control

individuals ( $\beta = 0.151$ ;  $p < 0.001$ ), indicating that the relationship between perceived benefits and disclosure intention is substantially stronger in the higher-PPC group.

Regarding perceived risk as an endogenous construct, significant differences were also observed. The positive association between privacy concerns and perceived risk was markedly stronger for low-control individuals ( $\beta = 0.636$ ) than for high-control individuals ( $\beta = 0.462$ ;  $p = 0.001$ ), indicating that the relationship between global information privacy concern and perceived risk is stronger in the lower-PPC group. Trust reduced perceived risk more strongly in the high-control group ( $\beta = -0.427$ ) than in the low-control group ( $\beta = -0.100$ ;  $p < 0.001$ ), indicating that the negative relationship between trust in e-commerce websites and perceived risk is stronger in the higher-PPC group. However, no significant group difference was found for the relationship between perceived benefits and perceived risk ( $\Delta\beta = -0.068$ ;  $p = 0.127$ ). Overall, the findings reveal significant structural heterogeneity in the higher-PPC group, the relationship between perceived benefits and disclosure intention and the negative relationship between trust and perceived risk are stronger. In the lower-PPC group, the relationship between global information privacy concern and perceived risk, the negative relationship between perceived risk and disclosure intention, and the relationship between trust and disclosure intention are stronger.

Figure 1 presents the theoretical model together with the PLS-SEM results for the full sample and the multigroup analysis results comparing consumers with high and low perceived privacy control.



**Figure 1.** Theoretical model and SEM results. Note.  $\beta$  values reported after H1–H7 are standardized path coefficients estimated for the full sample. High PPC and Low PPC denote the standardized path coefficients estimated for the two multigroup subsamples.  $\Delta\beta = \beta_{\text{High PPC}} - \beta_{\text{Low PPC}}$ . † indicates a statistically significant between-group difference consistent with the hypothesized direction according to both Henseler's MGA and the permutation test; ‡ indicates a statistically significant between-group difference in the opposite direction to that hypothesized. \*\*\*  $p < 0.001$ ; n.s. = not significant.

## 5. Discussion

The results reveal that consumers' intention to disclose PI is primarily driven by a privacy calculus in which perceived utility outweighs potential drawbacks. Perceived ben-

efits exerted the strongest positive influence on disclosure intention, while perceived risk acted as a significant deterrent. This pattern is consistent with privacy-calculus reasoning, where individuals weigh a benefit–risk trade-off under uncertainty [27], and aligns with empirical findings in comparable contexts [38,70]. Within the sample examined in this study, disclosure intention appears to be shaped more strongly by perceived benefits than by abstract concerns over potential losses. Respondents, navigating a digital landscape still characterized by developing logistical and payment infrastructures [71], appear to prioritize the benefits of the transaction, provided that a baseline of online vendor trustworthiness is established. Trust directly enhanced disclosure intention in the baseline model, while its negative association with perceived risk supported H6. However, the Gaussian-copula robustness assessment indicates that the TR → PR relationship is sensitive to potential endogeneity and should therefore be interpreted cautiously. By lowering perceived vulnerability, trust enables consumers to engage in data exchange even under conditions of uncertainty, functioning as a foundational belief that underpins the entire calculus. These findings confirm that when consumers perceive high value, such as customization or convenience, and trust the e-commerce website, their intention to disclose data increases.

Unlike what traditional privacy models would predict, this study found no significant direct relationship between global privacy concerns and disclosure intention. While this contradicts studies where concerns directly inhibited disclosure [33,35,72], it aligns with the privacy paradox phenomenon [13,73]. This result suggests that privacy concerns function not as an absolute barrier but as a latent factor that gains salience only when users evaluate the specific risks of a given transaction. One possible interpretation of this pattern is that it may be associated with digital resignation or privacy fatigue, where consumers, despite being aware of regulatory bodies, perceive data exposure as an inevitable cost of digital participation [74].

Furthermore, the rejection of the hypothesis that perceived benefits reduce perceived risk highlights a distinct cognitive compartmentalization among consumers. Unlike previous findings (e.g., [75]) suggesting that high rewards can lower the perception of risk through a heuristic effect, our results indicate that perceived benefits and risks operate as functionally independent evaluations. Consumers in our sample appear to compartmentalize these factors: they recognize the value of a service without allowing that value to artificially lower their risk assessment. This separation may be particularly relevant in an emerging digital market such as Morocco, where the perceived utility of an e-commerce service does not necessarily provide reassurance regarding how personal data are collected, stored, or used. Consumers may therefore recognize the convenience, personalization, or transactional value associated with disclosure while simultaneously maintaining concerns about data handling and potential misuse. In such a context, benefit-related cues and privacy-assurance cues may serve different evaluative functions: the former increase the attractiveness of the transaction, whereas the latter reduce perceived vulnerability. This interpretation is consistent with evidence from the Moroccan context showing the importance of trust and perceived control in shaping online consumer responses [5,21]. Accordingly, higher perceived benefits may motivate disclosure without functioning as a signal that privacy risks have diminished. This also helps explain why, in the baseline model, trust is associated with lower perceived risk rather than perceived benefits, although the Gaussian-copula assessment indicates that the TR → PR relationship is sensitive to potential endogeneity and should therefore be interpreted cautiously.

The multigroup analysis reveals substantial structural heterogeneity in the privacy calculus according to consumers' perceived level of privacy control. Consistent with the conceptualization of privacy as boundary regulation [4,10], the relative importance of the different privacy-calculus pathways differs between the higher- and lower-PPC

groups. The most notable shift is observed in the value-driven route, where the impact of perceived benefits on intention is substantially stronger for the high-control group than for the low-control group. This supports the interpretation proposed by Burkhardt et al. [76], where effective control cues affect how individuals process privacy trade-offs rather than merely shifting mean levels of concern. In the higher-PPC group, perceived benefits are substantially more strongly associated with disclosure intention. Conversely, the relationship between perceived benefits and disclosure intention is considerably weaker in the lower-PPC group, suggesting a more limited role for expected benefits in this segment.

Further structural differences emerge in the risk-related relationships. In the lower-PPC group, the relationship between global privacy concerns and perceived risk is stronger, and perceived risk is also more strongly negatively associated with disclosure intention. By comparison, both relationships are weaker in the higher-PPC group. This aligns with the control paradox phenomenon [20], where the provision of control cues does not necessarily eliminate objective danger but leads users to perceive risks as containable. The variation in the path from global concerns to perceived risk also corroborates recent findings that this conversion is not uniform but depends on how control is operationalized in the website interface [58,76]. In the Moroccan context, where digital governance structures continue to evolve, the observed pattern is consistent with a weaker relationship between global privacy concerns and perceived risk among consumers with higher PPC.

The hypothesis predicting a stronger trust-to-intention relationship among high-control consumers was not supported. Instead, the positive effect of trust on disclosure intention was stronger among low-control consumers, making this unexpected reversal theoretically informative. This finding may suggest that trust plays a compensatory role when perceived control is lower. When consumers feel unable to manage how their personal information is handled, they appear to rely more heavily on the trustworthiness of the e-commerce website as a heuristic safeguard. Conversely, in the higher-PPC group, the relationship between trust and disclosure intention is weaker, whereas the negative relationship between trust and perceived risk is stronger. This mechanism corroborates recent findings in the Moroccan market by Jadil et al. [5], who observed that trust leads consumers to place less weight on risk during online transactions. When governance cues are visible and credible, trust becomes actionable: it no longer merely motivates engagement but actively lowers the expectation of harm [57]. These findings suggest that the structural role of trust differs between the two groups: trust is more strongly associated with disclosure intention in the lower-PPC group and more strongly associated with reduced perceived risk in the higher-PPC group.

Finally, these between-group structural differences provide additional insight into how privacy-calculus relationships operate in the Moroccan context, where formal regulation coexists with varying perceptions of platform-level control and assurance. While Morocco possesses a formal regulatory framework through Law 09-08 and the CNDP, the variation in consumer behavior observed in this study suggests that the existence of formal regulation alone is not sufficient to explain disclosure decisions [77]. Research on Moroccan digital consumers reveals that perceived control over data, such as transparency and the ability to manage privacy settings, may be an important driver of trust than the mere existence of formal regulatory frameworks [78]. This pattern aligns with intercultural evidence including Morocco, where justice-based governance (transparency, procedural fairness) can build trust despite persistent privacy concerns, particularly when control affordances are visible [79]. Consequently, widely varying levels of digital literacy and platform sophistication create a split experience: users who perceive high control leverage platform capabilities to maximize benefits. Meanwhile, users who perceive low control do not necessarily exit the market but may engage in adaptive disclosure strategies (e.g., falsifying

data or withholding non-essential information) to manage the high perceived risk [75]. Thus, in Morocco's emerging digital economy, disclosure is not a binary choice based on concern, but a strategic negotiation heavily dependent on whether the consumer perceives sufficient agency over the interaction.

## 6. Conclusions and Implications

### 6.1. Conclusion and Key Findings

This study examined whether the structural relationships within the Privacy Calculus Model differ according to consumers' perceived level of privacy control. The results show that global information privacy concern significantly increases perceived risk but has no significant direct effect on disclosure intention. Perceived risk negatively influences disclosure intention, whereas perceived benefits exert a significant positive effect on intention but do not significantly reduce perceived risk. Trust positively influences disclosure intention, while its negative association with perceived risk supports H6 in the baseline model; however, the Gaussian-copula assessment indicates that the TR → PR relationship is sensitive to potential endogeneity and should therefore be interpreted cautiously.

The multigroup analysis further shows that several structural relationships differ significantly between consumers with higher and lower PPC. Perceived benefits exert a substantially stronger positive influence on disclosure intention among consumers with high PPC, whereas perceived risk has a stronger inhibiting effect among those with low PPC. Privacy concerns translate more strongly into perceived risk under low PPC, while trust reduces perceived risk more strongly under high PPC. The trust-to-intention relationship displays the opposite pattern to that hypothesized, with trust exerting a stronger positive influence under low PPC. Overall, these findings show that the privacy calculus does not operate uniformly, with several key relationships exhibiting significant structural heterogeneity according to perceived privacy control.

### 6.2. Theoretical Contributions

Theoretically, this study contributes to privacy calculus research in two ways. First, it extends the empirical scope of the extended privacy calculus model to the Moroccan/MENA e-commerce context, where evidence on privacy-related disclosure behavior remains limited. Second, it identifies significant structural heterogeneity in the relationships linking privacy concerns, perceived benefits, perceived risk, and trust to disclosure intention according to consumers' perceived level of privacy control. Beyond this contextual extension, the findings also refine the interpretation of privacy calculus mechanisms. The non-significant relationship between perceived benefits and perceived risk challenges the traditional compensatory assumption that utility automatically reduces privacy fears. Instead, the results suggest a cognitive separation in which benefits motivate disclosure without necessarily reassuring consumers about data opacity or potential loss of control, consistent with sensitivity-aware perspectives [24]. Similarly, the absence of a direct link between privacy concerns and disclosure intention reframes the privacy paradox not as evidence of apathy, but as a manifestation of adaptive coping, where consumers maintain participation through selective disclosure or misrepresentation strategies rather than total withdrawal [75,80].

### 6.3. Practical and Managerial Implications

From a practical perspective, e-commerce and marketing managers must recognize that increasing disclosure intention cannot rely on benefit design alone; since utility does not reduce perceived risk, privacy governance must be treated as a core component of the service architecture rather than a compliance afterthought. Given the observed structural

differences associated with PPC, firms should consider control-enhancing designs such as granular consent, default minimization, and accessible privacy settings to strengthen consumers' sense of agency and privacy assurance. Additionally, managers should shift their focus from maximizing data volume to ensuring data quality, as persistent privacy concerns often manifest not as transaction abandonment but as the falsification of sensitive information [75]. To mitigate this, platforms should adopt tiered data requests (e.g., ask what is necessary and justify why) and transparent justice-based measures that explain data handling practices. By tracking data quality metrics, including completion rates for sensitive data fields, rather than just signup numbers, firms can detect when privacy friction is degrading data reliability and intervene with meaningful assurance cues to restore consumer confidence.

#### 6.4. Research Limitations and Future Research Directions

Despite its contributions, this study presents several limitations that open avenues for future research. First, the dependent variable in this study captures self-reported disclosure intention rather than actual disclosure behavior. Although intention provides meaningful insight into consumers' willingness to disclose personal information, stated intentions may not necessarily translate into actual disclosure actions. In addition, while procedural and statistical remedies were applied, common method effects cannot be completely excluded because the data were collected from a single source at one point in time. Future studies could therefore complement this approach with experimental designs, behavioral tracking, or field data to examine actual information disclosure behavior in e-commerce environments. Second, although the Gaussian-copula assessment indicated no evidence of endogeneity for  $TR \rightarrow INT$  or  $PR \rightarrow INT$ , it identified a localized endogeneity concern for  $TR \rightarrow PR$ . Accordingly, the trust–risk relationship should be interpreted cautiously, and future research could reassess this relationship using longitudinal designs or alternative identification strategies. Third, the cross-sectional design provides a static snapshot of privacy perceptions and disclosure intentions at a single point in time and therefore cannot capture how these perceptions and relationships evolve as consumers accumulate digital experience, encounter specific privacy incidents, or respond to changes in platform governance. Future research using longitudinal designs could examine how privacy concerns, perceived risk, trust, perceived privacy control, and disclosure intentions change over time and following such experiences. Fourth, PPC was dichotomized using a median split to form the comparison groups. This categorization entails some loss of information and therefore limits the interpretation of differences associated with PPC. Future research could complement the present multigroup approach using alternative analytical approaches to further examine variation associated with PPC. Fifth, the transactional perspective adopted here may not extend to other digital contexts such as social media platforms, mobile applications, location-based or AI-driven services, where privacy decision-making dynamics may differ, and future research could investigate whether the identified mechanisms remain stable across these settings. Sixth, while the study identifies structural differences associated with PPC-based grouping, it does not examine how specific interface and platform design features, such as privacy dashboards, consent management systems, transparency cues, or data access tools, generate or strengthen consumers' perceived privacy control. Future research could therefore investigate which specific privacy design mechanisms are most effective in shaping users' sense of control over their personal information. Seventh, the use of convenience and snowball sampling limits the representativeness and generalizability of the findings. Although the study specifically targeted active online consumers rather than the Moroccan population as a whole, the sample is predominantly composed of younger respondents, with more than 80% aged below 35. This age distribution may overrepresent

younger and more digitally engaged consumers and may therefore limit the extent to which the findings apply to older or less digitally engaged consumer segments. Future research should employ probability-based or stratified sampling strategies to achieve broader representation across age, geographic, and socioeconomic groups and to examine whether the identified relationships remain stable across different consumer profiles. Finally, the finding that privacy concerns do not directly inhibit disclosure intention suggests that consumers may engage in adaptive coping strategies to manage privacy risks while maintaining participation in digital services. Future research could investigate the nature and prevalence of such behaviors, including data minimization, selective disclosure, and intentional information falsification, to better understand how users navigate privacy trade-offs in e-commerce environments. Addressing these limitations would further refine the understanding of privacy behavior in digital markets and deepen insights into how individuals navigate the trade-offs between value creation, trust, and control in the evolving digital economy.

**Author Contributions:** Conceptualization, M.O., A.E.B. and H.F.; methodology, M.O. and S.E.-D.; software, M.O.; validation, A.E.B.; formal analysis, M.O.; investigation, M.O. and H.F.; resources, H.F.; data curation, M.O.; writing—original draft preparation, M.O., A.E.B. and H.F.; writing—review and editing, S.E.-D.; visualization, M.O.; supervision, M.O.; project administration, M.O. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no funding.

**Institutional Review Board Statement:** Data for this study were collected through a non-interventional survey using a convenience sampling approach. In accordance with institutional policies and national guidelines, formal Ethics Committee/IRB approval was not required for this type of research. Nevertheless, the study strictly adhered to established ethical standards and complied with Morocco's Law No. 09-08 on the Protection of Personal Data (and its implementing Decree No. 2-09-165). Participation was entirely voluntary, informed consent was obtained prior to data collection, and complete anonymity and confidentiality of all responses were strictly maintained.

**Informed Consent Statement:** Online informed consent was obtained from all participants involved in the study prior to participation.

**Data Availability Statement:** The data presented in this study are available from the corresponding author upon reasonable request.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Appendix A Measurement Scales

**Table A1.** Measurement items and sources.

| Construct                                        | Code | Items                                                                                   | Source            |
|--------------------------------------------------|------|-----------------------------------------------------------------------------------------|-------------------|
| Intention to disclose personal information (INT) | INT1 | I am willing to provide my personal information when asked by e-commerce websites       | Adapted from [49] |
|                                                  | INT2 | I am willing to disclose even sensitive personal information to e-commerce websites     |                   |
|                                                  | INT3 | I am willing to be truthful in revealing my personal information to e-commerce websites |                   |

**Table A1.** *Cont.*

| Construct                                         | Code  | Items                                                                                                                   | Source                     |
|---------------------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Perceived risks of information disclosure (PR)    | PR1   | Providing the e-commerce websites with my personal information would involve many unexpected problems                   | Adapted from [27]          |
|                                                   | PR2   | It would be risky to disclose my personal information to the e-commerce websites                                        |                            |
|                                                   | PR3   | There would be high potential for loss in disclosing my personal information to the e-commerce websites                 |                            |
| Perceived benefits of information disclosure (PB) | PB1   | Providing my personal information to the e-commerce websites will entail benefits                                       | Adapted from [61] and [29] |
|                                                   | PB2   | Revealing my personal information to the e-commerce websites will help me obtain the services I want                    |                            |
|                                                   | PB3   | I believe that as a result of my personal information disclosure, I will benefit from a better, more customized service |                            |
| Global information privacy concern (GIPC)         | GIPC1 | All things considered, the Internet would cause serious privacy problems.                                               | Adapted from [17]          |
|                                                   | GIPC2 | Compared to others, I am more sensitive about the way online companies handle my personal information.                  |                            |
|                                                   | GIPC3 | To me, it is the most important thing to keep my privacy intact from online companies.                                  |                            |
|                                                   | GIPC4 | I believe other people are too much concerned with online privacy issues.                                               |                            |
|                                                   | GIPC5 | Compared with other subjects on my mind, personal privacy is very important.                                            |                            |
|                                                   | GIPC6 | I am concerned about threats to my personal privacy today                                                               |                            |
| Trust in e-commerce websites (TR)                 | TR1   | E-commerce websites are safe environments in which to exchange information with others                                  | Adapted from [27]          |
|                                                   | TR2   | E-commerce websites are reliable environments in which to conduct business transactions                                 |                            |
|                                                   | TR3   | E-commerce websites handle personal information submitted by users in a competent fashion                               |                            |

Table A1. Cont.

| Construct                       | Code | Items                                                                                                        | Source                     |
|---------------------------------|------|--------------------------------------------------------------------------------------------------------------|----------------------------|
| Perceived Privacy Control (PPC) | PPC1 | I believe I have control over who can get access to my personal information collected by E-commerce websites | Adapted from [35] and [61] |
|                                 | PPC2 | I think I have control over what personal information is released by E-commerce websites                     |                            |
|                                 | PPC3 | I believe I can control my personal information provided to E-commerce websites                              |                            |
|                                 | PPC4 | I believe I have control over how my personal information is used by E-commerce websites                     |                            |

## References

1. Kvalvik, P.; Misra, S.; Mishra, B.; Dash, S. Data as an Asset: Economic Traits, Market Dynamics, and Monetization Challenges. *WIREs Data Min. Knowl. Discov.* **2026**, *16*, e70072. [CrossRef]
2. Utami, R.D.; Aimin, W. Balancing Personalization, Privacy, and Value: A Systematic Literature Review of AI-Enabled Customer Experience Management. *Information* **2026**, *17*, 115. [CrossRef]
3. Acquisti, A.; Brandimarte, L.; Loewenstein, G. Privacy and Human Behavior in the Age of Information. *Science* **2015**, *347*, 509–514. [CrossRef] [PubMed]
4. Smith, H.J.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Q.* **2011**, *35*, 989–A27. [CrossRef]
5. Jadil, Y.; Rana, N.P.; Dwivedi, Y.K. Understanding the Drivers of Online Trust and Intention to Buy on a Website: An Emerging Market Perspective. *Int. J. Inf. Manag. Data Insights* **2022**, *2*, 100065. [CrossRef]
6. Agence Nationale de Réglementation des Télécommunications (ANRT). *Enquête sur l'Accès et l'Usage des Technologies de l'Information et de la Communication par les Individus et les Ménages 2024–2025*; Agence Nationale de Réglementation des Télécommunications: Rabat, Morocco, 2025.
7. Visa. *How Consumers Are Embracing Security Measures in the Era of Digital Payments: Insights from Visa's Stay Secure Study 2025*; Visa: San Francisco, CA, USA, 2025.
8. Visa. Visa Study: 83% in Morocco Use AI to Shop, But Trust Is Key at Checkout. Available online: [https://ma.visamiddleeast.com/en\\_MA/about-visa/newsroom/press-releases/prl-02062026.html](https://ma.visamiddleeast.com/en_MA/about-visa/newsroom/press-releases/prl-02062026.html) (accessed on 24 August 2026).
9. Kaspersky. *Defending as a Team: Kaspersky Works with INTERPOL to Secure Africa Cup of Nations*; Kaspersky: Moscow, Russia, 2026.
10. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*; ERIC—Brooks/Cole Publishing Company: Pacific Grove, CA, USA, 1975.
11. Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure*; SUNY Series in Communication Studies; State University of New York Press: Albany, NY, USA, 2002; ISBN 9780791487853.
12. Farooq, A.; Salminen, J.; Martin, J.D.; Aldous, K.; Jung, S.-G.; Jansen, B.J. Exploring Social Media Privacy Concerns: A Comprehensive Survey Study Across 16 Middle Eastern and North African Countries. *IEEE Access* **2024**, *12*, 147087–147105. [CrossRef]
13. Norberg, P.A.; Horne, D.R.; Horne, D.A. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J. Consum. Aff.* **2007**, *41*, 100–126. [CrossRef]
14. Culnan, M.J.; Armstrong, P.K. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organ. Sci.* **1999**, *10*, 104–115. [CrossRef]
15. Shouli, A.; Barthwal, A.; Campbell, M.; Shrestha, A.K. Unpacking Youth Privacy Management in AI Systems: A Privacy Calculus Model Analysis. *IEEE Access* **2025**, *13*, 115780–115803. [CrossRef]
16. Hong, Y.; Wan, M.; Yao, W. Exploring User Retention in WeChat E-Commerce for SME Retailers: Perspective of Perceived Quality and Privacy Calculus. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 151. [CrossRef]
17. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
18. Dinev, T.; Bellotto, M.; Hart, P.; Russo, V.; Serra, I.; Colautti, C. Privacy Calculus Model in E-Commerce—A Study of Italy and the United States. *Eur. J. Inf. Syst.* **2006**, *15*, 389–402. [CrossRef]

19. Xu, H.; Dinev, T.; Smith, J.; Hart, P. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *J. Assoc. Inf. Syst.* **2011**, *12*, 798–824. [\[CrossRef\]](#)
20. Brandimarte, L.; Acquisti, A.; Loewenstein, G. Misplaced Confidences: Privacy and the Control Paradox. *Soc. Psychol. Personal. Sci.* **2013**, *4*, 340–347. [\[CrossRef\]](#)
21. Maseeh, H.I.; Jebarajakirthy, C.; Pentecost, R.; Arli, D.; Weaven, S.; Ashaduzzaman, M. Privacy Concerns in E-Commerce: A Multilevel Meta-Analysis. *Psychol. Mark.* **2021**, *38*, 1779–1798. [\[CrossRef\]](#)
22. Wang, N.; Zhao, Y.; Zhou, R.; Li, Y. Factors Influencing Users' Online Information Disclosure Intention and the Moderating Effect of Cultural Background and Platform Type. *Aslib J. Inf. Manag.* **2023**, *75*, 1178–1208. [\[CrossRef\]](#)
23. Smith, H.J.; Milberg, S.J.; Burke, S.J. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Q.* **1996**, *20*, 167–196. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Bandara, R.; Fernando, M.; Akter, S. Privacy Concerns in E-Commerce: A Taxonomy and a Future Research Agenda. *Electron. Mark.* **2020**, *30*, 629–647. [\[CrossRef\]](#)
25. Liu, C.; Marchewka, J.T.; Lu, J.; Yu, C.-S. Beyond Concern—A Privacy-Trust-Behavioral Intention Model of Electronic Commerce. *Inf. Manag.* **2005**, *42*, 289–304. [\[CrossRef\]](#)
26. Kim, D.J.; Ferrin, D.L.; Rao, H.R. A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. *Decis. Support Syst.* **2008**, *44*, 544–564. [\[CrossRef\]](#)
27. Dinev, T.; Hart, P. An Extended Privacy Calculus Model for E-Commerce Transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [\[CrossRef\]](#)
28. Kolotylo-Kulkarni, M.; Xia, W.; Dhillon, G. Information Disclosure in E-Commerce: A Systematic Review and Agenda for Future Research. *J. Bus. Res.* **2021**, *126*, 221–238. [\[CrossRef\]](#)
29. Kehr, F.; Kowatsch, T.; Wentzel, D.; Fleisch, E. Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus. *Inf. Syst. J.* **2015**, *25*, 607–635. [\[CrossRef\]](#)
30. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information Privacy in E-Service: Effect of Organizational Privacy Assurances on Individual Privacy Concerns, Perceptions, Trust and Self-Disclosure Behavior. *Gov. Inf. Q.* **2020**, *37*, 101413. [\[CrossRef\]](#)
31. Olivero, N.; Lunt, P. Privacy versus Willingness to Disclose in E-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control. *J. Econ. Psychol.* **2004**, *25*, 243–262. [\[CrossRef\]](#)
32. Fernandes, T.; Pereira, N. Revisiting the Privacy Calculus: Why Are Consumers (Really) Willing to Disclose Personal Data Online? *Telemat. Inform.* **2021**, *65*, 101717. [\[CrossRef\]](#)
33. Sun, Y.; Fang, S.; Hwang, Y. Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce. *Sustainability* **2019**, *11*, 3311. [\[CrossRef\]](#)
34. Khoa, B.T.; Nguyen, M.H. The Moderating Role of Anxiety in the Relationship Between the Perceived Benefits, Online Trust, and Personal Information Disclosure in Online Shopping. *Int. J. Bus. Soc.* **2022**, *23*, 444–460. [\[CrossRef\]](#)
35. Al-Jabri, I.M.; Eid, M.I.; Abed, A. The Willingness to Disclose Personal Information: Trade-off between Privacy Concerns and Benefits. *Inf. Comput. Secur.* **2020**, *28*, 161–181. [\[CrossRef\]](#)
36. Ryu, S.; Park, Y. How Consumers Cope with Location-Based Advertising (LBA) and Personal Information Disclosure: The Mediating Role of Persuasion Knowledge, Perceived Benefits and Harms, and Attitudes toward LBA. *Comput. Hum. Behav.* **2020**, *112*, 106450. [\[CrossRef\]](#)
37. Nguyen, M.H.; Khoa, B.T. Perceived Mental Benefit in Electronic Commerce: Development and Validation. *Sustainability* **2019**, *11*, 6587. [\[CrossRef\]](#)
38. Wang, T.; Duong, T.D.; Chen, C.C. Intention to Disclose Personal Information via Mobile Applications: A Privacy Calculus Perspective. *Int. J. Inf. Manag.* **2016**, *36*, 531–542. [\[CrossRef\]](#)
39. Baek, S.J.; Lee, H.J. Unravelling the Effects of Privacy Policies on Information Disclosure: Insights from E-Commerce Consumer Behavior. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 49. [\[CrossRef\]](#)
40. Salam, A.F.; Rao, H.R.; Pegels, C.C. Consumer-Perceived Risk in e-Commerce Transactions. *Commun. ACM* **2003**, *46*, 325–331. [\[CrossRef\]](#)
41. Barth, S.; de Jong, M.D.T. The Privacy Paradox—Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review. *Telemat. Inform.* **2017**, *34*, 1038–1058. [\[CrossRef\]](#)
42. Pavlou, P.A. Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *Int. J. Electron. Commer.* **2003**, *7*, 101–134. [\[CrossRef\]](#)
43. Chen, M.; Chen, M. Privacy Relevance and Disclosure Intention in Mobile Apps: The Mediating and Moderating Roles of Privacy Calculus and Temporal Distance. *Behav. Sci.* **2025**, *15*, 324. [\[CrossRef\]](#) [\[PubMed\]](#)
44. Yu, L.; Li, H.; He, W.; Wang, F.-K.; Jiao, S. A Meta-Analysis to Explore Privacy Cognition and Information Disclosure of Internet Users. *Int. J. Inf. Manag.* **2020**, *51*, 102015. [\[CrossRef\]](#)
45. van der Schyff, K.; Flowerday, S. The Mediating Role of Perceived Risks and Benefits When Self-Disclosing: A Study of Social Media Trust and FoMO. *Comput. Secur.* **2023**, *126*, 103071. [\[CrossRef\]](#)

46. Abbas, A.E.; Kool, F.; Agahari, W.; de Reuver, M. Stimulating Data Marketplace Adoption in Manufacturing: The Impact of Perceived Control on Willingness to Share Data. *Technovation* **2026**, *149*, 103371. [\[CrossRef\]](#)
47. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An Integrative Model of Organizational Trust. *Acad. Manag. Rev.* **1995**, *20*, 709–734. [\[CrossRef\]](#)
48. Jenkner, C.S.; Ravi, N.; Gabel, M.; Vogt, J. Trust in Data-requesting Organizations—A Quantitative Analysis on Cultural Antecedents and Individual-level Perceptions. *Electron. J. Inf. Syst. Dev. Ctries.* **2022**, *88*, e12208. [\[CrossRef\]](#)
49. Campbell, D. A Relational Build-up Model of Consumer Intention to Self-Disclose Personal Information in E-Commerce B2C Relationships. *AIS Trans. Hum.-Comput. Interact.* **2019**, *11*, 33–53. [\[CrossRef\]](#)
50. McKnight, D.H.; Choudhury, V.; Kacmar, C. Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Inf. Syst. Res.* **2002**, *13*, 334–359. [\[CrossRef\]](#)
51. Xu, H.; Li, J. How Can Users Be Confident About Self-Disclosure in Mobile Payment? From Institutional Mechanism Perspective. *J. Theor. Appl. Electron. Commer. Res.* **2026**, *21*, 10. [\[CrossRef\]](#)
52. Grosso, M.; Castaldo, S.; Li, H.; Larivière, B. What Information Do Shoppers Share? The Effect of Personnel-, Retailer-, and Country-Trust on Willingness to Share Information. *J. Retail.* **2020**, *96*, 524–547. [\[CrossRef\]](#)
53. Marriott, H.R.; Williams, M.D. Exploring Consumers Perceived Risk and Trust for Mobile Shopping: A Theoretical Framework and Empirical Study. *J. Retail. Consum. Serv.* **2018**, *42*, 133–146. [\[CrossRef\]](#)
54. Westin, A.F. *Privacy and Freedom*; Atheneum: New York, NY, USA, 1967; Volume 1, ISBN 9781632460738.
55. Xu, H.; Teo, H.-H.; Tan, B.C.Y.; Agarwal, R. Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Inf. Syst. Res.* **2012**, *23*, 1342–1363. [\[CrossRef\]](#)
56. Eastin, M.S.; Brinson, N.H.; Doorey, A.; Wilcox, G. Living in a Big Data World: Predicting Mobile Commerce Activity through Privacy Concerns. *Comput. Hum. Behav.* **2016**, *58*, 214–220. [\[CrossRef\]](#)
57. Rodríguez-Priego, N.; Porcu, L.; Prados Peña, M.B.; Crespo Almendros, E. Perceived Customer Care and Privacy Protection Behavior: The Mediating Role of Trust in Self-Disclosure. *J. Retail. Consum. Serv.* **2023**, *72*, 103284. [\[CrossRef\]](#)
58. Tao, S.; Liu, Y.; Sun, C. Examining the Inconsistent Effect of Privacy Control on Privacy Concerns in E-Commerce Services: The Moderating Role of Privacy Experience and Risk Propensity. *Comput. Secur.* **2024**, *140*, 103794. [\[CrossRef\]](#)
59. Bartol, J.; Vehovar, V.; Petrovčič, A. Cross-Contextual Analysis of the Effects of Vertical and Horizontal Privacy Perceptions on Willingness to Disclose Personal Information on the Internet. *Int. J. Hum.-Comput. Interact.* **2026**, *42*, 478–491. [\[CrossRef\]](#)
60. Taddei, S.; Contena, B. Privacy, Trust and Control: Which Relationships with Online Self-Disclosure? *Comput. Hum. Behav.* **2013**, *29*, 821–826. [\[CrossRef\]](#)
61. Dinev, T.; Xu, H.; Smith, J.H.; Hart, P. Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. *Eur. J. Inf. Syst.* **2013**, *22*, 295–316. [\[CrossRef\]](#)
62. Hair, J.F., Jr.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3rd ed.; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 2022; Volume 3, ISBN 9780333227794.
63. Kline, R.B. *Principles and Practice of Structural Equation Modeling*, 4th ed.; Guilford Publications: New York, NY, USA, 2016; ISBN 978-1462523344.
64. Kock, N. Common Method Bias in PLS-SEM. *Int. J. e-Collab.* **2015**, *11*, 1–10. [\[CrossRef\]](#)
65. Hult, G.T.M.; Hair, J.F.; Proksch, D.; Sarstedt, M.; Pinkwart, A.; Ringle, C.M. Addressing Endogeneity in International Marketing Applications of Partial Least Squares Structural Equation Modeling. *J. Int. Mark.* **2018**, *26*, 1–21. [\[CrossRef\]](#)
66. Henseler, J.; Ringle, C.M.; Sarstedt, M. Testing Measurement Invariance of Composites Using Partial Least Squares. *Int. Mark. Rev.* **2016**, *33*, 405–431. [\[CrossRef\]](#)
67. Iacobucci, D.; Posavac, S.S.; Kardes, F.R.; Schneider, M.J.; Popovich, D.L. The Median Split: Robust, Refined, and Revived. *J. Consum. Psychol.* **2015**, *25*, 690–704. [\[CrossRef\]](#)
68. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to Use and How to Report the Results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [\[CrossRef\]](#)
69. Hair, J.F.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M.; Danks, N.P.; Ray, S. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*; Classroom Companion: Business; Springer International Publishing: Cham, Switzerland, 2021; ISBN 978-3-030-80518-0.
70. Degutis, M.; Urbonavičius, S.; Hollebeek, L.D.; Anselmsson, J. Consumers' Willingness to Disclose Their Personal Data in e-Commerce: A Reciprocity-Based Social Exchange Perspective. *J. Retail. Consum. Serv.* **2023**, *74*, 103385. [\[CrossRef\]](#)
71. Pankomera, R.; van Greunen, D. Opportunities, Barriers, and Adoption Factors of Mobile Commerce for the Informal Sector in Developing Countries in Africa: A Systematic Review. *Electron. J. Inf. Syst. Dev. Ctries.* **2019**, *85*, e12096. [\[CrossRef\]](#)
72. Martins, R.M.; Ferraz, S.B.; Fagundes, A.F.A. “Fundamentalist, Pragmatic, or Unconcerned?”: An Analysis of Consumers' Willingness to Disclose Information Online. *RAUSP Manag. J.* **2024**, *59*, 31–49. [\[CrossRef\]](#)
73. Yu, J. Explaining Inconsistent Privacy Effects: How Cognitive–Affective Inconsistency and Ambivalence Shape Online Information Disclosure. *J. Theor. Appl. Electron. Commer. Res.* **2026**, *21*, 58. [\[CrossRef\]](#)

74. Chen, M.; Chen, M. Trust, Privacy Fatigue, and the Informed Consent Dilemma in Mobile App Privacy Pop-Ups: A Grounded Theory Approach. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 179. [[CrossRef](#)]
75. Miltgen, C.L.; Smith, H.J. Falsifying and Withholding: Exploring Individuals' Contextual Privacy-Related Decision-Making. *Inf. Manag.* **2019**, *56*, 696–717. [[CrossRef](#)]
76. Burkhardt, G.; Boy, F.; Doneddu, D.; Hajli, N. Privacy Behaviour: A Model for Online Informed Consent. *J. Bus. Ethics* **2023**, *186*, 237–255. [[CrossRef](#)]
77. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information Privacy Practices in E-Government in an African Least Developing Country, Rwanda. *Electron. J. Inf. Syst. Dev. Ctries.* **2019**, *85*, e12074. [[CrossRef](#)]
78. Madane, Y.; Azeroual, M. Perceived Intrusiveness vs. Relevance: A PLS-SEM Analysis of Personalized Advertising in Morocco. *Digital* **2025**, *5*, 63. [[CrossRef](#)]
79. Krasnova, H.; Veltri, N.F.; El Garah, W. Effectiveness Of Justice-Based Measures In Managing Trust And Privacy Concerns On Social Networking Sites: An Intercultural Perspective. *Commun. Assoc. Inf. Syst.* **2014**, *35*, 4. [[CrossRef](#)]
80. Nuzulita, N.; Subriadi, A.P. The Role of Risk-Benefit and Privacy Analysis to Understand Different Uses of Social Media by Generations X, Y, and Z in Indonesia. *Electron. J. Inf. Syst. Dev. Ctries.* **2020**, *86*, e12122. [[CrossRef](#)]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.