ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 13 (2026) No. 4, pp. 105-124
DOI:10.33168/JLISS.2026.0407

Beyond Trust: Privacy Governance, Perceived Control, and Moral Appraisals in EU E-Commerce

Laith T. Khrais

Faculty of Business; Middle East University, Jordan.
lkhrais@meu.edu.jo

Abstract. In this study, the role of e-commerce privacy and security cues in terms of providing indications of service governance, influencing behavioral intentions through trust, perceived control, fairness–dignity, and perceived risk, is investigated. A total of 723 consumers were surveyed in five GDPR-regulated countries in Europe: Austria, Czech Republic, Hungary, Slovakia, and Slovenia.

The results of the study showed that privacy and security cues are positively linked to purchase intention and loyalty, as well as negatively linked to avoidance. These relationships are largely mediated by three internal evaluation mechanisms: online trust, perceived control, and fairness-dignity. Importantly, the study showed that fairness-dignity is as powerful as the utilitarian mechanisms, suggesting that consumers view privacy governance as a moral as well as a technical problem.

Perceived risk remains a powerful countervailing factor, suggesting a lingering level of consumer suspicion even with harmonized regulation. Further, the study showed that there are cross-national differences that highlight the maturity of institutions as well as the sensitivity to uncertainty as influencing the relationships between privacy-security cues, trust, and avoidance.

Keywords. ecommerce, privacy, security, trust, control, fairness, dignity, risk, governance, GDPR

1. Introduction

The increasing popularity of e-commerce has led to a shift in the consumer experience from sensory, in-person "atmospheric" effects to technology-mediated environments. In such environments, decisions are based on digital signals such as HTTPS padlocks, privacy information, cookie notifications, and recommendation systems (Klepek, 2025; Reuter et al., 2022). Unlike in physical environments, in which such signals are processed quickly and outside of conscious awareness, in technology-mediated environments, people must interpret abstract signals to make inferences about the trustworthiness, respectfulness, and safety of the platform (Liang et al., 2024; Robichaud et al., 2024). Repeated data breaches and lack of transparency in profiling practices increase the salience of both rational evaluation and moral-emotional responses such as exploitation, injustice, and outrage (Amanulla & Niyaz, 2024).

The Stimulus-Organism-Response (S-O-R) model of influence (Mehrabian & Russell, 1974) remains a prominent theory of environmental influence on internal states and behavior. However, the linear nature of the model is being questioned in the context of digital commerce (Ahmad et al., 2023). Critics of the model argue that it fails to capture the impact of cultural identity, social norms, and moral judgment in shaping the meaning of environmental signals for the consumer (Arachchi et al., 2025). At the same time, technology adoption models such as TAM and UTAUT have been criticized for their failure to account for the role of privacy and security in shaping the meaning of technology for the user (Taheri et al., 2024; Uddin et al., 2025). It tests this extension in five countries of the European Union. In these countries, the GDPR provides a common foundation for data protection, while cultural orientations vary. The theoretical contribution of this research is that the effects of privacy/security cues are not merely functional or risk-based; rather, they are also informed by considerations of fairness–dignity (Al-Muntasir, 2022).

In the service-informatics tradition, the management of privacy, security, and consent is an aspect of service operations that regulates the flow of information between platforms, payment processors, logistics companies, and data processors. To consumers, these are indicators of the governance of the service relationship as well as the ability of the service provider to prevent, detect, and respond to ‘last-mile’ digital service failures. Theoretically, trust is an aspect of the service provider’s competence and integrity; control is an aspect of the ability of the consumer to manage the disclosure of their personal data; fairness–dignity is an aspect of the respectfulness of the service relationship; while risk is an aspect of the potential for harm resulting from exploitation, misuse, or breach. Distinguishing between these concepts ensures that there is no overlap in their effects on loyalty, avoidance, and purchase intention.

2. Literature Review

Building on prior privacy and security research, this review positions e-commerce privacy/security not only as a consumer-attitude issue but also as a service governance problem: platforms must coordinate data handling across a network of actors, and customers evaluate the reliability of that coordination using visible cues. Prior work similarly treats design and security features as informatics variables that shape trust and digital service performance . In this study, we go beyond incremental S-O-R extensions by separating trust from perceived control and fairness–dignity, thereby clarifying the distinct technical, autonomy-based, and moral pathways through which privacy/security cues relate to loyalty, avoidance, and purchase intention.

2.1. S–O–R in e-commerce privacy and security

The Stimulus–Organism–Response (S–O–R) model of consumer behavior is a process in which the stimuli in the consumer's environment affect the consumer's internal psychological state, which in turn influences the consumer's behavior. In the context of e-commerce, the S–O–R model has been used extensively to link website cues, including service encounters, to consumer behavior, such as purchase intentions and loyalty (Abumalloh et al., 2025; Zhu et al., 2020). In the context of the current study, the

cues of website privacy and security are of critical importance, as the consumer cannot directly observe the process of data collection, storage, and sharing. Hence, the cues of website privacy and security act as high-diagnostic stimuli, which could trigger a response of trust, a sense of control, or a sense of risk, which in turn could affect the consumer's behavior of purchase or avoidance. In the context of the current study, the S–O–R model of consumer behavior could be represented as follows: Stimuli – Website cues of privacy and security Organism – Consumer's internal psychological state Response – Consumer's behavior of purchase or avoidance

However, it has also been argued that the S–O–R model of consumer behavior could be a linear, one-way model, which could be a limitation in the context of the current study. In the context of the current study, it has been argued that the consumer's behavior of purchase or avoidance could be a complex process, which could be embedded in the consumer's identity, social, and moral constructs. Hence, the S–O–R model of consumer behavior could be a useful framework in the context of the current study, as the organism component of the model could be broadened to include the consumer's moral-emotional response.

2.2. Justifying S–O–R over TAM and UTAUT

TAM and UTAUT models of technology adoption are based on utilitarian beliefs of technology use, including perceived usefulness and ease of use or performance and effort expectancy, respectively (Taheri et al., 2024; Yaqub et al., 2024). However, in the case of privacy-sensitive e-commerce, these beliefs might not be effective because the customer can still choose to leave the transaction even if it is easy to use if they perceive privacy invasion. S-O-R is more applicable to the privacy-security model because it considers privacy/security cues to be the primary stimuli and the psychological effects of these cues to be the organism states that lead to the response behavior (Morshed, 2024c).

This choice is further supported by the fact that the psychological safety of the customer is likely to have the same impact as the usability of the system in data-intensive exchanges (Uddin et al., 2025). Moreover, the privacy/security concern is likely to have an affective component because it can lead to dignity issues and moral outrage, especially in the case of personalization and invasion of privacy (Kalaiarasan et al., 2024). Methodologically speaking, the S-O-R model is also more applicable to the privacy-security model because it allows for more complex causal chains, which is consistent with the traditional mediation modeling tradition in consumer research (Gamage & Ashill, 2023; Müller & Grossniklaus, 2010).

2.3. Digitalization of stimuli and complex decision pathways

Physical environments, such as brick-and-mortar establishments, provide the consumer with sensory atmospherics and interpersonal reassurance. Virtual environments, on the other hand, provide the consumer with abstract stimuli such as the HTTPS lock icon, cookie consent messages, privacy information, and personalized recommendations through opaque and black-box technologies (Reuter et al., 2022). Consumers must have some degree of digital literacy and pre-existing familiarity with cyber risks to interpret the meaning of such stimuli, as the ability of people to distinguish between actual and symbolic security reassurance can be limited (Liang et al., 2024). Therefore, different stimuli can trigger different internal states depending on individual differences in prior experience, knowledge, and confidence in one’s ability to protect oneself (Klepek, 2025).

Furthermore, digital environments are more likely to trigger ambivalence, as they can provide consumers with feelings of pleasure through recommendations that are relevant and convenient, as well as feelings of discomfort due to being intrusively monitored, profiled, and manipulated (Kumar et al., 2025). The overall context of the environment plays an important role as well, as cultural orientations, such as a strong preference for uncertainty avoidance, can increase sensitivity to risks, leading to expectations of transparency and explicit compliance cues (Forkuor et al., 2024). However, ethical

orientations, such as sensitivity to data use, can increase sensitivity to personalization and data monetization, leading to increased avoidance tendencies when they are perceived as exploitative and disrespectful (Singh et al., 2024).

2.4. Toward a more nuanced and ethically attuned S–O–R

More recent studies extend the S–O–R model by adding further richness to the organism component through the application of other theories that attempt to account for interpretive processes. In this tradition, the consumer makes sense of privacy and security-related information through their expectations and moral evaluations of the brand, as determined by their culture (Yang, 2012). Similarly, the privacy calculus model describes the consumer's engagement as balancing the benefits and risks of engaging with the platform (Oreqat, 2021). This risk calculation is subject to information and cognitive limitations. Furthermore, it does not account for other important factors that arise in the context of data-driven personalization. When the consumer suspects the platform of engaging in covert profiling, their moral outrage about the platform's behavior will dominate the risk-minimization calculation and override the more traditional benefit-risk calculation (Morshed, 2024b).

The psychological contract theory of consumer behavior also supports the concept of perceived violation as the primary motivator of consumer behavior. This theory suggests that the consumer-platform relationship is based on an implicit contract of mutual understanding and respect, and that violations of these expectations, such as the platform engaging in covert and exploitative practices, lead to consumer outrage and perceived exploitation. This perceived violation, and not the actual risk of exploitation, drives the consumer behavior. As Ballas et al. (2024) note, perceived violation is the primary motivator of consumer behavior.

2.5. Privacy/security stimuli, organismic mechanisms, and mediation evidence

The most commonly cited stimuli are perceived data security, privacy transparency, and perceived regulatory compliance. Perceived data security, which is the belief that the site protects the data, is usually a positive factor that bolsters trust and reduces abandonment rates (Chawla & Kumar, 2022; Çiftçi & Çizel, 2020), though the cumulative effect of repeated mega-breaches is to create a "trust deficit" that undermines the effectiveness of security cues (Amanulla & Niyaz, 2024). Compliance cues, which are often related to GDPR or similar regulations, may also have a positive effect if perceived as credible institutional assurances (Boyko et al., 2024), though perceived "compliance theater" that is revealed to be false may also have a detrimental effect on trust (McVey et al., 2024). Transparency is also a double-edged sword that bolsters loyalty if perceived as a demonstration of respect for the customer but undermines loyalty if perceived as a demonstration of disrespect for the customer (El-Annan & Hassoun, 2025; Lv et al., 2024).

The most commonly cited organismic mediator is trust, which is a key predictor of loyalty and repeat purchase behavior (Wen et al., 2024; Tyagi, 2024), though fairness-dignity perceptions may also have a direct effect on behavior. Perceived control is also a key mediator, where the presence of dark patterns reduces perceived control and therefore abandonment rates and purchase willingness (Sin et al., 2025; Pinto & Prazeres, 2025), and perceived risk is a key mediator that reduces purchase and disclosure behaviors and supports avoidance behaviors (Bhukya & Singh, 2015; Ahn, 2025). In addition to the commonly cited organismic mediators, fairness-dignity perceptions also have a direct effect on behavior (Taqa, 2025). Profiling and the monetization of customer data are commonly perceived as a demonstration of disrespect for the customer, which undermines loyalty and purchase behaviors (Malgieri & Custers, 2018; Vänskä et al., 2024), and fairness is also a mediator that predicts behavior even when security is perceived to be strong (Ayeboafo et al., 2025).

The effects of the most commonly cited stimuli are typically mediated by organismic responses. Security cues are mediated by trust and perceived risk, which reduces abandonment rates and purchase

behaviors (Shahzad et al., 2024), and compliance cues are mediated by perceived control and institutional assurances (Zhang et al., 2024). Research on re-engagement after incidents similarly indicates that trust restoration channels the effect of post-incident transparency on future behavior (Nusair et al., 2024). Together, this evidence motivates an S–O–R model in which privacy/security cues shape consumer behavior primarily via multiple organismic mechanisms, rather than through a single direct path.

Hypotheses

H1a: Perceived data security, privacy transparency, and perceived regulatory compliance each positively influence consumer trust.

H1b: Perceived data security, privacy transparency, and perceived regulatory compliance each positively influence perceived control over personal data.

H1c: Perceived data security, privacy transparency, and perceived regulatory compliance each negatively influence perceived risk.

H2a: Consumer trust, perceived control, and perceived fairness/dignity each (i) positively influence approach behaviors (purchase intention and loyalty) and (ii) negatively influence avoidance behaviors.
H2b: Perceived risk (i) negatively influences approach behaviors (purchase intention and loyalty) and (ii) positively influences avoidance behaviors.

H3: Trust, perceived control, perceived fairness/dignity, and perceived risk mediate the impact of privacy and security cues on consumer behavior.

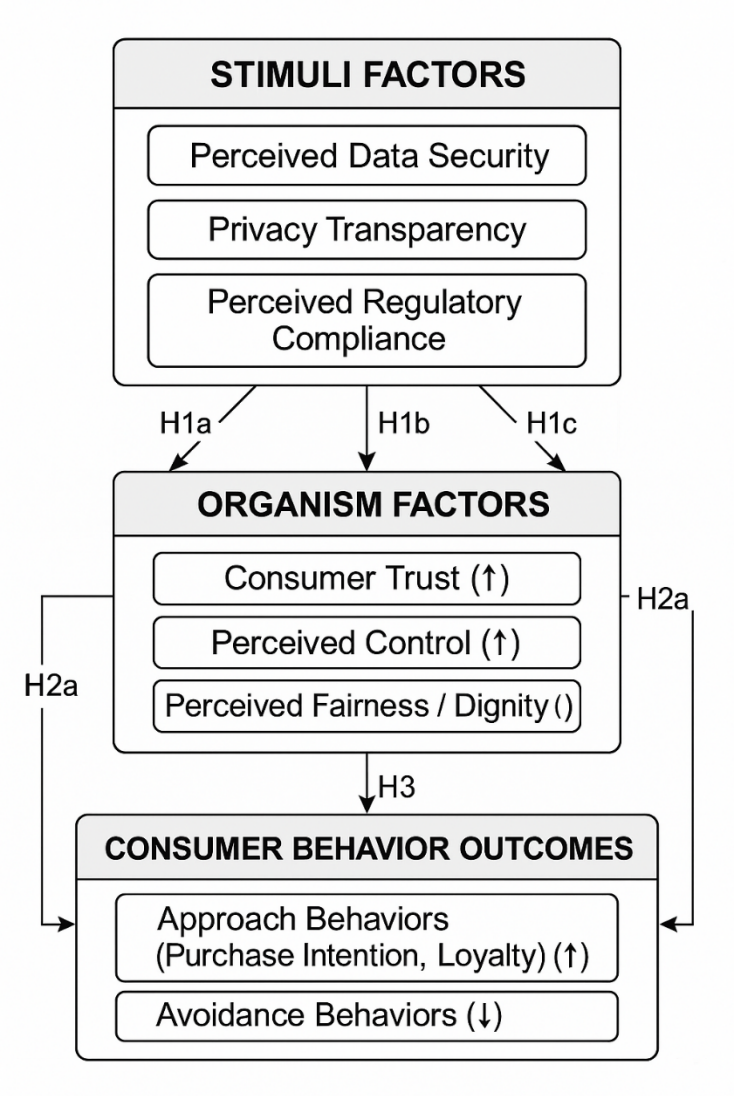

Fig.1: Hypotheses Development

3. Methodology

3.1 Research design and conceptual context

This study used a quantitative, cross-sectional survey to assess how privacy and security cues in e-commerce influence consumer behavioral intentions through internal evaluations. The model extends Stimulus–Organism–Response (S-O-R): stimuli (security, transparency, compliance) affect organismic states (trust, control, risk, fairness/dignity) that shape responses (purchase intention, loyalty, avoidance). Covariance-based SEM (CB-SEM) in AMOS was applied to evaluate overall fit (χ^2/df, RMSEA, CFI, TLI, SRMR) and to estimate direct and indirect paths within one system.

Pre-analysis screening followed current CB-SEM recommendations: Q–Q plots suggested approximate normality; multicollinearity was acceptable (VIF < 5); and residual/leverage checks identified no influential outliers (Gaskin et al., 2025).

3.2 Population and country selection

The population comprised adult online shoppers in Austria, Hungary, Slovakia, the Czech Republic, and Slovenia. A shared GDPR regulatory environment standardizes key privacy cues, while cultural diversity supports comparison of how similar cues are interpreted (Morshed, 2024a)

. Eligibility required at least one online purchase in the past six months and engagement with privacy/security features to ensure experience-based responses (Renuka et al., 2025).

Table 1. Respondents by country (N = 723)

Country	**Respondents**	**%**
Austria	165	23
Hungary	145	20
Czech Republic	140	19
Slovakia	138	19
Slovenia	135	19
Total	**723**	**100**

3.3 Sampling design and data collection

Data were collected March–June 2025 using an online questionnaire distributed via social media and e-commerce/privacy forums, complemented by snowball sharing. From 1,250 invitations, 802 responses were received; after excluding 79 incomplete or ineligible cases, 723 valid responses remained for analysis (Table 2) (Ghimire et al., 2023). To mitigate self-selection and coverage bias typical of online surveys, the invitation was disseminated through multiple channel types (general social media, shopping communities, and privacy-focused forums) and included eligibility screening (recent online purchase experience and informed consent). Nevertheless, the sample remains nonprobabilistic and the findings should be interpreted as associations rather than population estimates (Vliegenthart et al., 2024).

Table 2. Sampling and response summary

Stage	**Number**	**% of initial**
Invitations sent	1,250	100.0
Responses received	802	64.2
Excluded (incomplete/ineligible)	79	6.3
Final valid responses	**723**	**57.8**

3.4 Sample size determination

Sample size adequacy was assessed using SEM planning logic ($\alpha = 0.05$, power = 0.80, medium $f^2 = 0.15$) and parameter-based heuristics for a 10-construct, 27-indicator model, indicating a minimum of ~350–400 cases (Table 3) (Wang et al., 2024).

Table 3. Sample size justification

Method/Rule	Required N	Obtained N
Westland (2010) SEM formula	~400	723
Bentler & Bollen (5:1)	~350	723
General SEM guidance	≥200	723

3.5 Survey instrument and measurement items

All constructs were measured reflectively with multi-item scales developed from existing research in privacy, security, and e-commerce trust with a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The items included measures of technical assurance (e.g., encryption, policy clarity, compliance badges), as well as moral judgment (fairness/dignity and respect), with minimal reverse items to mitigate acquiescence bias (Morshed, 2025b). Face and content validity were ensured through expert review by three academics and two EU data compliance practitioners to refine the items to ensure clarity and equivalence across countries (Morshed et al., 2024). The reliability and convergent validity of the scales were assessed through alpha, CR, and AVE (Table 4).

Table 4. Constructs and reliability indices

Construct	α	CR	AVE
Perceived Data Security	0.88	0.92	0.75
Privacy Transparency	0.89	0.93	0.77
Regulatory Compliance	0.87	0.91	0.73
Consumer Trust	0.91	0.94	0.80
Perceived Control	0.90	0.93	0.78
Perceived Risk	0.88	0.92	0.76
Fairness/Dignity	0.89	0.93	0.77
Purchase Intention	0.92	0.95	0.82
Loyalty	0.90	0.93	0.79
Avoidance Intention	0.87	0.91	0.74

3.6 Exploratory factor analysis (EFA/PCA)

EFA assessed whether the item set supported the intended latent structure. Sampling adequacy was high (KMO = 0.91) and Bartlett's test confirmed factorability ($\chi^2 = 4{,}856.32$, df = 351, $p < 0.001$) (Furno et al., 2024). PCA with varimax rotation retained 10 factors (eigenvalue > 1), explaining 78.6% of variance; loadings ranged 0.65–0.88 without problematic cross-loadings (Table 5).

Table 5. EFA summary

Metric	Result
KMO	0.91
Bartlett's test	$\chi^2 = 4{,}856.32$, $p < .001$
Factors retained	10
Variance explained	78.6%
Loadings range	0.65–0.88

3.7 Confirmatory factor analysis (CFA)

CFA in AMOS confirmed the measurement model with significant standardized loadings (typically ≥ 0.70) and satisfactory discriminant validity based on Fornell–Larcker and HTMT criteria (all HTMT < 0.85), supporting construct separation (Lesia et al., 2024). Key fit indices and reliability/validity summaries are reported in the Results section (Tables 7–8).

3.8 Structural model estimation

The structural model was estimated in AMOS using maximum likelihood after measurement validation. Direct effects were tested using standardized coefficients (β) and significance tests, and mediation was assessed with bootstrapping (5,000 resamples) to obtain confidence intervals for indirect effects (Morshed, 2025d).

3.9 Handling nonresponse and bias

Nonresponse was documented across incomplete submissions, ineligible cases, and refusals/dropouts (Table 6) (Heirene et al., 2025).

Table 6. Nonresponse analysis

Category	Number	% of initial
Incomplete submissions	65	5.2
Ineligible cases	14	1.1
Refusals/dropouts	369	29.5
Final valid responses	**723**	**57.8**

4. Results

4.1 Measurement model

CFA supported excellent measurement model fit (Table 7): $\chi^2/df < 3.0$, RMSEA = 0.046, CFI = 0.962, TLI = 0.955, SRMR = 0.041. Reliability and validity were strong (Table 8): standardized loadings > 0.70, Cronbach's α and CR > 0.87, AVE > 0.70, and HTMT < 0.85, confirming convergent and discriminant validity.

Table 7. CFA model fit indices

Fit Index	Threshold	Obtained Value	Conclusion
χ^2/df	≤ 3.0	2.18	Acceptable fit
RMSEA	≤ 0.08 (≤ 0.05 = good)	0.046	Good fit
CFI	≥ 0.90 (≥ 0.95 = excellent)	0.962	Excellent fit
TLI	≥ 0.90 (≥ 0.95 = excellent)	0.955	Excellent fit
SRMR	≤ 0.08	0.041	Good fit

Table 8. Reliability and validity statistics

Construct	Factor Loadings (Range)	Cronbach's α	CR	AVE	HTMT Max	Conclusion
Perceived Data Security	0.72–0.86	0.88	0.92	0.75	0.81	Valid
Privacy Transparency	0.74–0.89	0.89	0.93	0.77	0.80	Valid
Regulatory Compliance	0.70–0.85	0.87	0.91	0.73	0.79	Valid
Consumer Trust	0.78–0.91	0.91	0.94	0.80	0.83	Valid
Perceived Control	0.76–0.89	0.90	0.93	0.78	0.81	Valid
Perceived Risk	0.71–0.87	0.88	0.92	0.76	0.84	Valid
Fairness/Dignity	0.74–0.90	0.89	0.93	0.77	0.80	Valid
Purchase Intention	0.82–0.91	0.92	0.95	0.82	0.83	Valid
Loyalty	0.79–0.89	0.90	0.93	0.79	0.82	Valid
Avoidance Intention	0.72–0.86	0.87	0.91	0.74	0.83	Valid

4.2 Structural model

Bootstrapped SEM (5,000 resamples) showed that privacy/security cues were positively associated with Trust, Control, and Fairness–Dignity and negatively associated with Risk. Trust, Control, and Fairness–Dignity were then positively associated with Purchase Intention and Loyalty and negatively associated with Avoidance, whereas Risk showed the opposite pattern (Table 9). These directions are consistent with prior evidence that privacy/security signals shape trust formation while perceived risk suppresses online purchase intentions (Bhukya & Singh, 2015; Liang et al., 2024).

Table 9. Direct effects (AMOS, bootstrapped)

Path	B	SE	t-value	p-value
Privacy/Security → Trust	0.67	0.05	13.42	<.001
Privacy/Security → Control	0.62	0.05	12.05	<.001
Privacy/Security → Fairness–Dignity	0.59	0.05	11.22	<.001
Privacy/Security → Risk	−0.55	0.05	10.73	<.001
Trust → Purchase Intention	0.52	0.05	9.88	<.001
Control → Purchase Intention	0.55	0.05	10.44	<.001
Fairness–Dignity → Purchase Intention	0.56	0.05	10.78	<.001
Risk → Purchase Intention	−0.43	0.05	8.76	<.001
Trust → Loyalty	0.53	0.06	9.65	<.001
Control → Loyalty	0.57	0.05	10.18	<.001
Fairness–Dignity → Loyalty	0.60	0.06	10.85	<.001
Risk → Loyalty	−0.41	0.05	8.34	<.001
Trust → Avoidance	−0.47	0.05	9.21	<.001
Control → Avoidance	−0.50	0.05	9.92	<.001
Fairness–Dignity → Avoidance	−0.49	0.05	9.54	<.001
Risk → Avoidance	0.50	0.05	10.11	<.001

4.3 Mediation analysis

Bootstrapped indirect effects confirmed multiple mediation (Table 10). Privacy/security cues were associated with higher Purchase Intention and Loyalty indirectly via Trust, Control, and Fairness–Dignity ($\beta = 0.31–0.38$, $p < .001$) and with lower Avoidance via the same mediators ($\beta = -0.27$ to -0.29, $p < .001$). Risk operated as a countervailing mediator, being associated with lower Purchase and Loyalty ($\beta \approx -0.26$ to -0.27, $p < .001$) and higher Avoidance ($\beta = 0.29$, $p < .001$), consistent with moral appraisal and risk pathways in consumer decision-making (Bhattacharya et al., 2024; Rahman, 2025).

Table 10. Indirect (mediated) effects (AMOS, bootstrapped)

Indirect Path	β	p-value	Result
Privacy/Security → Trust → Purchase	0.31	<.001	Supported
Privacy/Security → Control → Purchase	0.34	<.001	Supported
Privacy/Security → Fairness → Purchase	0.36	<.001	Supported
Privacy/Security → Risk → Purchase	−0.27	<.001	Supported
Privacy/Security → Trust → Loyalty	0.32	<.001	Supported

Privacy/Security → Control → Loyalty	0.35	<.001	Supported
Privacy/Security → Fairness → Loyalty	0.38	<.001	Supported
Privacy/Security → Risk → Loyalty	−0.26	<.001	Supported
Privacy/Security → Trust → Avoidance	−0.27	<.001	Supported
Privacy/Security → Control → Avoidance	−0.29	<.001	Supported
Privacy/Security → Fairness → Avoidance	−0.28	<.001	Supported
Privacy/Security → Risk → Avoidance	0.29	<.001	Supported

4.4 Explanatory power

The model was found to possess considerable explanatory potential, as indicated in Table 11, for Purchase Intention ($R^2 = 0.66$), Loyalty ($R^2 = 0.64$), and Avoidance Intention ($R^2 = 0.55$). This suggests that the ethically extended S-O-R model can account for a considerable proportion of important consumer outcomes, with trust, perceived control, fairness–dignity, and risk playing key roles in the process (Bhattacharya et al., 2024

Table 11. Explained variance (R^2) of endogenous constructs

Construct	**R^2**	**Interpretation**
Purchase Intention	0.66	Substantial
Loyalty	0.64	Substantial
Avoidance Intention	0.55	Moderate–substantial

4.5 Robustness, bias checks, and invariance

For robustness analyses of common method bias (CMB) and measurement invariance, see Table 12. The single-factor test according to Harman showed that the largest share of the variance was explained by the first factor (31.4%), which is less than 50%. The addition of a latent method factor was not significant for the model fit ($\Delta CFI = 0.004$). Such tests are suggestive but cannot exclude CMB for self-reported data in cross-sectional designs. We focus here on procedural solutions to CMB. Multi-group CFA showed support for configural and metric invariance across the five countries ($\Delta CFI = 0.005$). We partially supported scalar invariance after freeing three intercepts, which is often considered sufficient for cross-group comparisons in practical SEM research (Morshed, 2025c).

Table 12. Robustness and bias tests

Test / Stage	**Fit Indices / Results**	**Thresholds**	**Conclusion**
Harman's single-factor test	First factor = 31.4% variance explained	< 50%	CMB unlikely
CFA with method factor	$\Delta\chi^2 = 14.2$ ($\Delta df = 10$, $p > .05$); $\Delta CFI = 0.004$	$\Delta CFI \leq 0.01$	CMB minimal

Configural invariance	χ^2/df = 2.21; RMSEA = 0.048; CFI = 0.956; TLI = 0.951	χ^2/df ≤ 3; RMSEA ≤ 0.08; CFI ≥ 0.90	Supported
Metric invariance	$\Delta\chi^2$ = 21.7 (Δdf = 15, p > .05); ΔCFI = 0.005	ΔCFI ≤ 0.01	Supported
Scalar invariance	$\Delta\chi^2$ = 52.9 (Δdf = 25, p < .01); ΔCFI = 0.015	ΔCFI ≤ 0.01	Partially supported (after freeing 3 intercepts)

4.6 Multi-group analysis (MGA)

Overall structural invariance was supported: constraining all structural paths across countries did not significantly reduce fit (χ^2/df = 2.25, RMSEA = 0.049, CFI = 0.954, TLI = 0.950; $\Delta\chi^2$ = 37.8, Δdf = 30, p > .10; ΔCFI = 0.006). The results of the path-level comparisons were largely consistent, apart from two differences: the path of Privacy/Security → Trust was stronger in Austria than in Slovenia, and the path of Risk → Avoidance was stronger in Hungary than in the Czech Republic (Table 13) (Morshed, 2025a). These findings suggest overall stability of the ethically extended S-O-R model in Central Europe, along with minimal cultural differences in trust formation and risk-driven avoidance (Al-Daoud & Abu-AlSondos, 2025).

Table 13. Multi-group analysis of structural paths

Path	**Austria β**	**Hungary β**	**Czech β**	**Slovakia β**	**Slovenia β**	**Δβ Range**	**Significant Difference**
Privacy/Security → Trust	0.70	0.68	0.66	0.65	0.62	0.08	Yes (Austria > Slovenia)
Privacy/Security → Control	0.63	0.61	0.60	0.62	0.59	0.04	No
Privacy/Security → Fairness	0.60	0.58	0.59	0.61	0.57	0.04	No
Privacy/Security → Risk	−0.54	−0.56	−0.53	−0.55	−0.52	0.04	No
Risk → Avoidance	0.52	0.56	0.48	0.51	0.50	0.08	Yes (Hungary > Czech)
Trust → Purchase Intention	0.54	0.53	0.52	0.55	0.53	0.03	No
Control → Loyalty	0.58	0.57	0.56	0.59	0.57	0.03	No

5. Discussion

This study contributes to the digital trust literature by conceptualizing privacy and security cues in terms of service governance in e-commerce service systems. Consumers appear to assess the provider's data practices in terms of autonomy, i.e., perceived control, and moral issues, i.e., fairness-dignity, in addition to the more established constructs of trust and risk. Such differentiation helps to overcome the problem of construct duplication and provides insight into the underlying reasons for the heterogeneous behavioral outcomes of cues emphasizing compliance in different markets. The most surprising result was the finding of residual skepticism, suggesting that, despite the presence of privacy and security cues, perceived risk was a substantial inhibitor in its own right. This may indicate that consumers may anticipate potential infringements despite the formal policies in place, supporting the idea that privacy governance is assessed on the basis of informational asymmetry and the consumer's digital service experience, rather than formal policies and regulations. The mediation results support the process model of consumer decision-making, suggesting that the effect of privacy and security cues on loyalty, avoidance, and purchase intention is mediated by internal processes of evaluation. This means that, in practice, improving 'surface-level' cues, such as privacy seals and statements, will not be effective unless complemented by 'subsurface-level' cues, i.e., control and interaction design that conveys respect and non-manipulation.

The cross-national analyses showed that, despite the harmonized conditions in the GDPR, there are not corresponding homogeneous consumer behavior responses. Although the structure of the model was maintained, the strength of the relationships varied between countries, probably because of the varying levels of institutional trust, the presence of law enforcement, the development of digital services, and the cultural attitude to uncertainty and surveillance. These analyses should be interpreted with caution, since the sampling was based on nonprobability techniques. However, they support the idea that 'EU context' should not be treated as a homogeneous construct in the future.

5.1 Theoretical Implications

The present study extends theory beyond the incremental S-O-R extension by identifying the actual mechanisms that operate in the "Organism" box. By identifying four distinct mechanisms and their various meanings and consequences, the present study moves beyond the general concept of "attitude" to investigate the particular consequences of trust in the service's competence and integrity, perceived control in the service's data use and disclosure, fairness-dignity in the service's treatment of the consumer, and perceived risk in the likelihood and potential harm of the service's use. This more detailed understanding of the mechanisms may help to explain the apparent paradox in the consequences of privacy/security cues, wherein the cues have a positive effect in generating trust and a negative effect in generating moral responses to constrained control and dignity. Ultimately, "secure" does not necessarily mean "legitimate," and this model provides a better explanation for why consumers may comply in the short term but ultimately defect or resist when the overall relationship is unfair.

A second theoretical advancement comes from reframing cues for privacy and security as service-governance cues rather than interface cues. By understanding what cues like policy clarity, security cues, consent cues, and breach cues mean to consumers, this research reveals that consumers use cues to assess the capability of the service to coordinate the flow of information across a service system that involves multiple actors: the platform itself, the payment system, logistics providers, and vendors. This reframes the S-O-R model to a service-informatics model by recognizing that cues for privacy and security are part of the larger issue of service reliability in the digital age. As such, this research provides a clearer explanation for when cues for privacy and security stimulate consumer loyalty and when they stimulate avoidance.

5.2 Practical Implications

To the manager and the policymaker, the issue of privacy and security is a matter of last-mile service quality and a continuous process of governance, rather than a single event of compliance. What the findings suggest is that, in order to increase trust, it is not sufficient to merely increase trust levels, as users will still perceive a lack of control and dignity violations. What is required is a multi-faceted approach to the issue of user data and its handling, which addresses the following areas:

Make data practices intelligible in the moment of choice. Provide users with a brief and simple explanation of the data collected, the purpose of the data collected, the recipient of the data, and the period of data retention, especially during sign-up, checkout, payment, tracking, and returns.

Make user control usable, not merely "symbolic." Ensure that the mechanisms of user control are easily accessible, easily opt-outable, and easily revisable, without friction asymmetry. This means ensuring that opting out is as simple as opting in and not requiring many steps and clicks.

Operationalize dignity and fairness in design rules. This means ensuring data minimization, avoiding intrusive personalization, and providing users with a clear and simple explanation of targeting and ads, as well as providing opt-out mechanisms. "Respect" as a service standard is not merely a value statement; it is a standard to be met.

Third-party risks should be managed as part of the customer experience. Customers will rate the system on the weakest link in the network. Vendor due diligence, elimination of unnecessary data sharing, accountability of processors, and transparency in terms of the roles of the partner network (payment services, logistics, cloud, analytics) are key areas to focus on.

Strengthen monitoring, incidents, and service recoveries. Service promises (e.g., response to support incidents), breach readiness, transparent communication of incidents, and providing options to recover from service incidents (including handling complaints, rapid support, and providing adequate redress).

From the policymaker's point of view, the above implications suggest that policymakers should move away from broad and lengthy policy documents and instead focus on providing useful consent standards, improving enforcement against dark patterns, and providing clarity on service network accountability (controllers, processors, and third parties).

6. Conclusion

This study examined the relationship between privacy and security cues in e-commerce and behavioral intentions by examining four different internal appraisal processes: trust, perceived control, fairness-dignity perceptions, and perceived risk. The findings supported that privacy/security cues are related to purchase intention and loyalty, and avoidance behaviors, primarily through the internal organismic routes. Of the four routes, fairness-dignity is a significant mediator alongside trust and perceived control.

The study's contribution is not only the addition of a new mediator but also the clarification of the relationships between trust, perceived control, moral appraisal, and risks. The study also reframes the concepts of privacy/security cues in terms of service governance in a digital service network involving multiple service actors. This approach links the perception of privacy/security cues to service operation and governance that impact service reliability and the service experience.

Interpretation should be cautious in nature. The results obtained in the paper are based on intentions rather than actual behaviors, and the sampling method was nonprobability in nature, based on an online sampling frame. Although procedural and statistical controls minimize common method biases, they do not completely eliminate it. Thus, the results should be understood as strong associations and plausible mechanisms that need to be replicated in future studies.

The final obstacle should be privacy, providing true control, no manipulation, and governance/recovery with trust beyond notices and security. The future work should include testing other platforms and regulations, as well as digital literacy and breach history.

References

Abouelela, O., Diab, A., & Saleh, S. (2025). The determinants of the relationship between auditor tenure and audit report lag: Evidence from an emerging market. Cogent Business & Management, 12. https://doi.org/10.1080/23311975.2024.2444553

Abumalloh, R. A., Halabi, O., & Nilashi, M. (2025). The relationship between technology trust and behavioral intention to use Metaverse in baby monitoring systems' design: Stimulus-organism-response (SOR) theory. Entertainment Computing, 52, 100833.

Ahn, J. (2025). Understanding food delivery service customers' switching behavior. Journal of Hospitality and Tourism Technology, 16(1), 124–138.

Ahmad, A. K., Nahar, H. M., & Manajreh, M. M. N. (2023). Effect of social media on shaping the agenda of the communicator in the Jordanian TV channels. Middle East Journal of Communication Studies, 3(2), Article 3. https://doi.org/10.71220/2585-003-002-003

Al-Daoud, K. I., & Abu-AlSondos, I. A. (2025). Robust AI for Financial Fraud Detection in the GCC: A Hybrid Framework for Imbalance, Drift, and Adversarial Threats. Journal of Theoretical and Applied Electronic Commerce Research, 20(2), 121.

Al-Muntasir, M. (2022). The phenomenon of information flow from traditional and new media about the Corona pandemic from the perspective of newly graduated media professionals in Yemen. Middle East Journal of Communication Studies, 2(2), Article 1. https://doi.org/10.71220/2585-002-002-005

Aladwey, L. M. A., & Diab, A. (2025). Business bribery, corruption and fraud: Audit committee and external auditor's attributes in GCC countries. Journal of Financial Regulation and Compliance.

Alvi, T. H., Ilyas, H. M. S., Tariq, S., Qammar, A., & Wang, Y. (2024). Mitigating work alienation in public sector service-delivery projects caused by perceived overqualification: The roles of empowering leadership and the psychological contracts. International Journal of Managing Projects in Business, 17(3), 504–532.

Amanulla, A., & Niyaz, S. (2024). Marriot data breach: A case study analysis. In Information technology security and risk management (pp. 241–245). CRC Press. https://doi.org/10.1201/9781003264415-35

Anomah, S. (2025). Assessing the institutional readiness and capacity for AI adoption in public audit institutions in developing countries: Evidence from Ghana. Telematics and Informatics Reports, 20, 100260.

Anoop, T. S., & Rahman, Z. (2024). From urge to action: The hidden forces behind online impulse buying in electronic commerce—A meta analytic structural equation modelling (MASEM) research. Electronic Commerce Research. https://doi.org/10.1007/s10660-024-09945-z

Arachchi, H. A. D. M., Samarasinghe, G. D., & Wickramasinghe, A. (2025). Seeing is believing: Exploring deepfake video ads and brand loyalty in the experience economy. Journal of Global Marketing, 1–35. https://doi.org/10.1080/08911762.2025.2469293

Ayeboafo, B., Anomah, S., & Amofah, K. (2025). Leveraging blockchain technology adoption in the fight against corruption: An evaluation of Ghana's readiness. Journal of Economic Criminology, 8, 100158.

Ballas, L., Schuster, T., & Pflaum, A. (2024). Unravelling psychological contracts in a digital age of work: A systematic literature review. European Journal of Work and Organizational Psychology, 33(5), 614–631. https://doi.org/10.1080/1359432X.2024.2341821

Bhattacharya, S., Sharma, R. P., & Gupta, A. (2024). Country-of-origin and online retailing ethics: The mediating role of trust and satisfaction on purchase intention. International Journal of Emerging Markets, 19(10), 2778–2801.

Bhukya, R., & Singh, S. (2015). The effect of perceived risk dimensions on purchase intention: An empirical evidence from Indian private labels market. American Journal of Business, 30(4), 218–230.

Biswas, S., Fuentes, T. L., McCord, K. H., Rackley, A. L., & Antonopoulos, C. A. (2024). Decisions and decision-makers: Mapping the sociotechnical cognition behind home energy upgrades in the United States. Energy Research & Social Science, 109, 103411.

Boyko, N., Nes, K., & Schaefer, K. A. (2024). International trade and Ukraine's pursuit of self-determination. The World Economy, 47(4), 1460–1477. https://doi.org/10.1111/twec.13493

Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: The emerging trend. Journal of Business Ethics, 180(2), 581–604. https://doi.org/10.1007/s10551-021-04884-3

Çiftçi, Ş. F., & Çizel, B. (2020). Predictors of e-trust for web-based travel intermediaries: A survey on Istanbul visitors. Journal of Hospitality and Tourism Technology, 11(4), 667–680.

El-Annan, S. H., & Hassoun, R. (2025). Enhancing consumer trust through transparent data practices and ethical data management in business. In Innovation management for a resilient digital economy (pp. 105–148). IGI Global Scientific Publishing. https://www.igi-global.com/chapter/enhancing-consumer-trust-through-transparent-data-practices-and-ethical-data-management-in-business/366575

Elkhatibi, Y., Guelzim, H., & Benabdelouahed, R. (2024). Factors influencing the adoption of AI-powered chatbots in the Moroccan banking sector: An extended UTAUT model. Journal of Logistics, Informatics and Service Science, 11(7), 559–585.

Forkuor, J. B., Konadu-Yiadom, A., Agyemang, E., Deku, C. S., & Odongo, D. A. (2024). Negotiating cultural and legal demands in child protection cases: Experiences and lessons from Ghanaian social workers. Cogent Social Sciences, 10(1), 2323567. https://doi.org/10.1080/23311886.2024.2323567

Furno, A., Zanella, A. F., Stanica, R., & Fiore, M. (2024). Spatial and temporal exploratory factor analysis of urban mobile data traffic. Data Science for Transportation, 6(1), 4.

Gamage, T. C., & Ashill, N. J. (2023). #Sponsored-influencer marketing: Effects of the commercial orientation of influencer-created content on followers' willingness to search for information. Journal of Product & Brand Management, 32(2), 316–329.

Gaskin, J. E., Lowry, P. B., Rosengren, W., & Fife, P. T. (2025). Essential validation criteria for rigorous covariance-based structural equation modelling. Information Systems Journal. (Advance online publication)

Ghimire, B., Dahal, R. K., Rai, B., & Upadhyay, D. (2023). Employee performance factors in the Nepalese commercial banks: Insights from emerging markets. Journal of Logistics, Informatics and Service Science, 10(2), 29–42.

Heirene, R. M., Cobb-Clark, D., Tymula, A., Santos, T., & Gainsbury, S. M. (2025). Non-response bias in gambling surveys. International Gambling Studies, 1–24.

Kalaiarasan, S. M., Vafaei-Zadeh, A., Hanifah, H., & Ramayah, T. (2024). Can we engage players with extended reality in gaming applications? A stimulus-organism-response framework. Entertainment Computing, 50, 100651.

Klepek, M. (2025). How online retailers compete: Duplication of purchase and natural monopoly in e-commerce. The International Review of Retail, Distribution and Consumer Research, 1–18. https://doi.org/10.1080/09593969.2024.2448787

Kumar, R., Singh, T., Mohanty, S. N., Goel, R., Gupta, D., Alharbi, M., & Khanna, R. (2025). Study on online payments and e-commerce with SOR model. International Journal of Retail & Distribution Management, 53(4), 1–17.

Larsson, G., Mažeikienė, A., & Smaliukienė, R. (2025). Psychological prediction of stress-related hair steroid hormone levels in young men: A person-centered approach. Nordic Psychology, 77(1), 26–38. https://doi.org/10.1080/19012276.2023.2247571

Lesia, M. P., Aigbavboa, C. O., & Thwala, W. D. (2024). Factors influencing residential location choice in South Africa: Exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). Journal of Housing and the Built Environment, 39(1), 133–160.

Liang, X., Li, G., Ma, J., & Jiang, G. (2024). How do signaling and reputation function as critical clues to e-commerce platform governance? Evidence from Chinese rice transaction data. Electronic Commerce Research. https://doi.org/10.1007/s10660-024-09816-7

Lins, S., Greulich, M., Löbbers, J., Benlian, A., & Sunyaev, A. (2024). Why so skeptical? Investigating the emergence and consequences of consumer skepticism toward web seals. Information & Management, 61(2), 103920.

Lv, L., Kang, K. Q., & Liu, G. (Gus). (2024). Prick "filter bubbles" by enhancing consumers' novelty-seeking: The role of personalized recommendations of unmentionable products. Psychology & Marketing, 41(10), 2355–2367. https://doi.org/10.1002/mar.22057

Malgieri, G., & Custers, B. (2018). Pricing privacy–The right to know the value of your personal data. Computer Law & Security Review, 34(2), 289–303.

McVey, L., Gurrieri, L., & Tyler, M. (2024). Moral market compliance: How a logic of activism is used to 'fem wash' market violence against women in the user-generated pornography market. Marketing Theory. https://doi.org/10.1177/14705931241279268

Mehrabian, A., & Russell, J. A. (1974). A verbal measure of information rate for studies in environmental psychology. Environment and Behavior, 6(2), 233.

Morshed, A. (2024a). Comparative analysis of accounting standards in the Islamic banking industry: A focus on financial leasing. Journal of Islamic Accounting and Business Research. https://doi.org/10.1108/JIABR-12-2022-0349

Morshed, A. (2024b). Evaluating the effects of IFRS 9 on Jordanian banks' credit and financial metrics. Banks and Bank Systems, 19(4), 70–83. https://doi.org/10.21511/bbs.19(4).2024.06

Morshed, A. (2024c). Evaluating the influence of advanced analytics on client management systems in UAE telecom firms. Innovative Marketing, 20(4), 41–51. https://doi.org/10.21511/im.20(4).2024.04

Morshed, A. (2025a). Cultural norms and ethical challenges in MENA accounting: The role of leadership and organizational climate. International Journal of Ethics and Systems. https://doi.org/10.1108/IJOES-08-2024-0247

Morshed, A. (2025b). Ethical challenges in designing sustainable business models for responsible consumption and production: Case studies from Jordan. Management & Sustainability: An Arab Review. https://doi.org/10.1108/MSAR-09-2024-0131

Morshed, A. (2025c). Navigating tradition and modernity: Digital accounting and financial integration in family-owned enterprises in the Arab Gulf. Sustainable Futures, 100680.

Morshed, A. (2025d). Sustainable energy revolution: Green finance as the key to the Arab Gulf States' future. International Journal of Energy Sector Management. https://doi.org/10.1108/IJESM-10-2024-0007

Morshed, A., Maali, B., Ramadan, A., Ashal, N., Zoubi, M., & Allahham, M. (2024). The impact of supply chain finance on financial sustainability in Jordanian SMEs. Uncertain Supply Chain Management, 12(4), 2767–2776.

Morshed, A., Ramadan, A., Maali, B., Khrais, L. T., & Baker, A. A. R. (2024). Transforming accounting practices: The impact and challenges of business intelligence integration in invoice processing. Journal of Infrastructure, Policy and Development, 8(6), 4241.

Müller, B., & Grossniklaus, U. (2010). Model organisms—A historical perspective. Journal of Proteomics, 73(11), 2054–2063.

Nusair, K., Karatepe, O. M., Okumus, F., Alfarhan, U. F., & Shi, F. (2024). Exploring the pivotal role of community engagement on tourists' behaviors in social media: A cross-national study. International Journal of Information Management, 74, 102701.

Ogles, B. M., Hansen, K. L., & Erekson, D. M. (2024). Competence-based assessment and training for ethical situations in practice: A pilot study. Ethics & Behavior, 34(7), 473–490. https://doi.org/10.1080/10508422.2023.2263896

Oreqat, A. (2021). The degree of satisfaction of Facebook users about its features, usage motives and achieved gratifications: An applied study on students of the Faculty of Mass Communication at the Middle East University to attract attention. Middle East Journal of Communication Studies, 1(1), Article 1. https://doi.org/10.71220/2585-001-001-001

Pinto, G. P., & Prazeres, C. (2025). Data privacy in the Internet of Things: A perspective of personal data store-based approaches. Journal of Cybersecurity and Privacy, 5(2), 25.

Rahman, H. (2025). The ethical dimensions of digital interactions. In Digital citizenship and building a responsible online presence (pp. 123–164). IGI Global Scientific Publishing.

Ramadan, A., & Morshed, A. (2024). Impact of international accounting standards on Hungary's financial transparency. *Investment Management and Financial Innovations*, *21*(4), 11–24. https://doi.org/10.21511/imfi.21(4).2024.02

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data privacy and protection: Legal and ethical challenges. In Emerging threats and countermeasures in cybersecurity (pp. 433–465).

Reuter, C., Iacono, L. L., & Benlian, A. (2022). A quarter century of usable security and privacy research: Transparency, tailorability, and the road ahead. Behaviour & Information Technology, 41(10), 2035–2048. https://doi.org/10.1080/0144929X.2022.2080908

Robichaud, Z., Brand, B. M., & Yu, H. (2024). Bridging the information asymmetry in e-commerce: An intercultural perspective on sustainable clothing. International Journal of Retail & Distribution Management, 52(10/11), 1004–1019.

Shahzad, M. F., Xu, S., An, X., & Javed, I. (2024). Assessing the impact of AI-chatbot service quality on user e-brand loyalty through chatbot user trust, experience and electronic word of mouth. Journal of Retailing and Consumer Services, 79, 103867.

Sin, R., Harris, T., Nilsson, S., & Beck, T. (2025). Dark patterns in online shopping: Do they work and can nudges help mitigate impulse buying? Behavioural Public Policy, 9(1), 61–87.

Singh, V., Vishvakarma, N. K., & Kumar, V. (2024). Tracing the origins of manipulation: Modeling the enablers behind dark patterns usage in e-commerce through TISM and MICMAC analysis. Global Knowledge, Memory and Communication. https://doi.org/10.1108/GKMC-10-2023-0386

Taheri, B., Yousaf, A., Gannon, M., & Mishra, A. (2024). E-commerce website customer engagement: Delineating the role of UTAUT, vividness, and compulsion. Journal of Retailing and Consumer Services, 79, 103835.

Taqa, S. B. A. (2025). The mediating role of remote communication on the relationship between electronic human resource management practices and organizational performance in Iraqi commercial banks. Middle East Journal of Communication Studies, 5(1), Article 2. https://doi.org/10.71220/2585-005-001-001

Tian, S., Zhang, B., & He, H. (2024). Role of algorithm awareness in privacy decision-making process: A dual calculus lens. Journal of Theoretical and Applied Electronic Commerce Research, 19(2), 899–920.

Tyagi, A. (2024). Risk management in fintech. In The Emerald handbook of fintech: Reshaping finance (pp. 157–175). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83753-608-520241015

Uddin, S. F., Kirmani, M. D., Bin Sabir, L., Faisal, M. N., & Rana, N. P. (2025). Consumer resistance to WhatsApp payment system: Integrating innovation resistance theory and SOR framework. Marketing Intelligence & Planning, 43(2), 393–411.

Vänskä, A., Rauti, S., Heino, T., Carlsson, R., Mickelsson, S., & Särmäkari, N. (2024). Fair data is the new black: Online shopping, data leaks, and broadening the understanding of sustainable fashion. Fashion Theory, 28(3), 305–333. https://doi.org/10.1080/1362704X.2024.2339251

Vliegenthart, R., Vrielink, J., Dommett, K., Gibson, R., Bon, E., Chu, X., de Vreese, C., Lecheler, S., Matthes, J., & Minihold, S. (2024). Citizens' acceptance of data-driven political campaigning: A 25-country cross-national vignette study. Social Science Computer Review, 42(5), 1101–1119.

Wang, S., Cheah, J.-H., Wong, C. Y., & Ramayah, T. (2024). Progress in partial least squares structural equation modeling use in logistics and supply chain management in the last decade: A structured literature review. International Journal of Physical Distribution & Logistics Management, 54(7/8), 673–704.

Wen, B., Kurniasari, F., & Lestari, E. D. (2024). Elucidating drivers of repurchase intention in the e-marketplace through the lens of online trust-building mechanisms. Innovative Marketing, 20(1), 212.

Will Arachchige, I. S., Jahankhani, H., Oshadi Karunanayaka, K., & Amin Metwally Hussien, O. A. (2024). Exploring the balance between personalisation and automation in human–AI interaction. In Market grooming: The dark side of AI marketing (pp. 199–234). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83549-001-320241010

Yang, F. (2012). The influence mechanism and principle by studying advertising on consumer psychology. In D. Jin & S. Lin (Eds.), Advances in electronic commerce, web application and communication (Vol. 149, pp. 445–449). Springer. https://doi.org/10.1007/978-3-642-28658-2_68

Yaqub, M. Z., Badghish, S., Yaqub, R. M. S., Ali, I., & Ali, N. S. (2024). Integrating and extending the SOR model, TAM and the UTAUT to assess M-commerce adoption during COVID times. Journal of Economic and Administrative Sciences. https://doi.org/10.1108/JEAS-09-2023-0259

Zhang, J. H., Koivumäki, T., & Chalmers, D. (2024). Privacy vs convenience: Understanding intention-behavior divergence post-GDPR. Computers in Human Behavior, 160, 108382.

Zhu, L., Li, H., Wang, F.-K., He, W., & Tian, Z. (2020). How online reviews affect purchase intention: A new model based on the stimulus-organism-response (S-O-R) framework. Aslib Journal of Information Management, 72(4), 463–488.