*Advances in Consumer Research*
https://acr-journal.com/
Volume-2 | Issue-4 | September 2025

*Original Researcher Article*

# The Personalization-Privacy Paradox in AR: Consumer Trade-offs Between Hyper-Relevant Experiences and Data Vulnerability

**Dr. Rachita Sambyal**[1*]

[1*]Assistant Professor, University Institute of Applied Management Sciences(UIAMS), Panjab University, Chandigarh

**Received: 02/07/2025**
**Revised: 05/08/2025**
**Accepted: 09/09/2025**
**Published:15/09/2025**

**ABSTRACT**
Augmented Reality (AR) technology is rapidly embedding itself to various online retail applications supporting interactive and immersive shopping experiences. While these capabilities enhance consumer engagement and adoption, they rely heavily on confendiatial user data thereby intensifying privacy concerns. This creates a personalization–privacy paradox, where consumers' desire for hyper-relevant experiences is tempered by heightened vulnerability to data misuse. Although extensively studied in traditional e-commerce and social media, this paradox remains underexplored in AR contexts, where immersive features further elevate perceived risks. Grounded in Privacy Calculus Theory (PCT), this study investigates how consumers weigh perceived personalization value against privacy risks. Data for the study was collected from 276 respondents who has used AR apps/platforms and analysed using python 3.11. The findings contribute to theory by extending PCT to immersive AR environments, and to practice by guiding businesses in balancing personalization with privacy protection to foster consumer trust. Additionally, the study offers implications for technology managers tasked with regulating emerging AR technologies to safeguard user interests without stifling innovation.

**Keywords:** Augumented Reality(AR),Personalization, Privacy Concerns, immersive experience, PCT.

## INTRODUCTION

To provide customers with hyper relevant experience, many online retail firms have incorporated Augmented Reality (AR) feature on their application(apps) /platforms(Pandey & Pandey, 2025). AR help in lending online apps/platforms more features like immersability, interactability, improved visual imagery and personalization, thereby improving customer adoption of AR (Jiang et al.,2021). To provide such hyper realistic experiences AR apps/platforms access confidential information of the users like geolocation, biometrics, spatial information etc.(Cruz et al., 2025; Cunha & Krupsky 2025;Khan, 2024;). Thus providing customers with realistic and personalised experiences as the tradeoff between their privacy.

This type of data-dependence of AR powered apps/platforms has given rise to personalization-privacy paradox. This paradox is more intensified by the AR, wherein users on one side are conflicted by their desire for personalization and on the other hand are concerned by their privacy(Zimmermann et al., 2023; Patel, 2024). The very features that enhance realism require access to highly security and personal, thereby elevating the perceived stakes of data collection(Smink et al., 2019). The benefit of hyper-relevance is inextricably linked to a state of hyper-vulnerability. Despite extensive research on the personalization-privacy paradox in traditional e-commerce and social media, its implications within immersive AR environments remain significantly underexplored(Herriger et al., 2025; Mehmood et. al., 2025).Very less effort has been made to build an understanding of how consumers cognitively compare AR benefits against the perception of risk associated with sharing personal data(Qin, et al., 2024;Rauschnabel, et al., 2018; Lebeck, 2018). Also very few researchers have attempted to explore the application of PCT to the AR shopping context. Understanding this trade-off will ot merely help the academic researchers but is also critical for the businesses seeking to leverage AR for competitive advantage without eroding consumer trust, and for policymakers tasked with crafting regulations for these emerging technologies.

To address this gap, this study employs Privacy Calculus Theory (PCT) as its foundational framework. The study posit that a user's decision to use AR apps/websites is a result of a rational calculation, where the perceived personalization value is weighed against the perceived privacy risk, with trust acting as a antecedent in this decision-making process. Based on these discussions, the objectives of this research are threefold:

Obj1:To examine the influence of privacy concern on perceived privacy risk and further on trust and intention to use.
Obj2: To determine the role of trust as a key driver of intention to use, establishing its direct and essential relationship with adoption behavior

Obj3: To examine the effect of perceived personalization value on trust and intention to use.

## REVIEW OF LITERATURE

Augmented Reality technology enhances consumer visualization of the products /services(Tan & Reddy; 2022). AR enhances customer engagement by providing real world context and interactivity reduces uncertainty and helps consumer in better decision making (Thakkar & Kachhela, 2023). Studies have also shown that try-on feature supported by AR improves purchase confidence, reduce return rates and impacts consumer behavioural intention (Bezawada, 2025; Sekri, et al., 2024) The efficacy of AR technologies stems from its ability to provide hyper realistics ecperiencethat traditional online platforms cannot match (Nair et al., 2024). However, this immersive capability is computationally intensive and data-reliant, setting the stage for the central paradox this study examines.

### Privacy Concern and Perceived Privacy Risk

Privacy concern in AR refers to users' apprehension about how AR collects, process, and potentially misuse sensitive information such as biometric, facial, or location data (Herriger et al., 2025; Cowan et al., 2021). These concern arise from a perceived loss of control over personal information and influence users' trust, perceived usefulness of the app, immersive experience, and ultimately their willingness to adopt or recommend such technologies. An individual's pre-existing disposition towards privacy is a key determinant of how they perceive specific risks (Riaz, 2023). Studies consistently show that users with high privacy concern are more likely to perceive higher risks in specific online transactions and are more resistant to data disclosure (Beldad, at al., 2011; Harborth & Pape , 2021). This study positions privacy concern as an antecedent to AR-specific perceived privacy risk, hypothesizing that a user's general privacy disposition will directly influence their assessment of the risks associated with a specific AR application. Based on this following hypothesis has been formulated

Hyp1: Privacy concern is positively associated with perceived privacy risk in the context of AR app/ platform.

### Perceived Privacy Risk and Trust

Perceived privacy risk in AR apps arises when users feel vulnerable to misuse of their personal environment or identity information—for example, apps capturing biometrics, user's movements, personal information (O'Hagan et al., 2023).T hese risks often undermine trust, which represents confidence that the AR provider will safeguard data responsibly (Chandrika & Gupta, 2024). If users believe an AR app could share or sell sensitive data, their trust in the platform decreases, reducing willingness to engage (Taub et al., 2023). Based on this following hypothesis has been formulated

Hyp2: Perceived privacy risk is negatively associated with trust in the AR app/platform

### Perceived Personalization Value and Trust

Perceived personalization value is an important determinant of consumer trust in AR applications/platform. When users experience tailored content and relevant recommendations, they perceive higher utility and relevance, which fosters a sense of reliability in the platform. This personalized engagement signals that the technology understands user preferences, thereby enhancing confidence in its use. However, personalization must be perceived as beneficial rather than intrusive. If users believe personalization relies on invasive data collection, they may discount its benefits, perceiving the trade-off as unfavourable (Van Buggenhout, al. al., 2023). Trust emerges when consumers believe that data-driven personalization enhances value without compromising privacy. Thus, perceived personalization value directly strengthens trust, serving as a critical driver of sustained AR usage. Based on this following hypothesis is formulated

Hyp3: Perceived personalization value is positively associated with trust in the AR app/platform.

### Trust and Intention to Use

Trust is essential for AR app/platform usage because these app/platform often require access to personal data of the users like camera feeds, body movements, biometrics or private environments. When users trust AR applications and platforms to safeguard their data, they demonstrate greater willingness to adopt the technology despite its inherent risks (Elsotouhy, et al., 2024). Extent literature has concluded that trust in AR apps/platform directly influences user's willingness to use it for virtual try on and 3-D spatial visualization (Kang et al., 2023; Koppens, 2021). Hence, trust not only reduces uncertainty but also improvises perceptions of reliability, which are critical for sustained user engagement (Barta, et al., 2023). Based on this following hypothesis has been formulated.

Hyp4: Trust is positively associated with intention to use the AR app/platform.

### Perceived Privacy Risk and Intention to Use

In AR app/platform, risks such as collection of personal data like facial bio markers, past history, behaviour matrices, user profiling can significantly lower users' intention to use (Lehman et al., 2022). For example users may hesitate to use AR filters if they suspect their data collected is analysed without consent. Moreover, repeated reports of misuse or lack of transparency in data handling practices amplify these risks, further discouraging potential usage of technology (Bodhwani & Sharma, 2023). This negative relationship demonstrates the importance of clear communication regarding privacy policies, data usage policies of the apps/platforms using AR. Based on this following hypothesis has been formulated.

Hyp5: Perceived privacy risk is negatively associated with intention to use the AR app.

### Perceived Personalization Value and Intention to Use

Perceived personalization value enhances adoption of AR apps. Users engage more with AR app/platform when apps offer meaningful, customized, and immersive experiences, such as recommending clothes, type of makeup, different types of furniture (Ahmed, 2025). Prior research shows that high personalization increases perceived usefulness and enjoyment, directly boosting intention to use AR technologies (Adawiyah et al., 2024; Holdack et al., 2022; Hung et al., 2021). Personalization also fosters emotional connection and relevance, creating experiences that feel unique to the user and making them more willing to overlook potential privacy concerns in favor of convenience and engagement (Abtahi et al., 2023). Based on this following hypothesis has been formulated.

Hyp6: Perceived Personalization Value is negatively associated with intention to use the AR app/platform.

### Theoretical background

The study applies Privacy Calculus Theory(Culnan & Armstrong ,1999) in the context of AR app/platform to understand user's intention to use them. The theory reveals the delicate balance users strike between risks and benefits. Privacy concern increases perceived risks, undermining trust and discouraging intention to use. Personalization value strengthens perceived benefits, motivating use despite risks. Trust act as an enabler for adoption when users feel confident their sensitive AR data will be protected. This perspective explains why some users avoid AR apps due to privacy fears, while others adopt them eagerly when personalization value is high and trust in the provider is strong. Furthermore, the framework highlights that effective risk communication and transparent privacy policies can play a decisive role in tipping the balance toward adoption. Based on this following conceptual model of the study is proposed(Figure 1).

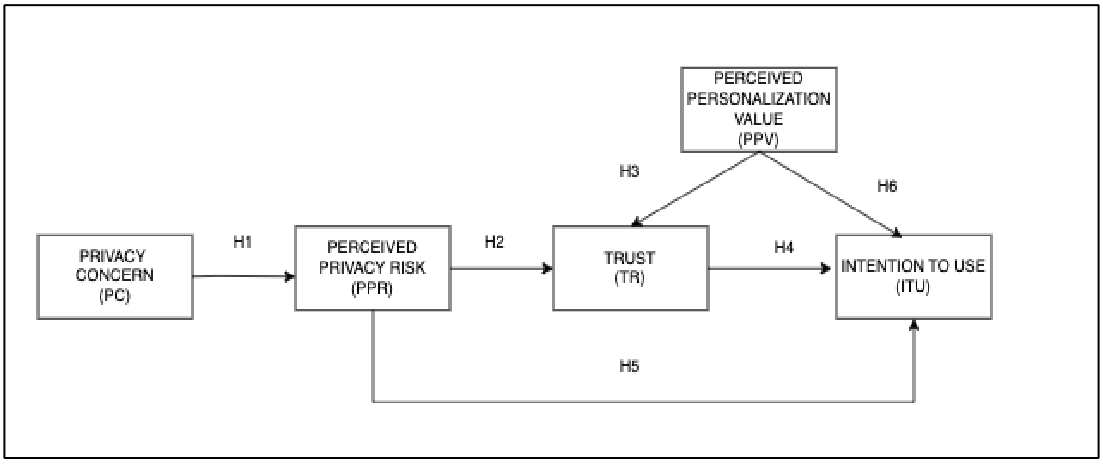
PERCEIVED PERSONALIZATION VALUE (PPV)
H3
H6
PRIVACY CONCERN (PC)
H1
PERCEIVED PRIVACY RISK (PPR)
H2
TRUST (TR)
H4
INTENTION TO USE (ITU)
H5

**FIGURE1**: **Conceptual Model of the Study**
Source: Authors' own

## RESEARCH METHODOLOGY

The methodology followed for the research is as follows.

### Research Design

The study undertaken uses quantitative research design. Data was collected from respondents who had used an AR application or platform for any of the following in the past one year: personal purchase, creating a social media post, used for education or played an immersive game.

### Measures and Instrumentation

The data was collected with the help of a self structured questionnaire(Annexture I**)**. The items related to privacy concerns were adapted from Xu et al, 2012 and Smith et al., 1996; for perceived privacy risk from Malhotra et al., 2004, Dinev& Hart, 2006; for Trust in AR Apps from Gefen et al., 2012 and McKnight et al., 2003; for perceived personalization value from Awad & Krishnan, 2006 and Bleier & Eisenbeiss,2015 and intention to use from Venkatesh et al, 2003 and Rauschnabel et al., 2019 respectively. All items were measures on likert scale 1-5 where 1 means strongly disagree and 5 means strongly agree.

### Sampling and Data Collection

The study employed purposive sampling to ensure that respondents had relevant experience with AR app/platform. The participants were expected to have used an AR-based platform or application for personal purchases within the past one year. This criterion ensured that respondents were familiar with both the personalization benefits and privacy implications of AR usage. The questionnaire for data collection was distributed via social media channels, email invitations, and professional networks. A total of 276 valid responses were obtained, which were deemed adequate for SEM.

### Data Analysis Strategy

The data was analysed using Python 3.11 on Google collab. Various data analysis libraries used were pandas for data preprocessing and numpy for numerical computations. For factor analysis (EFA) pingouin and semopy was used for confirmatory factor analysis (CFA).

## RESULT AND DISCUSSIONS

The result of the data analysis shows that (Table 1) of the sample of 276, 45.65 % were between the age of 18-24 years, 44.20% were between the age of 25-34 years and 10.14 % were of 35 and above age. Table 2 presents the results of the reliability and validity assessment for the measurement model.The KMO value and factor loadings for all items exceed the recommended threshold of 0.70, demonstrating strong item reliability. Cronbach's alpha values for all constructs are above 0.70, indicating satisfactory internal consistency. Composite Reliability (CR) values, ranged from 0.867 to 0.964, also exceed the 0.70 benchmark, confirming construct reliability (Hair et. al., 2022) . Average Variance Extracted (AVE) values for all constructs are above 0.50, establishing convergent validity(Fornell and Larcker, 1981). These results collectively suggest that the measurement model exhibits robust reliability and validity, supporting its use in subsequent analysis.

**Table 1: Demographic Profile of Respondents**

| Variable | Category | Frequency | Percentage (%) |
|---|---|---|---|
| Age | 18-24 years | 126 | 45.65 |
| | 25-34 years | 122 | 44.20 |
| | 35-and above | 28 | 10.14 |
| Gender | Male | 140 | 50.72 |
| | Female | 132 | 47.83 |
| | Other / Prefer not to say | 4 | 1.45 |
| AR app type | Social Media | 76 | 27.54 |
| | Education | 32 | 11.59 |
| | Gaming | 28 | 10.14 |
| | Shopping | 140 | 50.72 |

Source: Author's own

Table 3 reports the results of discriminant validity assessment using the Heterotrait-Monotrait (HTMT) ratio of correlations. All HTMT values are below the acceptable threshold of 0.85 (Henseler et al., 2015), indicating tthe constructs are empirically distinct from one another. Thereby establishing discriminant validity.

**Table 2: Analysis of measurement model: Reliability and Validity**

| Construct | Items | Factor Loadings | Cronbach's Alpha (α) | Composite Reliability (CR) | Average Variance Extracted (AVE) |
|---|---|---|---|---|---|
| Perceived | PPV1 | 0.966 | 0.970 | 0.964 | 0.87 |

| | | | | | |
|---|---|---|---|---|---|
| Personalization Value (PPV) | PPV2 | 0.902 | | | |
| | PPV3 | 0.921 | | | |
| | PPV4 | 0.942 | | | |
| Perceived Privacy Risk (PPR) | PPR1 | 0.857 | 0.943 | 0.867 | 0.621 |
| | PPR2 | 0.742 | | | |
| | PPR3 | 0.793 | | | |
| | PPR4 | 0.756 | | | |
| Trust (TR) | TR1 | 0.774 | 0.890 | 0.867 | 0.621 |
| | TR2 | 0.709 | | | |
| | TR3 | 0.906 | | | |
| | TR4 | 0.849 | | | |
| Intention to Use (ITU) | ITU1 | 0.952 | 0.965 | 0.831 | 0.831 |
| | ITU2 | 0.929 | | | |
| | ITU3 | 0.924 | | | |
| | ITU4 | 0.837 | | | |
| Privacy Concern (PC) | PC1 | 0.844 | 0.947 | 0.779 | 0.779 |
| | PC2 | 0.876 | | | |
| | PC3 | 0.896 | | | |
| | PC4 | 0.913 | | | |
| KMO=.876, Significance value=0.003 | | | | | |

*Source: Ouput from python*

The measurement model's outcome (Table 4) demonstrated a favourable fit with all the indices i.e $\chi2$ /df, GFI , CFI , TLI and RMSEA with values 2.201, 0.956, 0.962, 0.994 and0.021 respectively(Kline, 2015; Tabachnick and Fidell, 2012).

**Table 3: Discriminant Validity (HTMT Ratio)**

| **Construct** | **ITU** | **PC** | **PPR** | **PPV** | **TR** |
|---|---|---|---|---|---|
| **ITU** | 1 | | | | |
| **PC** | 0.238 | 1 | | | |

| Construct | ITU | PC | PPR | PPV | TR |
|---|---|---|---|---|---|
| PPR | 0.475 | 0.459 | 1 | | |
| PPV | 0.162 | 0.206 | 0.263 | 1 | |
| TR | 0.285 | 0.270 | 0.659 | 0.237 | 1 |

*Source: Output from python*

While the indices values obtained for the structural model for χ2 /df , GFI, CFI, TLI and RMSEA were 2.221, 0.954 , 0.993 , 0.991 and 0.025 respectively. Thus, the model fit values support the acceptance of the proposed model.

**Table 4: Goodness-of-Fit Indices for the Structural Model**

| Fit Index | Recommended Value | Measurment model | Structural model | Result |
|---|---|---|---|---|
| $\chi^2$/df | < 3.0 | 2.201 | 2.221 | **Good** |
| Standardized Root Mean Square Residual (SRMR) | < 0.08 | 0.040 | 0.045 | **Good** |
| Goodness of Fit Index(GFI) | > 0.90 | 0.956 | 0.954 | **Good** |
| Comparative Fit Index (CFI) | > 0.90 | 0.995 | 0.993 | **Good** |
| Tucker-Lewis Index (TLI) | > 0.90 | 0.994 | 0.991 | **Good** |
| Root Mean Square Error of Approximation (RMSEA) | < 0.08 | 0.021 | 0.025 | **Good** |

*Source: output from python*

Table 5 presents the results of the structural path analysis.All six hypothesized relationships were found to be statistically significant at p < 0.001, thereby supporting the proposed model. Privacy Concern had a strong positive effect on Perceived Privacy Risk (H1: β = 0.743, C.R. = 11.203), confirming that users with high privacy concerns are more likely to perceive risks when engaging with AR app/platform. In turn, Perceived Privacy Risk negatively influenced Trust (H2: β = -0.424, C.R. = -7.367), showing that when risks are salient, consumer trust is undermined. At the same time, Perceived Personalization Value exerted a strong positive effect on Trust (H3: β = 0.631, C.R. = 11.230), highlighting the role of personalization in building trust in AR app usage. Trust istrongly predicted Intention to Use (H4: β = 0.771, C.R. = 7.762), reinforcing its position as a strong strong predictor of usage intention. Moreover, Perceived Privacy Risk had a significant negative effect on Intention to Use (H5: β = -0.297, C.R. = -3.822), indicating that privacy concerns directly discourage AR usage. Conversely, Perceived Personalization Value positively influenced Intention to Use (H6: β = 0.547, C.R. = 6.213), showing that users are willing to tradeoff privacy concerns in lieu of personalized experience.

**Table 5: Hypothesis Testing**

| Hypothesis | Path | Std. Estimate (β) | S.E. | C.R. | p-value | Result |
|---|---|---|---|---|---|---|
| H1 | PC → PPR | 0.743 | 0.066 | 11.203 | *** | **Supported** |
| H2 | PPR → TR | -0.424 | 0.058 | -7.367 | *** | **Supported** |
| H3 | PPV → TR | 0.631 | 0.056 | 11.230 | *** | **Supported** |
| H4 | TR → ITU | 0.771 | 00.099 | 7.762 | *** | **Supported** |

| **Hypothesis** | **Path** | **Std. Estimate (β)** | **S.E.** | **C.R.** | **p-value** | **Result** |
|---|---|---|---|---|---|---|
| H5 | PPR → ITU | -0.297 | 0.077 | -3.822 | *** | **Supported** |
| H6 | PPV → ITU | 0.547 | 0.088 | 6.213 | *** | **Supported** |

*****p < 0.001**

*Source: output from python*

The results of this study emperically support the personalization–privacy paradox in the context of augmented reality (AR) application/platforms. Specifically, the findings reveal a dual dynamic in consumer decision-making: while privacy concerns intensify perceived risks, thereby eroding trust and discouraging adoption, the perceived benefits of personalization enhance both trust and behavioral intention to use AR platforms.

The positive relationship between privacy concern and perceived privacy risk reinforces prior work in online privacy concern studies, which suggests that consumers who are more sensitive to personal data misuse are more likely to perceive risks in data-driven technologies(Roesner & Kohno, 2021). In AR contexts, these risks are more magnified as the type of data collectd by AR apps is more personal.This findings are consistant with the findings of Yap et al., 2021 which outline to ensure more usage of AR apps/platforms firms need to cater to privacy issues emerging with technology usage.

The study highlights that perceived privacy risk negatively influences trust and intention to use. These results align with results of Zhang, 2024 and Almaiah et al, 2023 which concluded that elevated perceptions of privacy risk hinders the user's willinginess to adopt technology. In the AR context, this suggests that no matter how sophisticated the personalization features may be, if consumers perceive the platform as unsafe or intrusive, their trust in the platform declines and their likelihood of using the service is hampered. This emphasizes the fragility of consumer trust in digital ecosystems, particularly those operating in immersive environments where personal data collection is highly visible.

The results also demonstrate that perceived personalization value exerts a strong positive effect on both trust and intention to use**.** AR applications thrive on their ability to deliver hyper realistic experiences, such as virtual tryons, spatial positioning of digital products in physical spaces etc. When consumers perceive these personalized interactions as valuable, their willingness to accept potential privacy risks increases(Liu, & Tao,2022). This suggests that personalization can function as a counterweight to risk perceptions, shifting the cost–benefit calculation in favor of adoption.

Furthermore, user's trust in AR app/platformemerges as the strongest predictor of intention to use. Users are more willing to disclose personal information if they believe the AR app/platform will handle it responsibly and transparently(Sun et al, 2025). This reinforces the view that trust is not just another variable in adoption models but a central enabler of digital engagement in privacy-sensitive contexts.

Taken together, these findings extend our understanding of the personalization–privacy paradox by showing how these opposing forces play out in the AR environment. Unlike traditional online platforms, AR applications operate in highly immersive and data-intensive ecosystems, making the trade-offs more visible and more consequential. The results suggest that AR adoption depends on firms' ability to simultaneously manage consumer fears about data vulnerability and deliver personalization experiences that are both meaningful and tangible (Pandey & Pandey, 2025).

Finally, the study concludes that users are not passive victims of personalization or privacy threats but active evaluators of trade-offs(Malik, 2024). Their technology usage is shaped by weighing of risks and benefits. This reflects a broader cultural shift in customer engagment on online platforms where users assessse the value of personalization against the vulnerabilities of data privacy.

## Managerial Implications

The study has many implications for managers. Technology managers need to minimize the privacy concerns of the user regarding AR powered apps/platforms by including transparency in the data sharing guidelines, simplyfying consent mechanism & security guidelines. Simultaneously disclosure regarding what data /type of data is required, its storage and further usage for providing hyper relevant AR experiences will further strengthen the trust of the users. Ultimately, managers who successfully balance privacy protection with meaningful personalization will not only mitigate consumer skepticism but also foster stronger adoption intentions, thereby sustaing long term user engagement.

## Limitations and Future Research

While the study sheds light on the personalization–privacy paradox in AR applications, it faces certain limitations .First, data for the study was self reported and there was no control over the type of AR usage.

Future studies can adopt experimental research design wherein the users can first provided AR experience and then data can be collected. Second, the sample was restricted to users who had engaged with AR applications for personal purchases within the past year. While this ensures relevance, it may limit generalizability to non-purchasing users or those in other contexts such as education, entertainment, or healthcare. Finally, incorporating different data like like eye tracking, economic status, technical knowledge etc can strengthen the robustness of findings. Finally, the research was confined to a single cultural and geographical settings, which may influence privacy perceptions and personalization preferences. Comparative studies across different cultural settings eg digital divide could provide deeper insights into how context moderates the personalization–privacy paradox.

## REFERENCES

1. Abtahi, A., Shafique, T., Haque, T., Siam, S. A. J., & Rahman, A. (2023). Exploring consumer preferences: The significance of personalization in e-commerce. *Malaysian E Commerce Journal (MECJ)*, *8*(1), 01-07.
2. Adawiyah, S. R., Purwandari, B., Eitiveni, I., & Purwaningsih, E. H. (2024). The influence of AI and AR technology in personalized recommendations on customer usage intention: a case study of cosmetic products on shopee. *Applied Sciences*, *14*(13), 5786.
3. Ahmed, I. (2025). The Role of Augmented Reality in Enhancing User Experiences in Retail. *International journal of applied biology and forensic*, *9*(2), 116-134.
4. Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability*, *15*(13), 9908.
5. Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.
6. Barta, S., Gurrea, R., & Flavián, C. (2023). How augmented reality increases engagement through its impact on risk and the decision process. *Cyberpsychology, Behavior, and Social Networking*, *26*(3), 177-187.
7. Beldad, A., De Jong, M., & Steehouder, M. (2011). I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior*, *27*(6), 2233-2242.
8. Bezawada, S. (2025). The Influence of Augmented Reality Clothing on Consumer Behavior and Its Impact on Online Shopping. *Available at SSRN 5264995*.
9. Bleier, A., & Eisenbeiss, M. (2015). Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science*, *34*(5), 669-688.
10. Bodhwani, K., & Sharma, A. (2023). The Future of Augmented Reality: Emerging Trends and Challenges. *landscape*, 63.
11. Chandrika, M., & Gupta, P. (2024, November). Ethical and Privacy Implications of Augmented Reality. In *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.
12. Chen, C., & Duan, Y. (2022). Impact of personalization and privacy concerns on information disclosure and pricing. *Journal of Retailing and Consumer Services*, *69*, 103099.
13. Cowan, K., Javornik, A., & Jiang, P. (2021). Privacy concerns when using augmented reality face filters? Explaining why and when use avoidance occurs. *Psychology & Marketing*, *38*(10), 1799-1813.
14. Cruz, A. C., Costa, R. L. D. C., Santos, L., Rabadão, C., Marto, A., & Gonçalves, A. (2025). Assessing User Perceptions and Preferences on Applying Obfuscation Techniques for Privacy Protection in Augmented Reality. *Future Internet*, *17*(2), 55.
15. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.
16. Cunha, M. N., & Krupsky, O. P. (2025). Transforming online retail: The impact of augmented and virtual reality on consumer engagement and experience in e-commerce. *Uluslararası Sosyal Siyasal ve Mali Araştırmalar Dergisi*, *5*(1), 189-201.
17. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.
18. Elsotouhy, M. M., Khashan, M. A., Thabet, M. Z., Galal, H. M., & Ghonim, M. A. (2024). Do the technological anxiety, privacy and physical risks matter in retail customers' adoption of AR apps? An extended UTAUT2 approach. *EuroMed Journal of Business*.
19. Fornell, C. and Larcker, F.D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *International Journal of Current Research and Academic Review*, 18(1), 39-50.
20. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 51-90.
21. Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2022). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 3rd ed., Sage, Thousand Oaks, CA.
22. Harborth, D., & Pape, S. (2021). Investigating privacy concerns related to mobile augmented reality Apps–A vignette based online experiment. *Computers in Human Behavior*, *122*, 106833.
23. Henseler, J., Ringle, C.M. and Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling.

*Journal of the Academy of Marketing Science*, 43(1), 115-135.

24. Herriger, C., Merlo, O., Eisingerich, A. B., & Arigayota, A. R. (2025). Context-Contingent Privacy Concerns and Exploration of the Privacy Paradox in the Age of AI, Augmented Reality, Big Data, and the Internet of Things: Systematic Review. *Journal of Medical Internet Research*, *27*, e71951.
25. Holdack, E., Lurie-Stoyanov, K., & Fromme, H. F. (2022). The role of perceived enjoyment and perceived informativeness in assessing the acceptance of AR wearables. *Journal of Retailing and Consumer Services*, *65*, 102259.
26. Hung, S. W., Chang, C. W., & Ma, Y. C. (2021). A new reality: Exploring continuance intention to use mobile augmented reality for entertainment purposes. *Technology in Society*, *67*, 101757.
27. Jiang, Y., Wang, X., & Yuen, K. F. (2021). Augmented reality shopping application usage: The influence of attitude, value, and characteristics of innovation. *Journal of Retailing and Consumer Services*, *63*, 102720.
28. Kang, J. Y. M., Kim, J. E., Lee, J. Y., & Lin, S. H. (2023). How mobile augmented reality digitally transforms the retail sector: examining trust in augmented reality apps and online/offline store patronage intention. *Journal of Fashion Marketing and Management: An International Journal*, *27*(1), 161-181.
29. Khan, K. (2024). Advancements and Challenges in 360 Augmented Reality Video Streaming: A Comprehensive Review. *International Journal of Computing*, *13*(1), 1-20.
30. Kline, R.B. (2015), Principles and Practice of Structural Equation Modeling, Guilford Publications, New York.
31. Koppens, R. (2021). E-Commerce Retail & Augmented Reality. An Exploratory Study about Virtual Fitting Room Technologies and Online Customer Experiences.
32. Lebeck, K., Ruth, K., Kohno, T., & Roesner, F. (2018, May). Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 392-408). IEEE.
33. Lehman, S. M., Alrumayh, A. S., Kolhe, K., Ling, H., & Tan, C. C. (2022). Hidden in plain sight: Exploring privacy risks of mobile augmented reality applications. *ACM Transactions on Privacy and Security*, *25*(4), 1-35.
34. Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, *127*, 107026.
35. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), 336-355.
36. Malik, M. S. (2024). Analyzing the trade-offs of data sharing in social networks and privacy concerns. *International Journal for Electronic Crime Investigation*, *8*(4).
37. McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, *13*(3), 334-359.
38. Mehmood, K., Rehman, M. A., Abbass, A., & Woyo, E. (2025). Adaptive pathways: understanding consumer adaptive behavior toward hyper-personalized fashion retailing in emerging markets. *Journal of Consumer Behaviour*.
39. Nair, A. J., Manohar, S., Mittal, A., & Chaudhry, R. (2024). Unleashing digital frontiers: Bridging realities of augmented reality, virtual reality, and the metaverse. In *The metaverse dilemma: Challenges and opportunities for business and society* (pp. 85-112). Emerald Publishing Limited.
40. O'Hagan, J., Saeghe, P., Gugenheimer, J., Medeiros, D., Marky, K., Khamis, M., & McGill, M. (2023). Privacy-enhancing technology and everyday augmented reality: Understanding bystanders' varying needs for awareness and consent. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *6*(4), 1-35.
41. Pandey, P. K., & Pandey, P. K. (2025). Unveiling the transformative power of augmented reality in retail: a systematic literature analysis. *Journal of Strategy and Management*.
42. Pandey, P. K., & Pandey, P. K. (2025). Unveiling the transformative power of augmented reality in retail: a systematic literature analysis. *Journal of Strategy and Management*.
43. Patel, K. (2024). Revolutionizing Customer Experience: Integrating Blockchain with AR and VR in Retail. In *Augmenting Retail Reality, Part B: Blockchain, AR, VR, and AI* (pp. 1-22). Emerald Publishing Limited.
44. Qin, H., David, A., Harun, A., Mamun, M. R. A., Peak, D., & Prybutok, V. (2024). Assessing user benefits and privacy concerns in utilitarian and hedonic mobile augmented reality apps. *Industrial Management & Data Systems*, *124*(1), 442-482.
45. Rauschnabel, P. A., Felix, R., & Hinsch, C. (2019). Augmented reality marketing: How mobile AR-apps can improve brands through inspiration. *Journal of Retailing and Consumer Services*, *49*, 43–53. https://doi.org/10.1016/j.jretconser.2019.03.004
46. Rauschnabel, P. A., He, J., & Ro, Y. K. (2018). Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research*, *92*, 374-384.
47. Riaz, S. (2023). *The role of regulatory disposition in explaining the privacy paradox: a study of internet users' interaction with cookie consent notices* (Doctoral dissertation, Royal Holloway, University of London).
48. Roesner, F., & Kohno, T. (2021). Security and privacy for augmented reality: Our 10-year retrospective. In *VR4Sec: 1st International Workshop on Security for XR and XR for Security*.

49. Sekri, K., Bouzaabia, O., Rzem, H., & Juárez-Varón, D. (2024). Effects of virtual try-on technology as an innovative e-commerce tool on consumers' online purchase intentions. *European Journal of Innovation Management*.
50. Smink, A. R., Frowijn, S., van Reijmersdal, E. A., van Noort, G., & Neijens, P. C. (2019). Try online before you buy: How does shopping with augmented reality affect brand responses and personal data disclosure. *Electronic Commerce Research and Applications*, *35*, 100854.
51. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.
52. Sun, Y., Freeman, J., Shoenberger, H., & Shen, F. (2025). To Tell or Not to Tell: Investigating the Persuasive Appeal of Information Transparency for AR-Powered E-Commerce Sites. *International Journal of Human–Computer Interaction*, 1-15.
53. Tabachnick, B.G. and Fidell, L.S. (2012), Using Multivariate Statistics, 6th ed., Person Education, Boston
54. Tan, Y. C., Chandukala, S. R., & Reddy, S. K. (2022). Augmented reality in retail and its impact on sales. *Journal of marketing*, *86*(1), 48-66.
55. Taub, G., Elmalech, A., & Aharony, N. (2023). Willingness to grant access to personal information among augmented reality mobile app users. *Personal and Ubiquitous Computing*, *27*(2), 363-377.
56. Thakkar, K. Y., Joshi, B. B., & Kachhela, P. P. (2023). Consumer engagement with augmented reality (AR) in marketing: Exploring the use of ar technology in marketing campaigns and its impact on consumer engagement, brand experiences, and purchase decisions. *Journal of Management Research and Analysis*, *10*(2), 99-105.
57. Van Buggenhout, N., Van den Broeck, W., Van Zeeland, I., & Pierson, J. (2023). Personal data and personalisation in media: experts' perceptions of value, benefits, and risks. *Digital Policy, Regulation and Governance*, *25*(3), 305-324.
58. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540
59. Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.
60. Yap, S. F., Xu, Y., & Tan, L. (2021). Coping with crisis: The paradox of technology and consumer vulnerability. *International Journal of Consumer Studies*, *45*(6), 1239-1257.
61. Zhang, Y. (2024). Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors. *International Journal of Information Management Data Insights*, *4*(2), 100270.
62. Zimmermann, R., Mora, D., Cirqueira, D., Helfert, M., Bezbradica, M., Werth, D., ... & Auinger, A. (2023). Enhancing brick-and-mortar store shopping experience with an augmented reality shopping assistant application using personalized recommendations and explainable artificial intelligence. *Journal of Research in Interactive Marketing*, *17*(2), 273-298.