

Individual Privacy Perception in the Digital Age: The Interaction of Artificial Intelligence Attitude and Dependency

Üzeyir Fidan¹

¹ PhD, Uşak University, Distance
Education Vocational School

Uşak/Türkiye

ROR ID:

<https://ror.org/05es91y67>

ORCID:

[0000-0003-3451-4344](https://orcid.org/0000-0003-3451-4344)

E-Mail:

uzeyir.fidan@usak.edu.tr

September 2025

Volume:22

Issue:5

DOI: 10.26466/opusjsr.1725180

Abstract

The increasing dependence on AI-supported services raises important questions about how positive beliefs about AI can turn into privacy risks. This study tests a gender-moderated mediation model of AI attitude, AI dependence, and online privacy concern (OPC) among Turkish university students. A cross-sectional survey conducted on 478 students using validated scales (AIAS-4, AI Dependency Scale, OPC Scale) was analyzed using structural equation modeling and the PROCESS Model 59. The measurement model demonstrated excellent fit ($\chi^2/df = 1.01$, CFI = 0.999, RMSEA = 0.005) and strong reliability-validity indicators. AI attitude significantly increased AI dependency ($\beta = .50$, $p < .001$), which in turn strengthened OPC ($\beta = .77$, $p < .001$). Gender moderates both relationships and reveals a significant moderator-mediation index (-11 ; 95% CI $[-.21, -.01]$). Overall, the model explains 28% of the variance in OPC. The findings reveal a two-way effect of positive AI attitudes: while promoting beneficial participation, they also increase dependency-based privacy concerns, particularly among female users. Organizations should integrate privacy-aware AI literacy and gender-sensitive feedback mechanisms into digital platforms to mitigate risks while maintaining trust.

Keywords: digitalization, AI attitude, AI dependence, online privacy concern.

Öz

YZ destekli hizmetlere olan bağımlılığın artması, YZ hakkındaki olumlu inançların nasıl gizlilik risklerine dönüştüğü konusunda önemli sorular ortaya çıkarmaktadır. Bu çalışma, Türk üniversite öğrencileri arasında YZ tutumu, YZ bağımlılığı ve çevrimiçi gizlilik endişesi (OPC) arasında cinsiyete bağlı, ılımlı arabuluculuk modelini test etmektedir. 478 öğrenci üzerinde yapılan kesitsel bir anket, geçerliliği kanıtlanmış ölçekler (AIAS-4, YZ Bağımlılık Ölçeği, OPC ölçeği) kullanılarak gerçekleştirilmiş ve yapısal eşitlik modellemesi, PROCESS Model 59 ile analiz edilmiştir. Ölçüm modeli mükemmel uyum ($\chi^2/df = 1,01$, CFI = 0,999, RMSEA = 0,005) ve güçlü güvenilirlik-geçerlilik göstergeleri sergilemiştir. YZ tutumu, YZ bağımlılığını önemli ölçüde artırmakta ($\beta = .50$, $p < .001$), bu da OPC'yi güçlendirmektedir ($\beta = .77$, $p < .001$). Cinsiyet, her iki bağlantıyı da moderatör olarak etkilemekte ve önemli bir moderatör-aracılık indeksi (-11 ; %95 CI $[-.21, -.01]$) ortaya çıkarmıştır. Genel olarak, model OPC varyansının %28'ini açıklamıştır. Bulgular, olumlu YZ tutumlarının iki yönlü bir etkisi olduğunu ortaya koymaktadır: faydalı katılımı teşvik ederken, özellikle kadın kullanıcılar arasında bağımlılığa dayalı gizlilik kaygılarını artırmaktadır. Kurumlar, güveni sürdürürken ortaya çıkan riskleri azaltmak için dijital platformlara gizlilik bilincine sahip YZ okuryazarlığı ve cinsiyete duyarlı geri bildirim mekanizmaları entegre etmelidir.

Anahtar Kelimeler: dijitalleşme, yapay zeka tutumu, yapay zeka bağımlılığı, çevrimiçi gizlilik endişesi

Introduction

The rapid development of digital technologies is fundamentally transforming individuals' daily lives, communication patterns, and strategies for accessing information. In particular, the widespread use of artificial intelligence (AI)-based applications is reshaping individuals' behavior in digital environments and their perceptions of privacy (Li & Zhang, 2017). Despite the advantages offered by AI, such as automation, personalized services, and data analytics, the collection, processing, and interpretation of individuals' private data raise many ethical and psychological concerns (Maphosa, 2024).

In recent years, individuals' attitudes toward AI technologies have begun to play a decisive role in understanding their interaction with these technologies. Positive attitudes toward AI increase adaptation to technology and the level of use of digital services, while negative attitudes lead to increased distrust, uncertainty, and privacy concerns in the digital environment (Herbert et al., 2023). In this context, the interaction between individuals' levels of dependence on AI and their perceptions of digital privacy is an important issue that needs to be investigated.

AI dependency is defined by symptoms such as a constant desire for access to these technologies, developing excessive trust in AI, and an increase in the use of AI in everyday decision-making processes (Morales-García et al., 2024). Such dependency can create a situation that conflicts with individuals' privacy expectations, as high AI usage may imply the sharing of more personal data and potential exposure to privacy violations (Elliott & Soifer, 2022). On the other hand, some individuals refrain from using AI technologies and resist them at the expense of protecting their privacy.

This study aims to explain how university students' individual perceptions of privacy are related to their attitudes toward AI and their levels of AI dependency. Considering that today's young individuals are among the groups that adapt most quickly to digitalization and are also most exposed to privacy violations, explaining this relationship will fill an important gap in both theoretical and practical terms. Furthermore, this study aims to provide important insights into how the digital age

has created an ethical and psychological transformation at the individual level.

Conceptual Framework

The Evolution of Digital Privacy Concerns

Online privacy concern (OPC) refers to the level of perception that individuals have regarding the risk of their personal data being accessed without authorization or misused (Buchanan et al., 2007). With the rapid spread of AI applications in recent years, OPC has become a multidimensional and dynamic problem area that needs to be managed in digital life. Therefore, establishing a sustainable environment of trust in the online ecosystem requires the redesign of privacy protection strategies based on comprehensive, proactive, and ethical principles.

One of the most critical threats emerging in the field of privacy with the development of AI is the processing of biometric data without the user's consent. In particular, face analysis-based models do not merely verify identity; they can also predict a person's age, gender, and even their potential political and religious affiliations (Kosinski et al., 2024). This predictive capacity increases the risk of "biometric privacy violations" that individuals cannot control and extends the scope of the GDPR beyond traditional data breaches. Therefore, privacy protection strategies must be supported by technical and legal multi-layered measures that clearly define the ethical boundaries of advanced AI applications such as facial recognition systems.

When examining the reflections of privacy concerns in different contexts, the education ecosystem presents notable results. Generative AI-supported exam monitoring tools, while aiming to reduce cheating behavior, create a sense of constant surveillance over students, thereby strengthening the perception of privacy violations and weakening the intention to use the platform (Nigam et al., 2021). This situation demonstrates the need for educational institutions to re-examine the balance between security and privacy. On the other hand, a recent systematic review examining the measurement literature reveals significant gaps in privacy research conducted on emerging technologies such as IoT, AI, augmented reality, and big data. The

study reveals that contextual variables such as data sensitivity, recipient transparency, and transmission principles play critical roles in shaping privacy concerns and related behaviors, yet are often overlooked in most research. Additionally, it emphasizes that theoretical models developed based on traditional technologies are insufficient in explaining the multi-layered structure of modern digital environments. These findings, which comprehensively address psychological precursors, behavioral outcomes, and conceptual frameworks, necessitate the redesign of privacy research in the AI era with context-sensitive and interdisciplinary approaches (Herriger et al., 2025).

Attitudes Towards Artificial Intelligence

Attitudes toward AI encompass individuals' general beliefs about the extent to which they find this technology useful, reliable, and ethical. The four-item AI Attitude Scale (AIAS-4) developed by Grassini (2023) has been found to significantly predict AI usage intentions. Ibrahim et al. (2025) also validated the Extended Technology Acceptance Model (TAM-X) in the context of AI applications in their empirical study, reporting that perceived usefulness has an effect on attitude with a β value of 0.34. In addition to these findings, the literature shows that the "AI mindset" (growth/fixed tendency) variable is also a strong determinant of attitude (Yadrovskaya et al., 2023). Therefore, a positive attitude not only increases usage intention but also usage frequency and depth, which may trigger dependency or excessive usage risks.

Adaptation studies emphasize that AI attitude scales maintain cross-cultural equivalence of meaning, but adding ethical concerns and perceived fairness dimensions to the scales increases their explanatory power (Satici et al., 2025). Indeed, recent meta-analyses report that positive AI attitudes lead to increased productivity, trust in decision-making processes, and reduced cognitive load, while negative attitudes lead to technology rejection, increased privacy concerns, and organizational resistance behaviors (Emon, 2024). Thus, both the mechanisms that encourage AI adoption are better understood, and the potential risks of de-

pendency and privacy violations can be anticipated at an early stage. Building on this evidence—showing that favorable AI attitudes foster more frequent and intensive use, which can in turn nurture dependence—we advance the following hypothesis:

H1. *AI Attitude is positively associated with AI Dependency among university students.*

Artificial Intelligence Dependency

AI dependency is defined as the partial or complete loss of self-control over decision-making as a result of an individual's excessive reliance on AI systems in cognitive and behavioral processes. To measure this concept, Morales-García et al. (2024) consists of four subscales (loss of control, compulsive use, avoidance, and negative consequences). The results of the confirmatory factor analysis in the Turkish adaptation report AVE = 0.61 and CR = 0.87 (Savaş, 2024). These findings indicate that the scale maintains its validity and reliability, demonstrating that AI dependency can be measured consistently across cultural contexts.

Recent studies focusing on the cognitive effects of dependency have shown that intensive use of AI-based learning aids increases information processing load, which in turn reinforces perceptions of online privacy violations (Menard & Bott, 2025; Shrestha et al., 2024). High cognitive load directs users toward algorithms that offer faster and easier decisions; however, the scope of personal data sharing is often overlooked in this process. Therefore, dependency not only creates negative effects on psychological well-being but also undermines the sense of privacy by increasing privacy risks.

Recent years have witnessed a rapid accumulation of empirical evidence centered on the phenomenon of AI dependency. A systematic review by Zhai, Wibowo, and Li (2024) shows that the intensive use of generative language models in educational settings deepens dependency by creating a "cognitive shortcut" effect on decision-making, critical thinking, and analytical reasoning. Likewise, Zhang et al. (2024), in a multivariate analysis of ChatGPT users, found that academic self-efficacy and academic stress indirectly foster AI-de-

dependency behavior and documented consequences such as reduced creativity, misinformation diffusion, and weakened critical thinking. Focusing on the adverse impact of dependency on decision quality, Vasconcelos et al. (2023) experimentally demonstrated that properly designed explanatory interfaces can curb users' tendency to over-rely on erroneous AI advice. From a socio-emotional perspective, a qualitative study by Baylor et al. (2025) revealed that long-term interactions with AI companions such as Replica establish parasocial bonds, producing a "relationship-based dependency" that undermines user autonomy. Collectively, these findings underscore that AI dependency is a multilayered phenomenon encompassing cognitive, emotional, and social dimensions, thereby enriching the theoretical framework of the present study.

On the other hand, the perception of autopilot emerging in the context of decision support demonstrates that dependency can also have serious consequences at the organizational level. Users who are constantly fed AI feedback increase their decision confidence in the short term; however, in the long term, they experience cognitive passivity and weaken their critical inquiry skills (Fossa, 2025). This situation can lead to a decline in individual autonomy and algorithmic singularity in corporate decision-making processes. In conclusion, AI dependency creates a dual-sided pressure on both psychological well-being and privacy perception; therefore, developing awareness training to reduce dependency risks, responsible AI design principles, and regulatory guidelines is becoming increasingly important. Building on the empirical evidence reviewed above—showing that excessive reliance on AI systems heightens cognitive load, lowers critical thinking, and ultimately amplifies users' sense of vulnerability—we articulate three further hypotheses that anchor the remainder of the research model:

H2. *AI Dependency is positively associated with Online Privacy Concern among university students.* (Menard & Bott, 2025; Shrestha et al., 2024)

H3. *AI Attitude exhibits a statistically significant total effect on Online Privacy Concern.*

This expectation reflects mixed findings in the literature: while favorable attitudes may increase

exposure—and thus perceived risk—negative attitudes have been linked to heightened privacy worry (Emon, 2024; Herriger et al., 2025).

H4. *Net of the indirect pathway through AI Dependency, AI Attitude exerts a residual direct negative effect on Online Privacy Concern.*

In other words, once the mediating role of dependency is partialled out, a positive attitude toward AI is expected to reduce privacy concern by lowering risk salience (Ibrahim et al., 2025; Vasconcelos et al., 2023).

These hypotheses complement H1 by clarifying both the downstream impact of dependency on privacy concerns (H2) and the overall versus direct pathways linking AI attitude to those concerns (H3–H4).

The Moderating Role of Gender

In online environments, women generally exhibit higher privacy sensitivity and risk awareness compared to men (Fogel & Nehmad, 2009). Meta-analytic findings indicate that women have significantly higher levels of concern regarding the unauthorized use of their personal data (Tifferet, 2019). In contrast, the mitigating effect of positive technology attitudes on privacy concerns may follow a steeper slope among women due to the "trust–vulnerability paradox" (Hoy & Milne, 2010).

Gender differences have also become apparent in the context of AI dependency. These findings suggest that the gendered privacy calculus approach (cultural socialization and cognitive frameworks differentiating data sharing decisions) may also be valid in the AI ecosystem. Therefore, it is predicted that gender may significantly influence (i) the direct path from AI Attitude to Privacy Concerns, (ii) the intensity of the path from AI Dependency to Privacy Concerns, and (iii) the regulated (gender-dependent) mediation mechanism operating through these two paths. Based on these reasons, hypotheses H5–H7 have been developed.

H5. *Gender moderates the relationship between AI Dependency and Online Privacy Concern.*

H6. *Gender moderates the direct relationship between AI Attitude and Online Privacy Concern.*

H7. *Gender moderates the indirect effect of AI Attitude on Online Privacy Concern via AI Dependency (index of moderated mediation).*

Theoretical Approaches and Inter-Variable Dynamics

Technology Acceptance Model (TAM): The perceived benefit → attitude → usage intention chain remains valid in the AI context (Zhang, Hu & Zhou, 2025).

Socio-Technical Systems Theory: AI is evaluated as an “entangled” structure where technical components and social values are intertwined; this links social outcomes such as privacy concerns to technical design (Degeling, 2016).

Privacy Calculus: Users decide whether to share data by weighing perceived benefits and risks; AI dependency can skew this balance in favor of benefits, delaying risk perception (Rohden & Zeferino, 2023; Said et al., 2023).

Explainable AI (XAI): Providing explanations enhances system trust; however, detailed explanations may create unexpected risk awareness among users (Golda et al., 2024; Hyra & Premti, 2024).

This theoretical framework provides a comprehensive framework for explaining how the triad of AI attitude, dependency, and privacy concerns interact.

Research Model and Hypothesis Development

The conceptual framework addressed in this study is presented in Figure 1. The model assumes that attitudes toward AI (X) first influence AI dependency (M) and then online privacy concerns (Y). Furthermore, it is predicted that gender (W) conditions these relationships through both direct and indirect pathways.

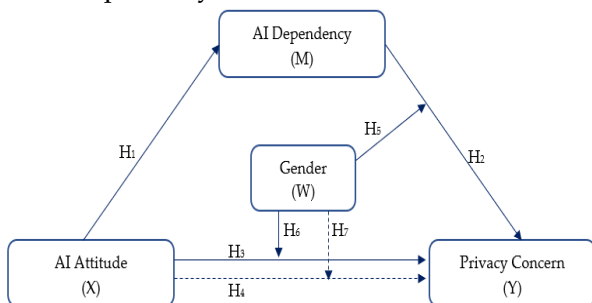


Figure 1. Research Model

When examining Figure 1, a positive relationship in the direction of X→M is tested under the

H1 hypothesis. H2 reveals the effect of M on Y, while H3 and H4 evaluate the total and direct effects of X on Y by assessing the mediation mechanism. Hypotheses H5, H6, and H7 reveal the moderating role of gender (W) on both indirect (M→Y) and direct (X→Y) pathways, thereby explaining the gender-differentiated dynamics of privacy concerns within the model.

The research hypotheses formulated in line with the conceptual model summarized in Figure 1, their theoretical background, and the expected relationship directions are presented in detail in Table 1.

Table 1. Hypotheses related to the research model

Hypothesis	Path	Theoretical Background	Expected relationship
H1	$X \rightarrow M$	Zhang vd., 2025	Positive
H2	$M \rightarrow Y$	Shrestha vd., 2024	Positive
H3	$X \rightarrow Y (c')$	Nigam vd., 2021	Empirically oriented
H4	$X \rightarrow M \rightarrow Y$	Fossa, 2025; Degeling, 2016	Indirect effect
H5	$W \times M \rightarrow Y$	Fogel & Nehmad, 2009; Tifferet, 2019	-
H6	$W \times X \rightarrow Y$	Hoy & Milne, 2010	-
H7	$W(\text{mediation})$	Barnes & Pressey, 2012	-

The hypotheses listed in Table 1 are tested through quantitative analyses described in the following section; thus, the holistic interaction between AI attitude, dependency, and privacy concerns is validated through structural equation modeling.

Method

Research Objective and Ethics

This study is conducted using a quantitative approach and a cross-sectional survey design. The research model aims to examine the direct and indirect relationships between the variables Artificial Intelligence Attitude (AIA) → Artificial Intelligence Dependency (AID) → Privacy Concerns (PC) through structural equation modeling (SEM).

Existing work rarely integrates AI attitude, AI dependency, and online privacy concern within a single, gender-contingent mediation model, and almost none of that evidence derives from emerging-economy contexts. By empirically testing this moderated-mediation framework among Turkish

university students, the present study fills both gaps and advances the privacy-calculus and socio-technical literatures with cross-cultural, gender-sensitive insights.

The research has been approved by the Ethics Committee of the Faculty of Social and Human Sciences at Uşak University under decision number 2025-151. Participants were informed about the purpose of the study, privacy guarantees, and voluntary participation conditions; those who selected the “I have read, understood, and agree” option in the online form proceeded to the survey. All data are anonymized in accordance with the principles of the General Data Protection Regulation (GDPR) and stored in a manner accessible only to the research team.

Data Collection Process

The study population consists of undergraduate students enrolled at state universities in Türkiye. The sample is selected using convenience sampling and accessed through a mixed online-face-to-face distribution strategy.

- **Target sample size:** At least $N = 400$. (Kline, 2013; 10:1 observation–parameter ratio; sufficient for 80% power and medium effect size for mediation testing.)
- **Inclusion criteria:** (i) Being between 18 and 30 years old, (ii) Having used AI-based tools at least once, (iii) Agreeing to participate in the research voluntarily.
- **Demographic variables:** Gender, age, class level, and perceived technological competence in the department are recorded as control variables.

Research data are collected through a cross-sectional and quantitative survey from undergraduate students aged 18–30 enrolled at state universities in Türkiye. The survey form first presents an informed consent statement to obtain participant approval; it then includes a psychometric section consisting of a total of 23 items structured using a five-point Likert scale. This section measures AI Attitude using the four-item AI Attitude Scale (AIAS-4) (Grassini, 2023; Satici et al., 2025), AI Dependency using the five-item Dependence on AI Scale (DAI-5) (Morales-García et al., 2024; Savaş, 2024) and Privacy Concerns are measured using

the 14-item Online Privacy Concern Scale (OPC-14) (Buchanan et al., 2007; Alakurt, 2017). The demographic section includes gender (Female/Male), age (open-ended), education level (High School, Associate Degree, Bachelor's Degree, Postgraduate), average daily internet usage (hours), owned technological devices (multiple choice: Desktop computer, Laptop, Tablet, Smartphone, other) and self-assessed technology knowledge (Low, Medium, High) are included; these variables are used as control variables in the structural model.

Data are collected during the spring semester of 2025. Participants are provided with an information letter and an informed consent form; students who give their consent are directed to the survey. Participants who access the online form complete all scales in a single session; in face-to-face applications, the paper-and-pencil method is used under the supervision of the research team. The average completion time is measured as 4–5 minutes.

Data Analysis

After the data set was transferred to SPSS 25 and AMOS 24, basic assumption checks were performed. Missing values are imputed using the “expectation–maximization” or mean imputation method as long as the proportion of missing values does not exceed 5% of the total observations; for higher missing value rates, multiple imputation techniques are recommended (Little & Rubin, 2019; Byrne, 2013). In this study, missing values were excluded from the analysis to avoid any bias in the data. Univariate normality skewness-kurtosis z values are assessed with the condition $|z| < 3$, while multicollinearity is assessed with the threshold $VIF < 5$ (Hair, Black, Babin, & Anderson, 2020). The internal consistency of the scales is considered acceptable with Cronbach's α values of .70 and above (Nunnally & Bernstein, 1994); composite reliability (CR) is also supported by the same .70 threshold. Based on confirmatory factor analysis, model fit is considered acceptable if the following criteria are met: $\chi^2/df < 3$, CFI-TLI $\geq .90$ (preferably $\geq .95$), and RMSEA $\leq .08$ (preferably $\leq .06$) (Hu & Bentler, 1999). Convergent validity is tested using the criterion of AVE $\geq .50$ criterion, while discriminant validity is tested by ensuring that the root

AVE values in the Fornell-Larcker matrix are greater than the related factor correlations (Fornell & Larcker, 1981); keeping the HTMT ratio below .85 also provides additional assurance (Henseler, Ringle, & Sarstedt, 2015). To assess the risk of common method variance, it is sufficient for the total variance to remain below 50% in Harman's single-factor test (Podsakoff, MacKenzie, & Podsakoff, 2012).

Following the validation of the measurement model, a structural equation model is constructed, and research hypotheses are estimated using the maximum likelihood method. The significance of standardized coefficients for the paths of AI Attitude on AI Dependency, Dependency on Privacy Concerns, and Attitude directly on Privacy Concerns are evaluated; Values of 0.10 or below are considered weak effects, values between 0.30 and 0.50 are considered moderate effects, and values above 0.50 are considered strong effects (Cohen, 1988). The mediating relationship is examined using a bias-corrected bootstrap method with 5,000 samples; an indirect effect is considered significant when the 95% confidence interval does not include zero (Preacher & Hayes, 2008). Gender, age, education level, internet usage duration, device ownership, and self-reported technology knowledge variables are included in the model as covariates; if measurement invariance is required, sequential constraints are tested in the multi-group analysis using the criterion $\Delta CFI \leq .010$ (Cheung & Rensvold, 2002).

Results

Of the total 478 students who participated in the study, 57.1% (n = 273) were female and 42.9% (n = 205) were male. The ages ranged from 18 to 28, with the majority of participants, 67.8% (n = 324), falling within the 21–24 age group. The educational level distribution was as follows: high school (5.2%, n = 25), associate degree (23.8%, n = 114), bachelor's degree (54.6%, n = 261), and graduate degree (16.3%, n = 78).

The daily internet usage time ranges from 1 to 10 hours, with an average of $M = 5.13$ hours ($SD = 2.02$). According to participants' self-assessments, the level of technology knowledge is reported as

“low” by 19.2% (n = 92), ‘moderate’ by 50.4% (n = 241), and “high” by 30.3% (n = 145).

Table 2. Reliability Values

	n	Cronbach' α	AVE	CR
Privacy Concerns	14	0.913	0.506	0.935
AI Attitude Scale (AIAS-4)	4	0.773	0.511	0.807
AI Dependency	5	0.795	0.525	0.846
Total	23	0.866		

The measurement quality of the three scales used in the data collection process was examined in detail, and the findings are presented in Table 2. The internal consistency coefficients (Cronbach α) obtained from the scales were above .70, and the composite reliability values were above .80, indicating that all three scales have acceptable levels of reliability (Nunnally & Bernstein, 1994). The average variance explained (AVE), which is a criterion for convergent validity, exceeded the threshold value of .50 in all dimensions; standardized factor loadings ranged from .60 to .78, indicating that the measurements adequately represent the target structures (Hair et al., 2020). Furthermore, Harman's one-factor test results, conducted to examine whether all item responses could be grouped under a single factor, showed that the first factor explained only 27.93% of the total variance; this ratio is well below the recommended 50% threshold, indicating that common method variance (CMV) does not pose a critical threat (Podsakoff et al., 2012).

When examining the fit statistics obtained at the end of the confirmatory factor analysis, the model's chi-square value was found to be low enough to be generalized to the population, $\chi^2(227) = 229.43$, $p = .442$; thus, the χ^2/df ratio is 1.01 and well within the recommended < 3 threshold (Hu & Bentler, 1999). Other absolute and incremental fit indices are also within acceptable limits: GFI = .960, AGFI = .951, IFI = .999, TLI = .999, and CFI = .999. The Root Mean Square Error of Approximation (RMSEA) is .005, which falls within the 90% confidence interval [.000, .020], and the PCLOSE value of 1.000 supports the likelihood of the model having excellent fit; the model's RMR value is also .033, which is below .08 (Hair et al., 2020). Additionally, parsimony-based measures were reported as PNFI = .848 and PCFI = .897; AIC = 327.43 and ECVI = .686

values indicate that the model exhibits a more economical fit compared to a saturated model. Hoelter's critical sample size of 548 at the .05 level and 582 at the .01 level indicates that the current sample (N = 478) is sufficient for structural model estimations.

This combination meets all recommended thresholds (CFI/TLI \geq .95, RMSEA \leq .06, $\chi^2/df \leq 3$), indicating that the measurement model is highly consistent with the data. Thus, the AI Attitude, AI Dependency, and Online Privacy Concerns scales are reliable and valid in the research sample, providing a solid foundation for testing the hypotheses in the structural model. When attitude and gender are included, the explained variance in the AI dependency equation is $R^2 = .24$; the Y equation in the full model is $R^2 = .28$, with the interaction terms created with gender explaining 1.4% of the additional variance ($\Delta R^2 = .006 + .008$).

The multilevel results examining the relationship between AI Attitude (X) and Online Privacy Concerns (Y) through AI Dependency (M) and moderated by Gender (W) using the Hayes Process Model 59 are summarized in Table 3.

Table 3. Mediation and Moderation Analysis results

Section	Effect	b	SE	t	p	LLCI	ULCI
Path coefficients	$X \rightarrow Y$	0.504	0.116	4.360	< .001	0.277	0.732
Path coefficients	$M \rightarrow Y$	0.770	0.125	6.150	< .001	0.524	1016.0
Path coefficients	$X \rightarrow Y (c')$	-0.623	0.120	-5.200	< .001	-0.858	-0.388
Path coefficients	$M \times W \rightarrow Y$	-0.198	0.086	-2.320	0.021	-0.367	-0.030
Conditional direct effects (c')	W(1)	-0.475	0.053	-9.000	< .001	-0.579	-0.371
Conditional direct effects (c')	W(2)	-0.327	0.057	-5.770	< .001	-0.438	-0.215
Conditional indirect effects	W(1) (boot)	0.270	0.040			0.195	0.350
Conditional indirect effects	W(2) (boot)	0.165	0.034			0.102	0.236
Moderated mediation index	W(1) – W(2) (boot)	-0.106	0.051			-0.206	-0.006

Table 4. Summary of hypothesis testing results

Hypothesis	Path	Effect B (SE)	t/z	p	95 % CI	Support
H1	$X \rightarrow M$	0.504 (0.116)	4.36	<0.001	0.28, 0.73	Supported
H2	$M \rightarrow Y$	0.770 (0.125)	6.15	<0.001	0.52, 1.02	Supported
H3	$X \rightarrow Y (c')$	-0.623 (0.120)	-5.20	<0.001	-0.86, -0.39	Supported
H4	$X \rightarrow M \rightarrow Y$	–	–	–	–	Supported
H5	$W \times M \rightarrow Y$	-0.198 (0.086)	-2.32	.021	-0.37, -0.03	Supported
H6	$W \times X \rightarrow Y$	0.148 (0.077)	1.92	.056	-0.00, 0.30	Not Supported
H7	W(mediation)	–	–	–	-0.206, -0.006	Supported

AI Attitude (X) significantly predicts AI dependency (M), $b = .50$, $SE = .12$, $t = 4.36$, $p < .001$, 95% CI [.28, .73]; dependency also positively and strongly increases privacy concerns (Y), $b = .77$, $SE = .13$, $t = 6.15$, $p < .001$, 95% CI [.52, 1.02]. The direct

effect of attitude on anxiety is negative ($b = -.62$, $SE = .12$, $t = -5.20$, $p < .001$), indicating that while a positive attitude indirectly increases anxiety through dependency, it directly reduces anxiety.

The gender variable (W) plays a significant moderating role in these relationships. The direct effect is more pronounced in women ($b = -.48$, $p < .001$) and the indirect effect is also larger (boot = .27, 95% CI [.20, .35]); the corresponding values for men are $b = -.33$ and boot = .17. The moderation-dependent mediation index is significant ($-.11$, 95% CI $[-.21, -.01]$), indicating that the strength of the attitude \rightarrow dependency \rightarrow anxiety pathway is higher in women than in men. In other words, female students with positive AI attitudes are more exposed to AI dependency and then privacy anxiety than males; however, the direct effect of positive attitudes in reducing anxiety is also stronger in females. These results reveal that AI applications are perceived differently in a gender context and that gender-sensitive strategies should be developed in interventions. The results related to the hypotheses are summarized in Table 4.

Discussion

The findings of this study show that individuals' perceptions of privacy in the digital age are intricately intertwined with their attitudes toward AI

and dependency dynamics. First, it was found that positive AI attitudes significantly increased AI dependency ($\beta = .50$) and, consequently, increased privacy concerns ($\beta = .77$). This result is consistent with recent studies suggesting that positive attitudes open the door to more intensive AI use and, over time, trigger a sense of “loss of control,” paralleling the TAM-X “perceived benefit \rightarrow usage tendency” chain (Ibrahim et al., 2025). Additionally, the direct negative effect of attitude on privacy concerns ($\beta = -.62$) is noteworthy; this inverse relationship suggests that individuals with positive attitudes initially suppress their risk perceptions because they perceive AI as more reliable, but increasing dependency weakens this “trust shield.” A similar two-way pattern intersects with discussions of the “comfort–risk paradox” observed in generative AI-based exam monitoring systems (Nigam et al., 2021). Recent large-scale investigations further corroborate this trajectory: systematic reviews and multivariate studies have shown that intensive reliance on generative AI produces “cognitive offloading” effects that erode critical-thinking and analytical-reasoning capacities, thereby amplifying privacy-related vulnerabilities (Zhai et al., 2024; Zhang et al., 2024; Shrestha et al., 2024; Menard & Bott, 2025).

Second, the significant indirect role of gender adds a new dimension to the gender differences increasingly emphasized in the literature. The findings indicate that female participants exhibit higher sensitivity to AI dependency-related risk perceptions compared to males, yet the direct mitigating effect of positive attitudes on privacy concerns is stronger among women. This “dual effect” is consistent with recent experimental data indicating that fears of biometric privacy violations are more pronounced among women (Kosinski et al., 2024) and supports theories of how “protection motivation” differs by gender in digital environments. Consistent with this pattern, Kosinski, Khambatta, and Wang (2024) illustrate that female users display heightened sensitivity to biometric privacy risks, while meta-analytic evidence indicates that women’s stronger privacy concerns can temper otherwise positive technology attitudes (Tifferet, 2019; Herriger et al., 2025), thus reinforcing the gendered “trust–vulnerability paradox.”

Furthermore, when considered alongside findings emphasizing that AI dependency undermines cognitive autonomy through the “decision support paradox” (Fossa, 2025), it becomes clear that privacy concerns are not merely about the fear of data leaks but are also shaped by risks of cognitive and behavioral dependency.

Extending beyond individual differences, design choices also shape dependency-driven privacy threats: socio-technical work emphasizes that omitting transparency and equity safeguards can magnify such risks (Degeling et al., 2016), whereas explanatory interfaces have been shown to mitigate over-reliance on algorithmic outputs (Vasconcelos et al., 2023). Embedding deliberate “friction” and clear data-use disclosures in AI interfaces may therefore serve as a practical antidote to autonomy erosion.

Finally, these results offer important contributions to both theory and practice. On the theoretical level, the study’s model integrates the “privacy calculus” and socio-technical systems literature by revealing the indirect–direct opposing effects of AI attitudes on privacy concerns (Rohden & Zeferino, 2023; Said et al., 2023). In practice, AI-based service designers must strengthen personal data transparency and dependency-preventing feedback mechanisms, particularly for female users. Educational institutions and platform providers can reduce dependency-related risks while preserving the beneficial aspects of positive attitudes by incorporating privacy awareness modules into AI literacy programs. Future research could use longitudinal designs to examine the evolution of dependency over time and the mediating–regulatory roles of gender in different cultural contexts; it should also explore the potential balancing effects of explainable AI solutions on these dynamics.

Conclusion

This study reveals how individuals’ perceptions of privacy in the digital age are shaped by their attitudes toward and dependence on AI from a multi-dimensional perspective. The findings reveal that positive attitudes toward AI increase users’ dependence on AI systems in their decision-making processes; this dependence, in turn, significantly

elevates online privacy concerns. At the same time, the direct effect of attitude on privacy concerns is negative, indicating that individuals who find technology useful initially suppress their risk perception; however, increasing levels of dependence render this suppression unsustainable. The gender variable's moderating effect on the indirect impact reveals that female users are positioned at more extreme levels in terms of both benefit expectations and risk sensitivity, contributing significantly to the limited literature on the gender dimension.

Theoretically, the study integrates technology acceptance theory, the socio-technical systems approach, and the privacy calculus framework to position AI dependency as an explanatory mechanism. This comprehensive model emphasizes that the dependency variable should not be overlooked in future AI-focused behavioral research. In practice, designers and policymakers are recommended to strengthen transparent data flow and dependency-preventing feedback mechanisms in AI-based services, especially for female users.

Due to its cross-sectional design, the study has limitations regarding causality; furthermore, as the sample consists only of university students, the findings cannot be directly generalized to a wider population. Future studies are recommended to track the evolution of dependency over time using longitudinal data sets, examine the role of gender in different cultural contexts, and investigate the balancing effects of explainable AI interventions on these dynamics. In conclusion, this study sheds light on the interaction between AI attitudes and dependency from a gender perspective, thereby guiding both theory and practical applications in the digital privacy literature.

Declarations

Funding: *No funding was received for conducting this study.*

Conflicts of Interest: *The author declares no conflict of interest.*

Ethical Approval: *This research was approved by the Ethics Committee of the Faculty of Social and Human Sciences at Uşak University (Decision No: 2025-151).*

Informed Consent: *Informed consent was obtained from all participants before they took part in the study.*

Data Availability: *The datasets generated and analyzed during the current study are available from the corresponding author on reasonable request.*

AI Disclosure: *No artificial intelligence-based tools or applications were used in the preparation of this study. All content of the study was produced by the author in accordance with scientific research methods and academic ethical principles.*

References

- Alakurt, T. (2017). Çevrimiçi mahremiyet kaygısı ölçeğinin Türk kültürüne uyarlanması. *Pegem Eğitim ve Öğretim Dergisi*, 7(4), 611-636.
- Barnes, S. J., & Pressey, A. D. (2012). In search of the "privacy paradox": Privacy concerns and willingness to disclose in online social networks. *Journal of Business Research*, 66(9), 1528-1535. <https://doi.org/10.1016/j.jbusres.2012.02.015>
- Bayor, L., Weinert, C., Maier, C., & Weitzel, T. (2025). Social-oriented communication with AI companions: Benefits, costs, and contextual patterns. *Business & Information Systems Engineering*, 67(4), 1-19. <https://doi.org/10.1007/s12599-025-00955-1>
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165. <https://doi.org/10.1002/asi.20459>
- Byrne, B. M. (2013). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (1st ed.). New York, NY: Routledge. <https://doi.org/10.4324/9780203807644>
- Cheung, G. W., & Rensvold, R. B. (2002). Evaluating goodness-of-fit indexes for testing measurement invariance. *Structural Equation Modeling*, 9(2), 233-255. http://doi.org/10.1207/S15328007SEM0902_5

- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum.
- Degeling, M., Lentzsch, C., Nolte, A., Herrmann, T., & Loser, K. U. (2016, November). Privacy by socio-technical design: A collaborative approach for privacy friendly system design. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)* (pp. 502-505). IEEE. <https://doi.org/10.1109/CIC.2016.077>
- Elliott, D., & Soifer, E. (2022). AI technologies, privacy, and security. *Frontiers in Artificial Intelligence*, 5, 826737. <https://doi.org/10.3389/frai.2022.826737>
- Emon, M. M. H., Khan, T., Rahman, M. A., & Siam, S. A. J. (2024, September). Factors influencing the usage of artificial intelligence among Bangladeshi professionals: Mediating role of attitude towards the technology. In *2024 IEEE International Conference on Computing, Applications and Systems (COMPAS)* (pp. 1-7). IEEE. <https://doi.org/10.1109/COMPAS60761.2024.10796110>
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160. <http://dx.doi.org/10.1016/j.chb.2008.08.006>
- Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50. <https://doi.org/10.1177/002224378101800104>
- Fossa, F. (2025). Artificial intelligence and human autonomy: the case of driving automation. *AI & Soc*, 40, 1851–1862. <https://doi.org/10.1007/s00146-024-01955-7>
- Golda, A., Mekonen, K., Pandey, A., Singh, A., Hassija, V., Chamola, V., & Sikdar, B. (2024). Privacy and security concerns in generative AI: a comprehensive survey. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2024.3381611>
- Grassini, S. (2023). Development and validation of the AI attitude scale (AIAS-4): a brief measure of general attitude toward artificial intelligence. *Frontiers in psychology*, 14, 1191628. <https://doi.org/10.3389/fpsyg.2023.1191628>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2020). *Multivariate data analysis* (9th ed.). Harlow, England: Pearson.
- Henseler, J., Ringle, C. M., & 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. <http://doi.org/10.1007/s11747-014-0403-8>
- Herbert, F., Becker, S., Schaewitz, L., Hielscher, J., Kowalewski, M., Sasse, A., ... & Dürmuth, M. (2023, April). A world full of privacy and security (mis) conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1-23). <https://doi.org/10.1145/3544548.358141>
- 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. <https://doi.org/10.2196/71951>
- Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of interactive advertising*, 10(2), 28-45. <https://doi.org/10.1080/15252019.2010.10722168>
- Hu, L.T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, 6(1), 1–55. <http://doi.org/10.1080/10705519909540118>
- Hyra, A., & Premti, F. (2024). The Double-Edged Sword of AI in Cybersecurity: Boosting Security While Addressing Privacy Risks. *Smart Cities and Regional Development (SCRD) Preprints*, 1(1).
- Ibrahim, F., Münscher, J. C., Daseking, M., & Telle, N. T. (2025). The technology acceptance model and adopter type analysis in the context of artificial intelligence. *Frontiers in*

- Artificial Intelligence*, 7, 1496518. <https://doi.org/10.3389/frai.2024.1496518>
- Kline, R. (2013). Exploratory and confirmatory factor analysis. In *Applied quantitative analysis in education and the social sciences*. 171-207. Routledge.
- Kosinski, M., Khambatta, P., & Wang, Y. (2024). Facial recognition technology and human raters can predict political orientation from images of expressionless faces even when controlling for demographics and self-presentation. *American Psychologist*, 79(7), 942-955. <https://doi.org/10.1037/amp-0001295>
- Li, X., & Zhang, T. (2017, April). An exploration on artificial intelligence application: From security, privacy and ethic perspective. In *2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 416-420). IEEE. <https://doi.org/10.1109/ICCCBDA.2017.7951949>
- Little, R. J. A., & Rubin, D. B. (2019). *Statistical analysis with missing data* (3rd ed.). Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781119482260>
- Maphosa, V. (2024). The rise of artificial intelligence and emerging ethical and social concerns. *AI, Computer Science and Robotics Technology*. <https://doi.org/10.5772/acrt.-20240020>
- Menard, P., & Bott, G. J. (2025). Artificial intelligence misuse and concern for information privacy: New construct validation and future directions. *Information Systems Journal*, 35(1), 322-367. <https://doi.org/10.1111/ijj.12544>
- Morales-García, W. C., Sairitupa-Sanchez, L. Z., Morales-García, S. B., & Morales-García, M. (2024, March). Development and validation of a scale for dependence on artificial intelligence in university students. In *Frontiers in Education* (Vol. 9, p. 1323898). Frontiers Media SA. <https://doi.org/10.3389/feduc.2024.1323898>
- Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and future. *Education and Information Technologies*, 26(5), 6421-6445. <https://doi.org/10.1007/s10639-021-10597-x>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York, NY: McGraw-Hill.
- Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63, 539-569. <http://doi.org/10.1146/annurev-psych-120710-100452>
- Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, 40(3), 879-891. <http://doi.org/10.3758/BRM.40.3.879>
- Rohden, S. F., & Zeferino, D. G. (2023). Recommendation agents: an analysis of consumers' risk perceptions toward artificial intelligence. *Electronic Commerce Research*, 23(4), 2035-2050. <https://doi.org/10.1007/s10660-022-09626-9>
- Said, N., Potinteu, A. E., Brich, I., Buder, J., Schumm, H., & Huff, M. (2023). An artificial intelligence perspective: How knowledge and confidence shape risk and benefit perception. *Computers in Human Behavior*, 149, 107855. <https://doi.org/10.1016/j.chb.2023.107855>
- Satici, S. A., Okur, S., Yilmaz, F. B., & Grassini, S. (2025). Psychometric properties and Turkish adaptation of the artificial intelligence attitude scale (AIAS-4): evidence for construct validity. *BMC Psychology*, 13(1), 1-14. <https://doi.org/10.1186/s40359-025-02505-6>
- Savaş, B. Ç. (2024). Yapay Zekâya Bağımlılık Ölçeğinin Türkçe'ye Uyarlanması: Geçerlik ve Güvenirlik Çalışması. *Herkes için Spor ve Rekreasyon Dergisi*, 6(3), 306-315. <https://doi.org/10.56639/jsar.1509301>
- Shrestha, A. K., Barthwal, A., Campbell, M., Shouli, A., Syed, S., Joshi, S., & Vassileva, J. (2024). Navigating AI to unpack youth privacy concerns: An in-depth exploration and systematic review. *arXiv preprint arXiv:2412.16369*. <https://doi.org/10.48550/arXiv.2412.16369>

- Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93, 1-12. <https://doi.org/10.1016/j.chb.2018.11.046>
- Vasconcelos, H., Jörke, M., Grunde-McLaughlin, M., Gerstenberg, T., Bernstein, M. S., & Krishna, R. (2023). Explanations can reduce over-reliance on AI systems during decision-making. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2), 1–38. <https://doi.org/10.1145/3579605>
- Yadrovskaya, M., Porksheyan, M., Petrova, A., Dudukalova, D., & Bulygin, Y. (2023). About the attitude towards artificial intelligence technologies. In *E3S Web of Conferences* (Vol. 376, p. 05025). EDP Sciences. <https://doi.org/10.1051/e3sconf/202337605025>
- Zhai, C., Wibowo, S., & Li, L. D. (2024). The effects of over-reliance on AI dialogue systems on students' cognitive abilities: A systematic review. *Smart Learning Environments*, 11(28), 1–24. <https://doi.org/10.1186/s40561-024-00316-7>
- Zhang, S., Zhao, X., Zhou, T., & Kim, J. H. (2024). Do you have AI dependency? The roles of academic self-efficacy, academic stress, and performance expectations on problematic AI usage behaviour. *International Journal of Educational Technology in Higher Education*, 21(34), 1–26. <https://doi.org/10.1186/s41239-024-00467-0>
- Zhang, X., Hu, J., & Zhou, Y. (2025). The role of perceived utility and ethical concerns in the adoption of AI-based data analysis tools: A multi-group structural equation model analysis among academic researchers. *Education and Information Technologies*, 1-33. <https://doi.org/10.1007/s10639-025-13535-3>