

Virtual Vogue: Unveiling Privacy Trade-offs in the Fashion Metaverse

Changhyun (Lyon) Nam¹, JeaGu Yu², and Srikant Manchiraju¹

¹Florida State University & ²Chung-Ang University

Keywords: Metaverse, fashion brands, sports brands, trust, benefits, privacy concerns

Introduction. The Metaverse, a three-dimensional world, is an evolving virtual space where users can interact with a computer-generated environment and other users (Friesen, 2017). In the fashion industry, the Metaverse offers opportunities for virtual try-ons, fashion shows, and social interactions (Mystakidis, 2022; Wang et al., 2022). As fashion and sports brands (e.g., Gucci, Nike, Ralph Lauren, etc.) integrate virtual environments into their marketing strategies, consumer interactions with these platforms raise critical questions about privacy and technology acceptance. This study explored the intersection of privacy concerns and the perceived benefits of metaverse technologies within the fashion field.

The Privacy Calculus Theory (PCT; Laufer & Wolfe, 1977) posits that individuals make rational decisions about disclosing personal information by weighing perceived benefits against the privacy risks associated with the disclosure. This decision-making process involves a cost-benefit analysis where users assess the potential advantages of sharing data, such as personalized services or social connectivity, against potential threats to their privacy, like data breaches or misuse (Dinev & Hart, 2006). Trust in data protection measures and the sensitivity of the information are also crucial factors influencing this calculus (Li, 2012). The theory has been applied across various contexts, including digital health, online shopping, and social media. In a study by Schomakers et al. (2022), the PCT was employed across diverse smart technology contexts—autonomous driving, activity trackers, and cardiac device remote monitoring. It illuminated the critical trade-offs users make between perceived benefits and privacy risks. Their findings revealed that while perceived benefits powerfully drive user intention to adopt technology, privacy concerns could remarkably deter usage. Furthermore, trust in data protection emerged as a pivotal factor influencing user intention and privacy concerns.

Proposed Conceptual Framework. Applying the PCT (Awad & Krishnan, 2006; Phelps et al., 2001), we investigated how users negotiate the trade-off between the perceived benefits of engaging in the fashion metaverse and the potential risks to their privacy. By examining factors such as perceived information sensitivity, trust, and perceived benefit, this study aimed to examine an understanding of consumer behavior and inform strategies for fostering responsible and user-centric Metaverse experiences in the fashion industry. Based on the extant literature review (Li, 2012; Schomakers et al., 2022), the following hypotheses (Hs) were proposed:

H1: Perceived information significantly influences (a) trust in data privacy, (b) perceived benefit, and (c) intention to use.

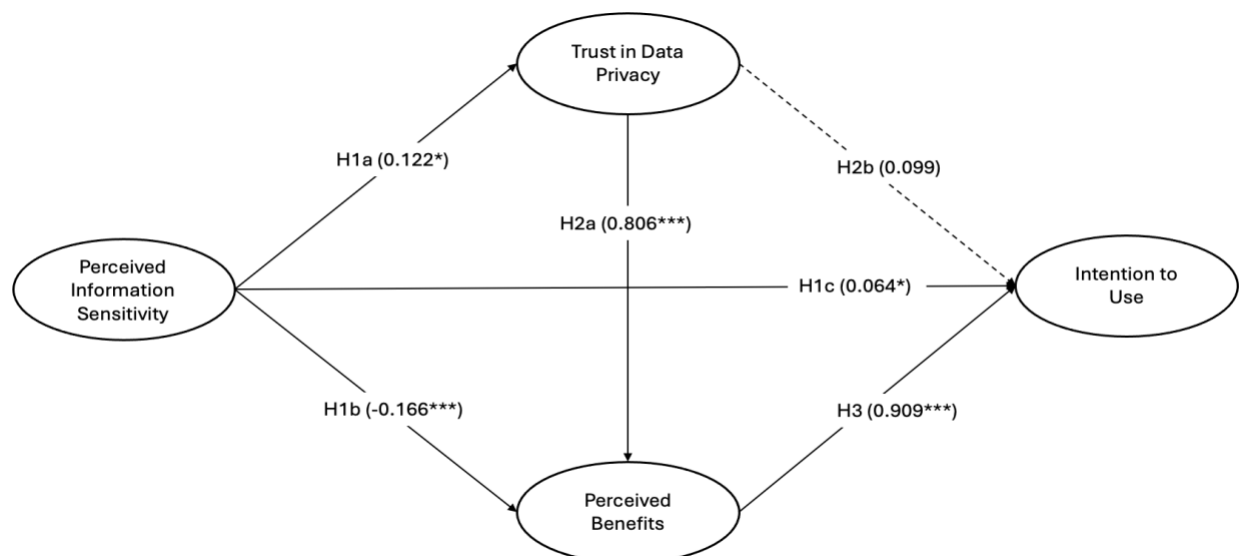
H2: Trust in data privacy significantly influences (a) perceived benefit and (b) intention to use.

H3: Perceived benefit significantly influences intention to use.

Method. Participants were recruited through an online survey using Amazon Mechanical Turk. The survey comprised three sections: (a) demographics, (b) open-ended questions, and (c) multiple-item measures including perceived information sensitivity (four items; Bansal & Gefen, 2010), trust in data privacy (four items; Schomakers et al., 2022), perceived benefits (eight items; Schomakers et al., 2022),

and intention to use the fashion metaverse platform (eight items; Bansal & Gefen, 2010). Participants responded to the questionnaire using a 7-point Likert scale. Structural equation modeling (SEM) was employed to test the proposed conceptual framework (see Figure 1). Additionally, various analyses were performed, including descriptive statistics and reliability analysis. All statistical analyses were conducted using SPSS 28 and AMOS 28 software.

Results. In total, 515 participants' responses were collected. The final usable sample of 455 was used for data analyses. Most participants were male, $n = 258$ (57%), and Caucasian, $n = 363$ (80%), with an average age of 45. Further, 47.5% ($n = 216$) had annual incomes between US\$50,000 and US\$74,999. Most respondents were full-time employees 94.1% ($n = 428$) and had a college degree 80.0% ($n = 364$). We conducted an SEM analysis to confirm the proposed conceptual framework—the regression estimate of how each variable affects the intention to use Metaverse. The measurement model showed an acceptable fit of the data (S-B $\chi^2 = 146.491$, $df = 71$, S-B $\chi^2/df = 2.063$, CFI = 0.981, RMSEA = 0.058, TLI = 0.976, RFI = 0.954). After confirming the psychometric properties of the measurement model, the hypotheses in the proposed conceptual framework were tested. As shown in Figure 1, SEM results showed that perceived information sensitivity had a significant effect on trust in data privacy (H1a; $\beta = 0.122$, $SE = 0.054$, $p < 0.05$), perceived benefits (H1b; $\beta = -0.166$, $SE = 0.039$, $p < 0.001$), and intention to use (H1c; $\beta = 0.064$, $SE = 0.032$, $p < 0.05$). Trust in data privacy had a significant effect on perceived benefit (H2a; $\beta = 0.806$, $SE = 0.054$, $p < 0.001$), but there was no significant effect on the intention to use (H2b; $\beta = 0.099$, $SE = 0.066$, $p = 0.078$). There were significant and positive effects of perceived benefit on intention to use (H3; $\beta = 0.909$, $SE = 0.089$, $p < 0.001$).



Note. $p < 0.05^*$; $p < 0.001^{***}$

Figure 1. Proposed conceptual framework.

Conclusion. The significance of this research lies in its ability to unravel the complex interplay between privacy concerns and technology acceptance among users in fashion Metaverse platforms. As Metaverse platforms blur the lines between virtual and physical realities, understanding how users perceive and manage privacy risks while seeking the benefits of virtual fashion experiences becomes crucial. The findings of this study identified that the perception of information sensitivity forms fashion Metaverse

usage. Even if individuals have information sensitivity, it was confirmed that usage intention is formed through trust in data privacy and perceived benefits of individual information protection. In addition, perceived benefits mediate among perceived information, trust, and intention to use in fashion Metaverse platforms. Therefore, Metaverse shopping planners should emphasize individual information protection policies and develop strategies to increase usage by promoting perceived benefits. Furthermore, the proposed conceptual framework was utilized to examine users' intentions within the fashion Metaverse platform in the fashion and e-commerce industries. This framework is valuable and essential for understanding the perceived benefits of engagement and potential privacy risks in metaverse platforms. Consequently, it can assist platform designers, retailers, and creators in identifying users' privacy concerns, benefits, and trust. Additionally, it can develop their fashion Metaverse platforms, enhancing users' intention to use them.

Overall, this study will contribute to understanding by examining the benefits and trust in data protection and its impact on user acceptance, which is vital for fostering a secure and thriving digital fashion ecosystem. By exploring the complexities of perceived information sensitivity, the research will offer insights into user behavior, guiding designers and policymakers in creating privacy-conscious and user-friendly virtual fashion platforms.

References

- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1), 13–28.
- Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern, and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138–150.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80.
- Friesen, N. (2017). *The textbook and the lecture: Education in the age of new media*. Johns Hopkins University Press.
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22–42.
- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471–481.
- Mystakidis, S. (2022). Metaverse. *Encyclopedia*, 2(1), 486–497.
- Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: an empirical investigation. *Journal of Interactive Marketing*, 15(4), 2–17.
- Schomakers, E. M., Lidynia, C., & Ziefle, M. (2022). The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. *International Journal of Human-Computer Interaction*, 38(13), 1276–1289.