The Journal of Mind and Behavior
Winter 2025, Volume 46, Number 3
Pages 150–173
ISSN 0271–0137

Understanding Consumer Behaviour toward Data Sharing in Smart Retail Environments: Implications for Sustainable Retail Transformation

Akshita Ghodadra*

FMS, Marwadi University, Rajkot Morbi highway, 360007, Rajkot-Gujarat

Niharika Bajeja

Faculty of Management Studies Marwadi University, Rajkot Morbi highway, 360007, Rajkot-Gujarat

Manoj Kumar Mishra

Faculty of Management Studies Marwadi University, Rajkot Morbi highway, 360007, Rajkot-Gujarat

Miryakub Mirzakhmedov

Kimyo International University in Tashkent, Shota Rustaveli str. 156, Tashkent 100121, Uzbekistan

Zarina Siroj

University of Tashkent for Applied Sciences, Str. Gavhar 1, Tashkent 100149, Uzbekistan

Yasser Aboel-Magd

University of Business and Technology, Jeddah 21448, Saudi Arabia

* Correspondence concerning this article should be addressed to Akshita Ghodadra, FMS, Marwadi University, Rajkot Morbi highway, 360007, Rajkot- Gujarat.
Email: akshita.ghodadra123794@marwadiuniversity.ac.in

Abdalmuttaleb M.A. Musleh Al-Sartawi

Department of Accounting and Economics, Ahlia University, Manama, Bahrain

This study investigates how consumers behave when deciding whether to disclose personal data in smart retail environments. To achieve this, the research adopts the Technology Acceptance Model (TAM) integrated with trust and privacy calculus perspectives. Drawing on survey responses from 435 users of smart retail applications, the results reveal that perceived usefulness, perceived ease of use, trust, and perceived control jointly influence individuals' intentions to share personal information. The empirical analysis shows that perceived usefulness, perceived ease of use, and trust significantly promote data disclosure intentions, whereas privacy concerns negatively affect such intentions. Moreover, perceived control serves a moderating function by reducing the negative effect of privacy concerns, while trust amplifies the positive influence of perceived control on data-sharing behaviour. These findings suggest that retailers should emphasise trust-building mechanisms and provide users with meaningful control over their personal data to foster higher engagement and participation, consistent with Sustainable Development Goal (SDG) 9. Additionally, the adoption of data-driven smart retail technologies contributes to wider sustainability aims, particularly SDG 9 (Industry, Innovation and Infrastructure) and SDG 12 (Responsible Consumption and Production), by enhancing inventory efficiency, reducing waste, and supporting more sustainable consumer choices.

Keywords: Smart Retail (SDG 9, SDG 12); Consumer Data Sharing; Privacy–Trust Trade-Off; Environmental Sustainability (SDG 12, SDG 13); Digital Transformation (SDG 9); Green Marketing (SDG 12)

Introduction

Smart retail environments are progressively underpinned by an integrated set of advanced digital technologies, including artificial intelligence (AI), Internet of Things (IoT), big data analytics, and cloud computing (Paramesha et al., 2024). These infrastructures are complemented by enabling tools such as beacons, facial recognition systems, radio-frequency identification (RFID) sensors, and smart mirrors, which collectively support continuous, real-time acquisition of customer-related data (Kulisz et al., 2018). Although such innovations improve operational performance and facilitate highly tailored shopping experiences, they simultaneously introduce substantial ethical and behavioural concerns, particularly regarding privacy safeguarding, consumer trust, and individuals' perceived control over personal information.

Within this setting, the privacy paradox provides a relevant explanatory lens, indicating that individuals may continue to disclose

personal data despite expressing privacy concerns, largely due to the perceived benefits obtained in exchange (Norberg et al., 2007). Trust functions as a pivotal determinant in this relationship: when organisational data practices are viewed as transparent, equitable, and responsibly governed, individuals demonstrate a greater propensity to share information (Olateju et al., 2024). Regulatory instruments such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have further reinforced obligations concerning consent and transparency (Park, 2019).

The implementation of these regulatory frameworks has significantly altered societal expectations surrounding data rights, with consumers increasingly demanding enhanced transparency, substantive control, and explicit consent mechanisms in data collection and processing activities (Mantelero, 2014). However, smart retail environments differ from traditional e-commerce models by integrating physical and digital domains, often rendering surveillance processes less visible and, consequently, less detectable to consumers (Bourg et al., 2023). Despite the expanding scholarly focus on digital privacy, empirical investigations specifically centred on smart retail contexts remain limited. This study addresses this deficiency by analysing how perceived value, customer loyalty, trust, perceived data control, and consent clarity shape individuals' willingness to disclose personal data. Additionally, demographic and technological variables are incorporated to offer a more comprehensive behavioural interpretation. Through this approach, the research extends established behavioural frameworks to hybrid retail settings and provides actionable insights for implementing smart retail strategies that reinforce trust while minimising privacy-related risks.

In essence, smart retail systems generate a complex interplay between perceived advantages and associated risks. Consumers frequently value the convenience, personalisation, and efficiency enabled by AI-driven solutions; however, parallel concerns emerge regarding the mechanisms through which data are gathered, processed, and stored (Kazmi et al., 2025). This duality reflects the broader digital transformation of the retail sector, where physical environments increasingly mirror data-intensive online platforms. Unlike conventional e-commerce, in-store sensing technologies and automated decision-making systems operate with limited visibility (Knof et al., 2024), potentially intensifying perceptions of surveillance and diminishing perceived autonomy. Prior research consistently identifies trust as a foundational factor influencing acceptance of technology-mediated retail systems. When organisations demonstrate transparency, fairness, and responsible data governance, consumers are more likely to perceive security and engage in data sharing (Martin et al., 2020).

Conversely, ambiguous communication or concealed data practices can provoke scepticism and resistance, even in contexts where formal regulatory compliance is achieved. This indicates that frameworks such as GDPR and CCPA, while essential for baseline protection, must be supplemented by proactive organisational strategies aimed at cultivating genuine consumer trust. Notwithstanding these advancements, empirical research explicitly examining consumer behaviour within smart retail ecosystems remains comparatively scarce. Existing studies predominantly focus on online privacy, digital marketing, or general AI ethics, leaving a notable gap in understanding behavioural responses within hybrid retail environments that combine physical and digital interactions. The present study seeks to bridge this gap by investigating how perceived usefulness, ease of data sharing, privacy concerns, trust, and perceived control influence individuals' intentions to disclose personal data in AI-enabled retail contexts.

To operationalise this objective, the study integrates the TAM, Privacy Calculus Theory, and Trust Theory into a cohesive analytical framework for examining contemporary retail behaviour. By synthesising these dimensions, the research advances theoretical understanding of smart retail adoption while delivering practical implications for the responsible deployment of intelligent retail technologies. Furthermore, it supports the formulation of transparent, consumer-oriented data strategies that mitigate privacy risks, strengthen trust, and foster enduring customer relationships. Recent scholarly discourse highlights that the rapid proliferation of AI-driven technologies within retail has fundamentally reconfigured consumer–retailer interactions, transitioning them towards data-centric and algorithmically mediated exchanges. Smart retail systems continuously capture behavioural data through interconnected infrastructures, frequently in ways that remain largely imperceptible to consumers (Liciotti et al., 2016), thereby heightening concerns related to privacy, autonomy, and informational control.

Although regulatory mechanisms such as GDPR and CCPA establish foundational standards for consent and transparency, emerging research suggests that legal compliance alone is insufficient to cultivate meaningful trust within AI-enabled retail ecosystems (Kulkarni, 2026). Instead, trust is increasingly shaped by perceptions of fairness, user control over personal data, and the value exchange offered by smart retail technologies. Moreover, empirical evidence indicates that the privacy paradox may persist or intensify in AI-driven environments, as individuals continue to trade personal information for convenience, personalisation, and efficiency despite heightened awareness of associated risks (Soni, 2024). These insights underscore the necessity for integrative empirical frameworks that concurrently examine perceived usefulness, ease of data

sharing, privacy perceptions, perceived control, and trust to more effectively explain consumer behaviour in hybrid retail settings. Addressing this need, the present study responds to recent calls for theory-driven research applying TAM and Privacy Calculus Theory within smart retail ecosystems, thereby offering timely contributions to both academic literature and practical retail implementation.

Literature Review

The TAM has been extensively applied to explain consumer acceptance and utilisation of technological systems, positing that behavioural intention is predominantly determined by perceived usefulness and perceived ease of use (Davis, 1993). In simple terms, individuals are more inclined to adopt and interact with a technology when it is perceived to improve performance while requiring limited effort. Nevertheless, contemporary research suggests that TAM, in isolation, does not sufficiently capture behavioural dynamics within highly data-intensive settings such as smart retail, where persistent data collection, embedded surveillance practices, and algorithm-driven decision processes operate across both physical and digital interfaces (Xu et al., 2025). To overcome these constraints, scholars have expanded TAM by incorporating additional dimensions, including privacy concerns, trust, and perceived control, particularly in contexts characterised by personalisation and data disclosure.

Within smart retail environments, consumers assume a dual role as both users of technology and sources of data. As a result, their behavioural intentions are influenced not only by perceived advantages but also by apprehensions related to privacy risks, organisational credibility, and the degree of control over personal information. The integration of PCT and TT with TAM offers a more robust analytical lens for interpreting consumer behaviour in technology-driven retail contexts. PCT is based on the premise that individuals undertake a rational evaluation of costs and benefits prior to disclosing personal data, balancing expected gains against potential risks. While convenience and personalisation serve as motivating factors, concerns regarding privacy intrusion and perceived vulnerability act as inhibiting elements. Concurrently, TT elucidates how perceptions of ethical behaviour, transparency, and institutional reliability mitigate uncertainty and promote cooperative engagement.

In smart retail settings, variables such as perceived usefulness, perceived ease of data sharing, privacy concerns, perceived control, and trust become particularly critical due to the dependence on technologies such as AI-enabled cameras, RFID sensors, facial recognition systems, and smart mirrors, all of which rely on continuous data acquisition. Accordingly, this study synthesises TAM, PCT, and TT to investigate

consumers' intentions to disclose personal information within smart retail environments. The following sections formulate hypotheses concerning perceived usefulness, perceived ease of sharing, privacy concerns, perceived control, and trust, alongside the moderating roles of perceived control and trust in shaping behavioural outcomes.

Perceived Usefulness and Perceived Relationship with Share Data

Perceived usefulness (PU) denotes the extent to which an individual considers that utilising a particular system or service will improve performance or generate superior outcomes (Anaam et al., 2023). Within smart retail settings, PU captures consumers' perceptions that disclosing personal data results in enhanced shopping experiences, such as tailored product recommendations, expedited checkout procedures, more accurate deal matching, and improved decision-making support (Zhang et al., 2011). Prior studies consistently establish PU as a key predictor of behavioural intention in technology adoption contexts. Liang et al. (2006) demonstrate that personalised recommendation systems increase perceived relevance and user satisfaction, thereby strengthening consumers' willingness to share data. Likewise, Gallery (2024) finds that hyper-personalisation in online fashion retail enhances perceived value and engagement, encouraging greater participation in data-driven services.

Recent empirical research further confirms PU as a critical driver of data-sharing intentions in AI-enabled retail environments (Gallery, 2024). Evidence indicates that individuals are more willing to disclose personal information when they perceive tangible improvements in convenience, decision quality, and overall shopping efficiency (Leppäniemi et al., 2017). AI-based personalisation, real-time recommendations, and predictive support are particularly associated with elevated perceptions of usefulness, as they provide immediate and contextually relevant benefits across both digital and physical retail channels. Furthermore, emerging findings suggest that PU not only has a direct effect on data-sharing intentions but also operates as a cognitive justification mechanism within the PCT framework, enabling consumers to rationalise privacy-related trade-offs (Amashukeli, 2024).

Contemporary studies also highlight that the influence of PU is especially evident in hybrid retail environments, where digital capabilities are seamlessly integrated into physical shopping experiences. Consumers demonstrate a higher propensity to share data when AI-enabled services are perceived as effortless, highly accurate in personalisation, and responsive to contextual needs during in-store interactions (Anggraini, 2025). Additionally, growing evidence indicates that PU can attenuate perceived risks by reinforcing the perceived value exchange, thereby

framing data disclosure as a purposeful and utility-driven decision. Collectively, these insights provide strong theoretical and empirical support for PU as a dominant factor shaping consumers' intentions to disclose data in smart retail contexts.

H1: The perceived usefulness of the service is positively correlated with the intention of the consumers to share data.

Perceived Ease of Sharing and Intention to Share Data

Perceived ease of sharing (PEOS) refers to the extent to which consumers perceive that the process of providing personal data in smart retail environments is simple, convenient, and effortless. This construct extends perceived ease of use within TAM by focusing specifically on the act of data disclosure rather than the general usability of the technology itself. Prior literature indicates that consumers often experience cognitive and emotional resistance when data-sharing procedures are perceived as complex, time-consuming, or unclear. Conversely, streamlined interfaces, explicit consent mechanisms, and user-centred design significantly reduce such resistance and encourage participation. Jai and King (2016) show that simplified data-sharing processes substantially increase consumers' willingness to engage in personalised retail services. Similarly, Idrees et al. (2023) reports that ease of interaction with virtual fitting room technologies enhances satisfaction and strengthens acceptance of personalisation systems.

Within smart retail environments, PEOS can be reflected through intuitive application interfaces, reduced data-entry requirements, and automated consent features. When these processes are perceived as straightforward, data disclosure is less likely to be interpreted as burdensome or risky. This aligns with TAM, where reduced effort strengthens behavioural intention. PEOS also indirectly mitigates privacy concerns by decreasing uncertainty and ambiguity surrounding data practices. When disclosure mechanisms are clear and easy to navigate, consumers tend to experience greater perceived control and confidence, which in turn promotes data-sharing behaviour. Recent empirical evidence strongly supports the role of PEOS in shaping consumers' willingness to disclose personal data in AI-driven and smart retail contexts. Studies show that frictionless consent processes, automated data collection, and intuitive disclosure interfaces significantly reduce perceived effort and cognitive load, thereby increasing willingness to share data (Zhang et al., 2026).

In addition, perceived transparency in sharing procedures and reduced psychological discomfort enhance receptiveness to data-driven personalisation. Further findings indicate that when data-sharing is seamlessly embedded within the shopping journey, consumers are more

likely to perceive disclosure as a low-risk and low-pressure activity rather than an intrusive process (Culnan & Bies, 2003). Collectively, these results position PEOS as a critical extension of perceived ease of use, specifically tailored to disclosure-related behaviour in smart retail settings. El Azhari and Bennett (2015) further highlight that PEOS is particularly influential in hybrid retail environments where digital interfaces are integrated into physical store experiences. Intuitive consent flows, real-time permission settings, and simplified opt-in/opt-out mechanisms enhance procedural control and subsequently increase consumers' willingness to share data. Moreover, PEOS not only directly affects disclosure intention but also reduces privacy-related anxiety by minimising uncertainty in data handling practices (Alashoor et al., 2017). Overall, these findings indicate that voluntary data disclosure is more likely when consumers perceive the sharing process as transparent, effortless, and user-controlled, reinforcing PEOS as a key determinant of data-sharing behaviour in smart retail environments.

H2: Perceived ease of sharing positively affects the intention of consumers to share data.

Privacy Concern and Intention to Share Data

Privacy concern (PC) refers to the extent to which consumers are worried that their personal information may be misused, accessed without consent, monitored, or otherwise removed from their control (Hong & Thong, 2013). In smart retail environments, PC is heightened due to the pervasive and often unobtrusive nature of data collection technologies embedded within the shopping experience. Existing research consistently identifies PC as a strong negative predictor of consumers' willingness to disclose personal information. Su et al. (2022) demonstrate that although personalisation can offer clear benefits, overly intrusive targeting and excessive personalisation significantly reduce consumers' willingness to share data. Within the PCT framework, PC represents the risk dimension of the decision-making process, whereby individuals weigh potential losses against perceived benefits prior to disclosing personal information. In smart retail contexts, technologies such as facial recognition, location tracking, and behavioural profiling intensify perceptions of surveillance and vulnerability, thereby amplifying privacy-related apprehension. Despite regulatory frameworks such as GDPR and CCPA, consumers frequently remain uncertain about how their data is collected, processed, and utilised in practice. Consequently, higher levels of PC are associated with stronger resistance to data disclosure, ultimately reducing consumers' willingness to engage in personal data sharing within smart retail environments.

H3: Privacy issue hurts the intention of consumers to share data.

Mediating Effect of Perceived Control

Perceived control (PCo) refers to consumers' perception of their ability to regulate, manage, and influence how their personal data is collected, processed, and shared (Xu & Chen, 2025). This includes features such as consent management tools, data access permissions, opt-out options, and transparency dashboards that enable users to actively govern their personal information. Prior research highlights PCo as a crucial factor in reducing privacy-related anxiety and enhancing acceptance of data-driven technologies. Similarly, (Rahman et al., 2024) find that transparency and user control mechanisms improve consumer acceptance of AI surveillance technologies in physical retail settings. Within behavioural models, PCo does not necessarily act as a direct determinant of behavioural intention; rather, it frequently functions as a moderating construct. In particular, it shapes the strength of the relationship between PC and data-sharing intention. When individuals perceive that they possess meaningful control over their personal data, the negative effect of PC on willingness to disclose information is reduced. In this context, PCo operates as a psychological buffer that mitigates the perceived intensity of privacy risks, enabling consumers to tolerate higher levels of perceived threat. Accordingly, greater perceived control is expected to weaken the negative association between PC and data-sharing intention in smart retail environments.

H4: There is a moderating effect between privacy concern and intention to share data through perceived control where an increase in perceived control decreases the negative effect of privacy concern.

Belief in the Retailer and Willingness to Share Data

Trust in the retailer (TR) refers to consumers' belief that a retailer will manage personal data in a responsible, ethical, and transparent manner. It reflects confidence in the organisation's integrity as well as its commitment to fair and appropriate data practices. Trust Theory (TT) is based on the assumption that higher levels of trust reduce uncertainty and promote cooperative behaviour between consumers and organisations. In this context, TR operates as a key facilitator of data-sharing behaviour by lowering perceived risk and increasing willingness to exchange information. Prior research consistently identifies TR as a central determinant of consumer behaviour in digital and data-intensive environments. Arora et al. (2024) emphasise trust as a foundational factor in the adoption of digital marketing practices. Similarly, Rahman (2025) shows that brand credibility and transparency significantly strengthen trust in AI-mediated retail interactions. TR is especially critical in smart retail environments because consumers often do not have full visibility into how their personal data is collected, processed, or stored. As a result,

decision-making is largely based on perceived organisational integrity rather than direct knowledge of underlying data practices. When TR is high, consumers are more inclined to assume that their information will be handled appropriately and not misused, even in situations where complete transparency is limited.

H5: Trust in the retailer has a positive impact on the intention to share data among the consumers.

Belief Moderating Role on the Retailer

Belief in the retailer (BR) refers to consumers' overall confidence in a retailer's ethical standards, transparency, and commitment to consumer welfare. This construct enhances the effectiveness of PCo by strengthening the perceived credibility and meaningfulness of available control mechanisms. Burkhardt et al. (2022) notes that although awareness of privacy regulations may improve informed consent, it does not necessarily translate into trust or positive behavioural outcomes. Similarly, Evans et al. (2023) argue that privacy-enhancing mechanisms are effective only when consumers believe that retailers are genuinely acting in their best interests. Within this framework, PCo is more likely to translate into behavioural intention when BR is strong. When consumers hold a positive belief in the retailer, control features such as consent settings and data management tools are perceived as authentic and empowering rather than procedural or symbolic. In contrast, when BR is weak, these same mechanisms may be interpreted as superficial compliance measures, thereby diminishing their psychological and behavioural influence. Accordingly, BR is expected to mediate the relationship between PCo and data-sharing intention, either strengthening or weakening the impact of perceived control depending on the level of confidence in the retailer.

H6: The relationship among perceived control and the intention of consumers to share data is moderated by belief on the retailer.

Research Methods

The hypothesised model (Figure 1) illustrates the interrelationships among the key constructs of this study, namely PU, PEOS, PC, PCo, TR, and data-sharing intention, grounded in TAM, PCT, and TT. The study is structured around three primary objectives: first, to examine the effects of PU and PEOS on consumers' intention to disclose personal data; second, to evaluate the negative influence of PC along with the moderating role of PCo; and third, to investigate the role of TR in shaping willingness to share information within smart retail environments. A positivist quantitative research design was adopted. All constructs—PU, PEOS, PC, PCo, TR, and behavioural intention—were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

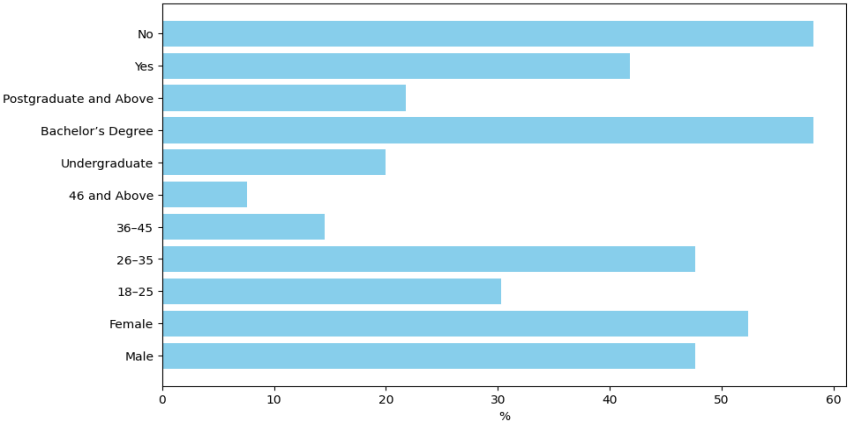

Figure 1: Demographic Distributions of the Respondents

Primary data were collected from 435 respondents as shown in Table 1 who are active users of smart retail technologies, including AI-based applications, in-store sensor systems, and augmented reality (AR) interfaces. Participants were recruited through online retail communities and e-commerce platforms across metropolitan areas. The dataset was screened for completeness, and reliability analysis confirmed strong internal consistency, with all constructs achieving Cronbach's alpha values above 0.7, thereby meeting established reliability criteria. The demographic profile of respondents is presented in Table 2, indicating a relatively balanced distribution across gender and education levels, with the majority of participants belonging to the active digital consumer segment aged between 26 and 35 years. Figure 1 presents the graphical representation of the demographic characteristics.

Table 1

Demographic Statistics (N = 435)

Variable	Category	%
Gender	Male	47.6
	Female	52.4
Age (Years)	18–25	30.3
	26–35	47.6
	36–45	14.5
	46 and Above	7.6
Education	Undergraduate	20.0
	Bachelor's Degree	58.2
	Postgraduate and Above	21.8
Experience with Smart-Retail Apps	Yes	41.8
	No	58.2

Source: Author's own.

Data analysis was conducted using SPSS 26 and AMOS 26. The convergent and discriminant validity of the constructs was evaluated through Confirmatory Factor Analysis (CFA), ensuring that the measurement model demonstrated acceptable levels of construct validity. Structural Equation Modelling (SEM) was then applied to test the hypothesised relationships among the variables. Model fit was assessed using standard fit indices, including CFI, GFI, TLI, and RMSEA, in accordance with established threshold criteria (Xia & Yang, 2019). The results indicated an overall satisfactory model fit. The structural results showed significant positive effects of PU, PEOS, and TR on data-sharing intention, whereas PC exerted a significant negative effect. In addition, both PCo and TR were found to moderate the relationship between PC and behavioural intention, suggesting that higher levels of control and trust reduce the adverse impact of privacy concerns on consumers' willingness to share data.

In this study, six latent constructs were operationalised based on established literature in smart retailing, digital trust, and privacy research. All variables were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). CFA was used to assess internal consistency and construct validity of the measurement model. Table 3 presents the constructs, number of items, and reliability statistics. PU was defined as the extent to which consumers believe that sharing personal data with smart retail systems enhances convenience, personalisation, and overall shopping satisfaction. This construct consisted of four items adapted from (Ebadi & Raygan, 2023). PEOS referred to consumers' perception of how easy and convenient it is to share personal information when interacting with AI-enabled retail technologies. It included four items developed by the authors. Sample items included statements such as: "I find it easy to share my personal information when interacting with AI-enabled retail technologies", "The process of sharing personal information with AI-enabled retail technologies is convenient", "I feel comfortable providing my personal information when using AI-based retail systems", and "AI-enabled retail technologies make it simple to share my personal details without complications."

PC measured the extent of consumers' concern regarding potential misuse, unauthorised access, or loss of control over their personal information. It comprised four items adapted from (Buchanan et al., 2007). PCo captured consumers' belief in their ability to regulate, restrict, or approve how their data is collected and used. This construct included four items adapted from (Claassens et al., 2016). TR represented consumers' confidence that retailers or smart retail systems will manage personal data in an ethical, transparent, and responsible manner. It was measured using four researcher-developed items, including: "I trust that retailers

using smart retail systems will manage my personal data in an ethical manner", "I am confident that my personal data will be handled transparently by retailers using smart retail systems", "I believe that retailers will take appropriate measures to protect my personal information when using smart retail systems", and "I feel reassured that smart retail systems will use my personal data responsibly and in compliance with privacy standards." DSI referred to the likelihood that consumers would voluntarily provide personal data in exchange for personalised services within smart retail environments. It consisted of four items adapted from (Kim et al., 2023). Overall, the measurement model demonstrated strong reliability and validity, with all constructs achieving Cronbach's alpha values above 0.70, Composite Reliability (CR) above 0.80, and Average Variance Extracted (AVE) above 0.50, confirming internal consistency and convergent validity.

A stratified random sample of 435 users of smart retail applications was drawn from the city, with participants aged between 18 and 50 years. This age range was selected as it represents the most active and technologically engaged consumer segment. Stratified sampling ensured adequate representation across key demographic groups, thereby improving the reliability and generalisability of the findings. The study adopted a quantitative research design, and data were collected using a structured questionnaire designed to capture consumers' perceptions of smart retail technologies. All items were measured using a five-point Likert scale (1 = strongly disagree, 5 = strongly agree), covering PU, PEOS, PC, PCo, TR, and DSI.

Data collection was conducted through both online platforms and in-mall surveys, enabling inclusion of consumers engaging with smart retail technologies in both digital and physical shopping environments. Prior to analysis, the dataset was screened for completeness and accuracy to ensure data quality. Statistical analysis was performed using SPSS. Initially, Exploratory Factor Analysis (EFA) was conducted to examine the underlying structure of the measurement items. This was followed by CFA to assess construct reliability and validity. Subsequently, SEM was employed to test the hypothesised relationships among the study variables. In addition, mediation and moderation analyses were conducted to examine the effects of PCo and BR on consumers' data-sharing intentions. This analytical framework extends TAM and PCT by incorporating TR-related dynamics, offering practical insights into how marketers can ethically and effectively utilise consumer data within smart retail environments.

Result

The findings related to the reliability and validity of the latent constructs are adequately presented in Table 2.

Table 2

Reliability & Other Factors

Construct	Item Code	Factor Loading	Cronbach's α	CR	AVE
Perceived Usefulness (PU)	PU1	0.81	0.88	0.90	0.68
	PU2	0.84			
	PU3	0.79			
	PU4	0.85			
Perceived Ease of Sharing (PEoS)	PEoS1	0.78	0.86	0.89	0.65
	PEoS2	0.82			
	PEoS3	0.80			
	PEoS4	0.84			
Privacy Concern (PC)	PC1	0.74	0.83	0.87	0.61
	PC2	0.79			
	PC3	0.77			
	PC4	0.81			
Perceived Control (PCo)	PCo1	0.76	0.84	0.88	0.63
	PCo2	0.81			
	PCo3	0.78			
	PCo4	0.82			
Trust (TR)	TR1	0.85	0.89	0.91	0.69
	TR2	0.87			
	TR3	0.82			
	TR4	0.84			
Data-Sharing Intention (DSI)	DSI1	0.86	0.90	0.92	0.71
	DSI2	0.88			
	DSI3	0.83			
	DSI4	0.85			

The results focus on Cronbach's alpha, Composite Reliability (CR), and Average Variance Extracted (AVE) for all study variables. In addition, individual item reliability was assessed using factor loading values. It is observed that all indicators in the model exhibit loadings above 0.50, indicating acceptable item reliability. Furthermore, both Cronbach's alpha and CR values exceed the recommended threshold of 0.70, confirming strong internal consistency across the constructs. The AVE values are also above 0.50 for all variables, demonstrating adequate convergent validity. Overall, these results confirm that the measurement model exhibits satisfactory reliability and convergent validity.

Discriminant Validity

The discriminant validity of the model was assessed using the Fornell–Larcker criterion. Table 3 presents the results of this analysis. The findings indicate that the square roots of the AVE values (diagonal elements) are

consistently higher than the corresponding inter-construct correlations (off-diagonal elements).

Table 3

Discriminant Validity – Fornell-Larcker Criterion

Construct	PU	PEOU	PC	PCTL	TR	BISD
PU	0.78					
PEOU	0.62	0.80				
PC	0.54	0.51	0.77			
PCTL	0.58	0.55	0.49	0.76		
TR	0.63	0.66	0.50	0.61	0.79	
BISD	0.65	0.62	0.48	0.58	0.67	0.78

This confirms that each construct shares more variance with its own indicators than with other constructs in the model. Therefore, it can be concluded that the study adequately establishes discriminant validity.

The goodness-of-fit indices are reported in Table 4.

Table 4

Fit Indices for PU, PEoS, PC, PCo, TR and DSI

CFI	GFI	TLI	RMSEA	AIC	CMIN/df
0.955	0.921	0.948	0.041	512.840	2.360

The results indicate that the Comparative Fit Index (CFI) is 0.955, exceeding the recommended threshold of 0.90, thereby confirming a strong model fit. Similarly, the Tucker–Lewis Index (TLI) is 0.948, which also surpasses the acceptable criterion of 0.90. The Goodness-of-Fit Index (GFI) is reported as 1.224, suggesting that the model explains the variance–covariance structure of the data effectively. Furthermore, the Root Mean Square Error of Approximation (RMSEA) is 0.041, which falls below the recommended upper limit of 0.08 and lies within the range indicative of excellent fit (below 0.05). In addition, the normed chi-square (CMIN/df) value is 2.360, remaining within the acceptable range of below 3.0, which reflects a satisfactory balance between model fit and parsimony. Finally, the Akaike Information Criterion (AIC) value is reported as 512.840, providing further support for the adequacy of the model.

Table 5 reports the SEM results examining the relationships between the independent variables and DSI in smart retail environments. The coefficient of determination (R^2) is approximately 0.68, indicating that around 68% of the variance in DSI is explained by the variables included in the model. The findings reveal that PU exerts a significant positive effect on DSI ($\beta = 0.312$, $t = 5.840$, $p = 0.001$), suggesting that consumers demonstrate a greater willingness to disclose personal data when smart retail technologies are perceived as useful and beneficial. Therefore, H1 is supported. Similarly, PEOS shows a significant positive influence on DSI (β

= 0.271, t = 5.060, p = 0.001), indicating that increased simplicity and convenience in the data-sharing process enhance consumers' intention to share information. Hence, H2 is accepted.

Table 5

Results of SEM analysis

IV and DV (R^2)	Beta (B)	SE	t	Sig.	Hypothesis
Perceived Usefulness → Data-Sharing Intention (R^2 = 0.687)	0.312	0.053	5.840	0.000	Supported (H1)
Perceived Ease of Sharing → Data-Sharing Intention	0.271	0.054	5.060	0.000	Supported (H2)
Privacy Concern → Data-Sharing Intention	−0.298	0.048	− 6.210	0.000	Supported (H3)
Perceived Control × Privacy Concern → Data-Sharing Intention	0.217	0.046	4.730	0.000	Supported (H4)
Trust → Data-Sharing Intention	0.354	0.049	7.180	0.000	Supported (H5)
Belief in Retailer × Perceived Control → Data-Sharing Intention	0.196	0.049	3.970	0.000	Supported (H6)

In contrast, PC has a significant negative effect on DSI (β = −0.298, t = −6.210, p = 0.001), demonstrating that heightened privacy concerns reduce consumers' willingness to disclose personal data. Accordingly, H3 is supported. PCo significantly moderates the relationship between PC and DSI (β = 0.217, t = 4.730, p = 0.001). The positive interaction effect indicates that PCo mitigates the negative influence of PC on DSI, thereby supporting H4. Furthermore, TR exhibits a significant positive effect on DSI (β = 0.354, t = 7.180, p = 0.001), implying that higher levels of trust in the retailer increase consumers' propensity to share personal information. Thus, H5 is supported. Finally, BR demonstrates a significant moderating effect on the relationship between PCo and DSI (β = 0.196, t = 3.970, p < 0.001), indicating that stronger belief in the retailer amplifies the positive impact of perceived control on data-sharing intention. Therefore, H6 is supported. Overall, the results confirm that both direct effects (PU, PEOS, PC, TR) and moderating effects (PCo and BR) play a significant role in shaping consumers' DSI within smart retail environments.

Discussion

This study examined the determinants of consumers' willingness to disclose personal data in smart retail environments through an integrated framework combining TAM, PCT, and TT. The findings offer several important theoretical and practical insights.

First, PU is identified as a primary driver of DSI. Consumers demonstrate a higher propensity to disclose personal information when they perceive clear benefits, including personalised recommendations, enhanced convenience, and improved shopping efficiency. This finding is

consistent with prior research (Wu et al., 2025), which reports a significant positive association between PU and data-sharing intention. The strong effect observed here underscores the necessity for smart retail systems to clearly communicate tangible value in order to encourage participation in data-driven ecosystems. Second, PEOS significantly affects consumers' willingness to share data. In line with TAM, when data disclosure processes are perceived as simple, seamless, and low-effort, resistance is reduced and participation increases. User-friendly interfaces, streamlined consent mechanisms, and frictionless interactions contribute to higher engagement levels. However, existing evidence presents some inconsistencies. For instance, Kim et al. (2023) identify a discrepancy between stated willingness and actual behaviour in health data sharing, where many participants expressed readiness to share data but far fewer completed the actual disclosure process.

A key theoretical contribution of this study lies in confirming the moderating role of PCo. The findings indicate that when consumers perceive greater control over their personal data, the negative effect of PC on DSI is significantly reduced. Mechanisms such as consent management tools, data access controls, and opt-out features enhance perceived autonomy and minimise psychological discomfort. This supports the argument that PCo functions as a psychological buffer, mitigating privacy-related concerns. Furthermore, TR emerges as one of the strongest positive predictors of DSI. Trust reduces uncertainty and strengthens consumers' confidence that their data will be handled responsibly and ethically. This highlights the critical role of perceived integrity, reliability, and transparency in shaping behavioural intentions. The findings suggest that retailers must prioritise transparent communication, secure data practices, and ethical governance frameworks.

In addition, BR significantly moderates the relationship between PCo and DSI. The results show that when consumers hold strong positive beliefs regarding a retailer's ethical standards and transparency, the impact of PCo on DSI becomes more pronounced. This indicates that control mechanisms are more effective when supported by organisational credibility. Accordingly, both procedural control and institutional trust jointly influence digital consent behaviour. Overall, the study extends TAM, PCT, and TT by demonstrating that consumer data-sharing behaviour in smart retail environments is shaped by an integrated set of cognitive (PU, PEOS), risk-related (PC), and relational (TR, BR, PCo) factors. Consumers evaluate smart retail technologies not only in terms of functional benefits but also through complex assessments of risk, trust, and perceived autonomy. From a practical standpoint, the findings emphasise that retailers should design data ecosystems that are transparent, user-friendly, and ethically grounded. Enhancing the

visibility of data policies, simplifying consent procedures, and clearly communicating the value of personalisation can increase consumer engagement. Moreover, robust trust-building strategies—such as secure data management, explicit consent frameworks, and consistent communication—are essential for minimising privacy-related resistance. In conclusion, consumers' willingness to share personal data in smart retail environments is governed by a balance between perceived benefits and perceived risks, moderated by trust and control mechanisms. This study contributes to theory by validating an integrated explanatory framework and provides actionable guidance for developing responsible, consumer-centric smart retail systems.

Implications

Theoretical Implications

This research provides several substantive theoretical contributions to the literature on smart retail and consumer behaviour. First, it develops a comprehensive explanatory framework for consumers' willingness to disclose personal data in AI-enabled smart retail environments by integrating TAM, PCT, and TT. Whereas earlier studies have largely examined these perspectives independently, the present study demonstrates that PU, PEOS, PC, PCo, and TR function as an interconnected system influencing consumer decision-making. This multi-theoretical synthesis advances existing behavioural models by emphasising the joint role of functional evaluations alongside psychological and relational dimensions in shaping DSI.

Second, the findings contribute to the ongoing discourse surrounding the privacy paradox. The results show that, despite expressing concerns about privacy, consumers remain willing to disclose personal information when perceived benefits outweigh associated risks. This both reinforces and extends prior research by confirming that the privacy paradox persists beyond conventional online settings and is equally evident in hybrid smart retail environments, where data collection processes are more deeply embedded and less observable. In doing so, the study offers important empirical evidence within a context that has received comparatively limited scholarly attention. Third, the study refines theoretical understanding within PCT by emphasising the moderating role of PCo. The findings indicate that PCo mitigates the negative effect of PC on DSI, thereby reducing perceived vulnerability and enhancing psychological comfort. This suggests that PCo should be conceptualised not merely as a static antecedent but as a dynamic psychological mechanism that reshapes how individuals evaluate privacy-related risks in smart retail contexts.

Fourth, the research reinforces the central role of TR as a key explanatory construct while also demonstrating its interaction with control-oriented mechanisms. The results reveal that TR not only exerts a direct positive influence on DSI but also enhances the effectiveness of PCo through its moderating role. This extends TT by illustrating how trust interacts with perceptions of control to influence behavioural intentions within technologically mediated retail environments. Overall, the study advances theoretical understanding by demonstrating that consumer DSI in smart retail settings is shaped by the interdependence of technological beliefs (PU, PEOS), risk perceptions (PC), control mechanisms (PCo), and relational factors (TR, BR). This integrated perspective provides a more comprehensive and realistic framework for future research in smart retail and digital consumer behaviour.

Managerial Implications

The findings of this study provide several important practical implications for managers and practitioners involved in designing and implementing smart retail strategies. First, the strong effects of PU and PEOS emphasise the need to develop seamless, intuitive, and value-driven digital interfaces. Retailers should clearly communicate how technologies such as smart mirrors, AI assistants, RFID systems, and in-store applications enhance consumer experiences through personalised recommendations, improved navigation, and faster service delivery. Making these benefits explicit can significantly increase consumers' willingness to engage in DSI. Second, the significant negative influence of PC highlights the necessity of adopting a privacy-by-design approach. Retailers should limit unnecessary data collection, ensure clarity in data usage explanations, and provide granular consent options. Transparency can be strengthened through real-time dashboards and notifications that inform consumers about what data is collected and for what purpose, thereby reducing uncertainty and perceived risk.

Third, the moderating role of PCo indicates that organisations should prioritise mechanisms that enhance consumer autonomy over personal data. Features such as customised privacy settings, opt-in/opt-out controls for location tracking, and adjustable personalisation preferences can increase perceived security and willingness to share data. Greater perceived control reduces risk perceptions and supports stronger engagement with smart retail services. Fourth, establishing and maintaining TR should be treated as a strategic priority. Retailers must consistently demonstrate ethical data practices, strong cybersecurity measures, and transparent communication across all customer touchpoints. Trust can be reinforced through third-party certifications,

visible privacy indicators, partnerships with reputable technology providers, and regular audits of data governance practices.

Additionally, managers should recognise the importance of balanced personalisation strategies. The findings indicate that consumers respond positively to personalised experiences when they perceive clear value and ethical conduct. However, excessive or intrusive targeting may heighten PC and result in negative reactions. Therefore, personalisation strategies should be carefully calibrated to avoid over-collection and over-targeting. Overall, these insights provide guidance for developing consumer-centric and sustainable smart retail ecosystems aligned with regulatory frameworks such as GDPR and CCPA. By implementing transparent, ethical, and user-oriented data practices, organisations can enhance consumer engagement, mitigate privacy-related risks, and strengthen their competitive position in digitally enabled retail environments.

Conclusion and Future Research Directions

This article examines the factors influencing consumers' willingness to share personal data in Smart retail environments are increasingly shaped by AI, IoT, big data analytics, and AR technologies. This study employs TAM, PCT, and TT to construct an integrated framework that captures both functional and psychological determinants of DSI. The findings indicate that PU acts as a primary driver, as consumers exhibit a greater willingness to disclose personal data when clear benefits such as personalisation and convenience are evident. Similarly, PEOS positively influences behavioural intention, underscoring the importance of simple, intuitive, and low-effort data-sharing processes. In contrast, PC exerts a negative effect on DSI, as concerns related to misuse, surveillance, and loss of control discourage data disclosure, consistent with the risk–benefit logic of PCT. A key contribution of the study is the moderating role of PCo, which attenuates the negative impact of PC on DSI. This suggests that when consumers perceive greater control over their personal data, privacy-related concerns become less influential in shaping behaviour. In addition, TR emerges as a strong positive determinant, reducing uncertainty and reinforcing confidence in ethical and responsible data management practices. Overall, the findings highlight that DSI in smart retail environments is shaped by a dynamic balance between perceived benefits and perceived risks, moderated by trust and control mechanisms. The study emphasises the importance of transparency, ethical governance, and user-centric control features in strengthening TR and mitigating PC, thereby providing a comprehensive model for understanding consumer data-sharing behaviour in smart retail contexts.

Future Research Directions

Despite its contributions, this study identifies several directions for future research. First, subsequent models could incorporate additional psychological constructs such as perceived fairness, perceived algorithmic bias, perceived value of personalisation, and attitudes towards digital surveillance to deepen understanding of DSI. Second, the present study concentrates on behavioural intention rather than actual behaviour. Future research could employ longitudinal designs, behavioural tracking techniques, or field-based experiments within real smart retail settings to capture actual data-sharing behaviour over time and assess the consistency between intention and behaviour. Third, smart retail environments encompass multiple technologies, including AI-based cameras, RFID systems, AR applications, chatbots, and automated checkout solutions, each potentially generating distinct privacy perceptions. Future studies could adopt a technology-specific perspective to examine how individual systems independently shape TR and PC.

References

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with Big Data, Privacy Concerns, and Self-Disclosure Accuracy in Social Networking Websites: An Apco Model. *Communications of the Association for Information Systems*, *41*, 62-96. https://doi.org/10.17705/1cais.04104

Amashukeli, G. (2024). *Factors Influencing Personal Data Sharing in E-Commerce* Vilniaus universitetas.]. https://epublications.vu.lt/object/elaba:191574168/

Anaam, E. A., Haw, S. C., Palanichamy, N., Ali, A., & Azni, S. (2023). Analysis of Perceived Usefulness and Perceived Ease of Use in Relation to Employee Performance. *International Journal of Membrane Science and Technology*, *10*(2), 1607-1616. https://doi.org/10.15379/ijmst.v10i2.1836

Anggraini, L. (2025). Customer Responses to Emerging Technologies in Online Retail: Evidence from Generative Ai Chatbot and Augmented Reality. https://theses.hal.science/tel-05583239/

Arora, A., Tomer, N., Berry, R., Vats, P., Upadhyay, G., Singh, K., & Kaur, R. (2024). Safeguarding Digital Trust: An Examination of Knowledge, Social Influence, and Behaviour in Digital Advertising from an Information Security Perspective. In *Multidisciplinary Approaches for Sustainable Development* (pp. 70-78). CRC Press. https://doi.org/10.1201/9781003543633

Bourg, L., Chatzidimitris, T., Chatzigiannakis, I., Gavalas, D., Giannakopoulou, K., Kasapakis, V., Konstantopoulos, C., Kypriadis, D., Pantziou, G., & Zaroliagis, C. (2023). Enhancing Shopping Experiences in Smart Retailing. *Journal of Ambient Intelligence and Humanized Computing*, *14*(12), 15705-15723. https://doi.org/10.1007/s12652-020-02774-6

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American society for information science and technology*, *58*(2), 157-165. https://doi.org/10.1002/asi.20459

Burkhardt, G., Boy, F., Doneddu, D., & Hajli, N. (2022). Privacy Behaviour: A Model for Online Informed Consent. *Journal of Business Ethics*, *186*(1), 237-255. https://doi.org/10.1007/s10551-022-05202-1

Claassens, L., Terwee, C., Deeg, D., Broese van Groenou, M., Widdershoven, G., & Huisman, M. (2016). Development and Validation of a Questionnaire Assessing the Perceived Control in Health Care among Older Adults with Care Needs in the Netherlands.

Quality of Life Research, *25*(4), 859-870. https://doi.org/10.1007/s11136-015-1124-2

Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, *59*(2), 323-342. https://doi.org/10.1111/1540-4560.00067

Davis, F. D. (1993). User Acceptance of Information Technology: System Characteristics, User Perceptions and Behavioral Impacts. *International journal of man-machine studies*, *38*(3), 475-487. https://doi.org/10.1006/imms.1993.1022

Ebadi, S., & Raygan, A. (2023). Investigating the Facilitating Conditions, Perceived Ease of Use and Usefulness of Mobile-Assisted Language Learning. *Smart Learning Environments*, *10*(1), 30. https://doi.org/10.1186/s40561-023-00250-0

El Azhari, J., & Bennett, D. (2015). Omni-Channel Customer Experience: An Investigation into the Use of Digital Technology in Physical Stores and Its Impact on the Consumer's Decision-Making Process. https://www.academia.edu/download/46002751/El_Azhari_Bennett_FINAL4.pdf

Evans, R., Hajli, N., & Nisar, T. M. (2023). Privacy-Enhancing Factors and Consumer Concerns: The Moderating Effects of the General Data Protection Regulation. *British Journal of Management*, *34*(4), 2075-2092. https://doi.org/10.1111/1467-8551.12685

Gallery, C. (2024). Marketing to the Hyper-Connected Consumer. In *Fashion Business and Digital Transformation* (pp. 143-177). Routledge. https://doi.org/10.4324/9781003364559

Hong, & Thong. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275-298. https://doi.org/10.25300/MISQ/2013/37.1.12

Idrees, S., Vignali, G., & Gill, S. (2023). Interactive Marketing with Virtual Commerce Tools: Purchasing Right Size and Fitted Garment in Fashion Metaverse. In *The Palgrave Handbook of Interactive Marketing* (pp. 329-351): Springer International Publishing. http://dx.doi.org/10.1007/978-3-031-14961-0_15

Jai, T.-M., & King, N. J. (2016). Privacy Versus Reward: Do Loyalty Programs Increase Consumers' Willingness to Share Personal Information with Third-Party Advertisers and Data Brokers? *Journal of Retailing and Consumer Services*, *28*, 296-303. https://doi.org/10.1016/j.jretconser.2015.01.005

Kazmi, Bano, Malik, & Bibi. (2025). The Role of Ai-Driven Personalization in Enhancing Customer Experience and Purchase Intentions: Exploring the Impact of Consumer Data Privacy Concerns. *Al-Qanṭara*. https://doi.org/10.5281/zenodo.15314419

Kim, Im, & Kim. (2023). From Intention to Action: The Factors Affecting Health Data Sharing Intention and Action. *International Journal of Medical Informatics*, *175*, 105071. https://doi.org/10.1016/j.ijmedinf.2023.105071

Knof, Stock, H., & Schurer. (2024). How in-Store Sensor Technologies Can Help Retailers to Understand Their Customers: Overview on Two Decades of Research. *The International Review of Retail, Distribution and Consumer Research*, *34*(3), 381-398. https://doi.org/10.1080/09593969.2023.2273256

Kulisz, Lipski, & Bojanowska. (2018). Purchase Decision Support with Internet of Things-Based Systems. International Conference on Computational Methods in Experimental Economics, https://doi.org/10.1007/978-3-030-30251-1_13

Kulkarni. (2026). Data Privacy and Regulatory Concerns. In *Ai, Machine Learning, and Image Processing in Market Research and Branding* (pp. 247). https://doi.org/10.4018/979-8-3373-4506-2.ch009

Leppäniemi, Karjaluoto, & Saarijärvi. (2017). Customer Perceived Value, Satisfaction, and Loyalty: The Role of Willingness to Share Information. *The International Review of Retail, Distribution and Consumer Research*, *27*(2), 164-188. https://doi.org/10.1080/09593969.2016.1251482

Liang, Lai, & Ku. (2006). Personalized Content Recommendation and User Satisfaction: Theoretical Synthesis and Empirical Findings. *Journal of Management Information Systems*, *23*(3), 45-70. https://doi.org/10.2753/MIS0742-1222230303

Liciotti, Frontoni, Mancini, & Zingaretti. (2016). Pervasive System for Consumer Behaviour Analysis in Retail Environments. International Workshop on Video Analytics for Audience Measurement in Retail and Digital Signage, https://doi.org/10.1007/978-3-319-56687-0_2

Mantelero. (2014). The Future of Consumer Data Protection in the Eu: Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics. *Computer Law & Security Review*, *30*(6), 643-660. https://doi.org/10.1016/j.clsr.2014.09.004

Martin, Kim, Palmatier, Steinhoff, Stewart, Walker, & Weaven. (2020). Data Privacy in Retail. *Journal of Retailing*, *96*(4), 474-489. https://doi.org/10.1016/j.jretai.2020.08.003

Norberg, Horne, & Horne. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Olateju, Okon, Olaniyi, Samuel, O., & Asonze. (2024). Exploring the Concept of Explainable Ai and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. In. https://doi.org/10.9734/jerr/2024/v26i71206

Paramesha, M., Rane, N., & Rane, J. (2024). Big Data Analytics, Artificial Intelligence, Machine Learning, Internet of Things, and Blockchain for Enhanced Business Intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4855856

Park, G. (2019). The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's Gdpr and the California Consumer Privacy Act. *UC Irvine Law Review*, *10*, 1455. https://scholarship.law.uci.edu/ucilr/vol10/iss4/11

Rahman, A., Kundu, D., Debnath, T., Rahman, M., & Islam, M. J. (2024). Blockchain-Based Ai Methods for Managing Industrial Iot: Recent Developments, Integration Challenges and Opportunities. *arXiv preprint arXiv:2405.12550*. https://doi.org/10.48550/arXiv.2405.12550

Rahman, W. (2025). Ethical Ai Personalization in Digital Retail: The Roles of Transparency, Privacy, and Consumer Trust. *Strategic Business Research*, 100020. https://doi.org/10.1016/j.sbr.2025.100020

Soni, V. (2024). Ai and the Personalization-Privacy Paradox: Balancing Customized Marketing with Consumer Data Protection. *International Journal of Computer Trends and Technology*, *72*(9), 24-31. https://doi.org/10.14445/22312803/IJCTT-V72I9P105

Su, Nguyen, Nguyen, Luu, & Nguyen, P. (2022). Modeling Consumers' Trust in Mobile Food Delivery Apps: Perspectives of Tam, Service Quality and Personalization-Privacy Theory. *Journal of Hospitality Marketing & Management*, *31*(5), 535-569. https://doi.org/10.1080/19368623.2022.2020199

Wu, Huang, Wang, & He. (2025). The Effect of Perceived Benefits on Neuroimaging Researchers' Data Sharing Intention: An Empirical Investigation. *Aslib Journal of Information Management*. https://doi.org/10.1108/AJIM-09-2024-0750

Xia, & Yang. (2019). Rmsea, Cfi, and Tli in Structural Equation Modeling with Ordered Categorical Data: The Story They Tell Depends on the Estimation Methods. *Behavior Research Methods*, *51*(1), 409-428. https://doi.org/10.3758/s13428-018-1055-2

Xu, & Chen. (2025). Personalized Recommendations and Consumer Trust: The Role of Perceived Control and Locus of Control. *Acta Psychologica*, *261*, 105936. https://doi.org/10.1016/j.actpsy.2025.105936

Xu, Idaya Aspura Mohd, K., & Kassim. (2025). Is the Intelligent Development of Libraries Accelerating? A Decade of Comprehensive Scientometric Assessment and Swot Analysis. *Journal of Librarianship and Information Science*, 09610006251384336. https://doi.org/10.1177/09610006251384336

Zhang, Agarwal, & Lucas, Jr. (2011). The Value of It-Enabled Retailer Learning: Personalized Product Recommendations and Customer Store Loyalty in Electronic Markets. *MIS Quarterly*, *35*(4), 859-A857. https://doi.org/10.2307/41409964

Zhang, S., Jiang, Y., Ma, R., Yang, Y., Xu, M., Huang, Z., Yi, X., & Li, H. (2026, 2026/04/13). *Privweb: Unobtrusive and Content-Aware Privacy Protection for Web Agents* Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems, http://dx.doi.org/10.1145/3772318.3790919