International Journal of Communication 20(2026), 148–171 1932–8036/20260005

The Dark Side of Algorithms: How Ethical and Privacy Considerations Affect Individuals' Engagement With Health Information on Social Media?

MENGXUE OU
Peking University, China

HAN ZHENG
BAIJUE LI
CHEN LUO
Wuhan University, China

Algorithm-driven social media platforms are increasingly designed to deliver personalized health content that caters to users' varied information needs. However, the opaque collection and use of personal data raise significant privacy concerns. Drawing on communication privacy management (CPM) theory, this study examines how users' ethical considerations of algorithm-driven social media shape their privacy-related perceptions and, in turn, influence their trust in and engagement with health information recommended by these platforms. An online survey of 1,051 users revealed that ethical considerations were positively associated with both social privacy concerns and perceptions of institutional privacy practices. Social privacy concerns negatively predicted trust and engagement with recommended health information, whereas perceptions of institutional privacy practices positively predicted trust, which subsequently enhanced engagement. Ethical considerations exhibited dual indirect effects on engagement: a negative pathway via social privacy concerns and trust and a positive pathway via perceptions of institutional privacy practices and trust. Theoretical and practical implications are discussed.

Keywords: engagement with health information, algorithm-driven social media, communication privacy management theory, ethical and privacy considerations

Algorithm-driven social media platforms, such as Facebook, TikTok, and Instagram, have transformed how health information is curated, prioritized, and disseminated, tailoring content to users' individual preferences and needs (Kotilainen et al., 2020; Zhang et al., 2017). While these platforms provide

Mengxue Ou: mengxueou@pku.edu.cn
Han Zheng (corresponding author): hanzheng@whu.edu.cn
Baijue Li: libaijue@whu.edu.cn
Chen Luo: chenluo@whu.edu.cn
Date submitted: 2025-08-29

Copyright © 2026 (Mengxue Ou, Han Zheng, Baijue Li, and Chen Luo). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at https://ijoc.org.

opportunities for personalized health communication, they also raise profound ethical and privacy concerns. The integration of machine learning allows algorithms to continuously learn from users' online behavior, including browsing habits and personal information shared on these platforms, yet often without transparent disclosure of how such data are collected, analyzed, or monetized (Jozani et al., 2020). Notably, research shows that more than 20% of mobile applications mislead users into consenting to unrestricted data sharing without proper authorization (Nguyen et al., 2022), suggesting the risks inherent in engaging with health content on algorithm-driven platforms. These challenges highlight the need for a critical examination of how algorithmic curation intersects with users' trust, privacy, and ethical engagement in the health communication domain.

While prior research has established that privacy concerns and ethical apprehensions surrounding social media use can discourage users from engaging with platform-recommended content (e.g., Bright et al., 2021; Majjate et al., 2025), most existing studies have approached these relationships at a general behavioral level rather than within specific informational domains. For instance, Cain and Imre (2022) demonstrated that a lack of transparency in how personal data are collected, accessed, and used on social media is associated with decreased engagement behaviors, such as liking, sharing, and commenting. Similarly, a recent meta-analysis (Ou et al., 2023) found that privacy concerns significantly contribute to social media fatigue and discontinuation of use. However, this body of work primarily treats engagement as a uniform outcome, overlooking how privacy concerns may operate differently across content types. In particular, little is known about how such concerns influence engagement with health information, a domain where algorithmic curation intersects with highly sensitive personal data. Given that health-related interactions on social media entail heightened risks of inadvertent disclosure of personal conditions or medical histories, understanding how users negotiate these privacy boundaries remains a crucial but underexplored question. Addressing this gap is essential for explaining the nuanced ways in which ethical and privacy considerations shape user behavior in algorithm-driven health communication environments.

Although prior studies have shown that ethical concerns (e.g., algorithmic transparency, fairness, and accountability) shape users' trust in algorithmically curated content on social media (e.g., Kim & Moon, 2021; Shin et al., 2022), existing research remains fragmented in explaining how these ethical considerations precede privacy concerns and subsequently influence engagement behaviors. Much of the literature treats ethical and privacy dimensions as parallel rather than interdependent constructs, overlooking the possibility that users' ethical evaluations of algorithms may trigger or intensify distinct types of privacy considerations (e.g., institutional vs. social). Moreover, the mechanisms through which these considerations translate into behavioral outcomes, particularly the mediating roles of privacy perceptions between ethical considerations and engagement with algorithmically recommended health information, remain theoretically underdeveloped and empirically untested. This gap is increasingly consequential as social media evolve into important sources of health information, where algorithmic curation intersects with sensitive personal data and the risk of inadvertent disclosure. Addressing these limitations requires an integrative framework that explains how ethical and privacy considerations jointly shape users' trust and engagement within algorithmic health communication contexts.

Informed by the communication privacy management theory (CPM; Petronio & Kovach, 2011), this study examines how ethical considerations about algorithm-driven social media shape users' privacy-

https://doi.org/10.65476/7tp42020

related perceptions (i.e., social privacy concerns and perceptions of institutional privacy practices) and how these perceptions, in turn, influence trust in and engagement with health information on such platforms. Extending this framework, we investigate the mediating roles of trust and privacy-related perceptions (both social and institutional) in the relationship between ethical considerations and user engagement (see Figure 1). To test these relationships, we conducted an online survey of 1,051 social media users in China. By applying CPM to the context of algorithm-driven health communication, this study extends the theory beyond its traditional focus on interpersonal exchanges to encompass human–algorithm interactions. In doing so, it advances our understanding of how ethical concerns about algorithmic systems heighten privacy-related perceptions and, ultimately, shape users' trust in and engagement with health content curated by algorithm-driven social media.

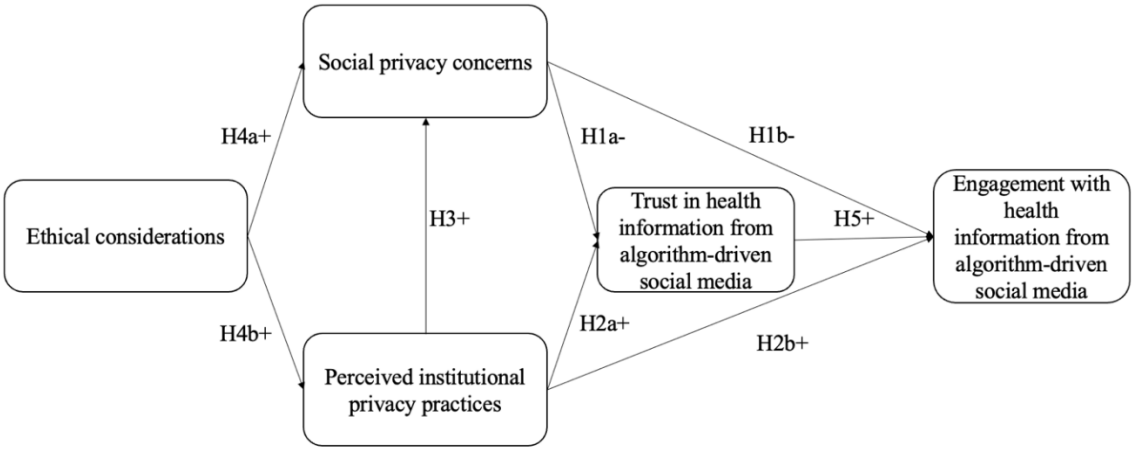

Figure 1. Proposed model.

Literature Review

Communication Privacy Management (CPM) Theory

Privacy is commonly defined as "an individual's ability to determine when, how, and to what extent personal information is disseminated to others" (Metzger, 2007, p. 336). It entails establishing and maintaining boundaries to regulate the flow of information between oneself and others (Altman, 1977). On algorithm-driven social media, privacy concerns typically arise from users' perceived lack of control and transparency about how their personal data are collected, processed, and shared. These concerns are amplified by algorithmic systems that continuously learn from users' browsing patterns, shared content, and interaction behaviors (Jozani et al., 2020). Yet despite these risks, the convenience of personalized information and tailored health content continues to attract users to these platforms. This paradox illustrates an ongoing negotiation in which individuals recalibrate their privacy boundaries, applying privacy management rules to balance the perceived risks of data disclosure against the benefits of algorithmically curated health information.

https://doi.org/10.65476/7tp42020

CPM theory (Petronio & Kovach, 1997) has emerged as one of the most influential frameworks for explaining how individuals navigate algorithm-powered platforms and decide whether to disclose or conceal personal information. CPM posits that individuals weigh the benefits of disclosure—for example, sharing interaction data to gain personalized health content—against the potential risks, such as data misuse or leakage. This decision-making process provides a systematic lens for understanding and predicting user engagement with algorithm-driven platforms, highlighting the delicate balance between the gratifications of algorithmic personalization and the privacy and ethical risks inherent in these systems.

Traditionally, CPM posits that privacy boundary management involves several key processes (Metzger, 2007). The first is boundary rule formation, which refers to the development of rules individuals use to decide when and under what circumstances to disclose or withhold information. These rules are typically shaped by personal factors (e.g., perceived risks and benefits), relational factors (e.g., seeking support or building relationships), and situational factors (e.g., social expectations; Petronio & Sargent, 2011). The second process, boundary coordination, involves negotiating privacy rules between individuals, such as determining whether disclosed information can be shared with others outside the relationship (Petronio & Sargent, 2011). In this stage, individuals establish rules governing boundary linkages (whether others may be included), boundary ownership (who has access rights to the information), and boundary permeability (what information can be shared and with whom). The third process, boundary turbulence, occurs when privacy rules are unclear, violated, or poorly coordinated—for instance, when one person shares information outside the relationship against another's expectations (Petronio & Kovach, 1997).

CPM has expanded beyond its origins in interpersonal communication (e.g., Petronio & Sargent, 2011; Wilson et al., 2021) to computer-mediated contexts, including algorithm-driven social media (De Wolf, 2016; Petronio & Kovach, 1997). In these settings, CPM explains how individuals balance privacy threats from recommendation systems with the gratifications of personalized content (Jozani et al., 2020). The framework has also been applied to human–AI interactions, such as autonomous driving and health technologies, where privacy concerns and boundary management shape trust and adoption (Craig, 2025; Meng, 2024; Schomakers et al., 2022). Prior research shows that social privacy concerns and perceived control over personal data jointly influence engagement with mobile health applications, with greater control mitigating the impact of privacy concerns (Zheng et al., 2024). Similarly, on algorithm-driven social media, users may hesitate to engage with recommended health content out of concern that their interactions are tracked, prompting boundary adjustments that ultimately affect engagement (Jozani et al., 2020).

Therefore, guided by CPM theory, we propose a model to examine how privacy-related perceptions of algorithm-driven social media (i.e., social privacy concerns and perceptions of institutional privacy practices) shape users' trust in and engagement with health content recommended on these platforms. We further investigate how ethical considerations of social media algorithms influence these privacy-related perceptions, which, in turn, affect trust and engagement.

Social Privacy Concerns

Social privacy concerns involve individuals' worries about the access, dissemination, and misuse of their personal information by others within their social network (Jozani et al., 2020, p. 3). These concerns

https://doi.org/10.65476/7tp42020

often manifest in various forms on social media, such as anxieties about identity theft, information leakage, hacking, and cyberstalking (Lutz & Ranzini, 2017). Studies have consistently shown that such concerns negatively impact individuals' trust in and engagement with social media platforms (Bansal et al., 2016; Brinson et al., 2024; Ozdemir et al., 2017; Rosenthal et al., 2020), often leading to the discontinuation of social media use. For example, Lutz and Ranzini (2017) found that perceptions of online privacy threats related to Internet-mediated sharing economies (e.g., home-sharing platforms like Airbnb) diminished users' perceived benefits and trust in the system.

Moreover, social privacy concerns are also associated with adverse user behaviors on algorithm-driven social media, such as discontinuing use, reducing engagement, and limiting interactions (e.g., Rosenthal et al., 2020; Trifiro, 2023). For instance, previous studies have found that privacy concerns about information disclosure on TikTok often lead influencers to protect their family members' privacy and affect the details they share online (Trifiro, 2023). Additionally, a recent study in Asia found that university students who realize the privacy risks associated with TikTok use tend to adopt strategies like selective content sharing and avoiding engagement with recommended content to mitigate these risks (Duong et al., 2024). Consequently, individuals concerned about safeguarding their privacy on algorithm-driven social media platforms are likely to exhibit lower levels of trust and engagement with these platforms, as well as reduced involvement with the health information they provide (Jozani et al., 2020; Nguyen et al., 2024). Based on these findings, we hypothesize:

H1: Users' social privacy concerns will be negatively associated with their (a) trust in and (b) engagement with health information on algorithm-driven social media platforms.

Perceived Institutional Privacy Practices

Perceptions of institutional privacy practices refer to users' awareness and understanding of how platforms manage personal data, including privacy policies, operational practices, and regulatory frameworks (Culnan & Bies, 1999; Foxman & Kilcoyne, 1993). This construct reflects the extent to which users believe institutions handle their personal information responsibly (Culnan & Bies, 1999; Foxman & Kilcoyne, 1993; Jozani et al., 2020). It encompasses users' knowledge of privacy policies, data collection methods, and protective measures adopted by platforms (Xu et al., 2011). When people navigate the trade-offs between the benefits and risks of engaging with health content curated by the algorithm-driven platforms, perceptions of institutions' privacy practices shape users' expectations of privacy protection, increasing their trust in and engagement with these platforms.

Previous research has shown that when individuals understand a platform's privacy policies, data-handling practices, and regulatory compliance, they are more likely to perceive the platform as transparent and responsible (Matei et al., 2017). Such transparency with data collection, storage, and sharing reassures users that their personal information is not being exploited, fostering trust in the platform (DiStaso & Bortree, 2012). Empirical evidence further suggests that effective institutional privacy assurances can reduce perceived privacy risks and enhance trust in a platform's services (Lutz & Tamo-Larrieux, 2020; Wells et al., 2011). In turn, trust in institutional privacy practices has been found to positively influence users' online interactions and engagement. Drawing on these insights, we argue that users with stronger

https://doi.org/10.65476/7tp42020

perceptions of institutional privacy practices will demonstrate greater trust in and engagement with health information on social media platforms. Accordingly, we hypothesize:

H2: Perceived institutional privacy practices implemented by algorithm-driven social media platforms will be positively associated with users' (a) trust and (b) engagement in the health information recommended by such platforms.

Social privacy concerns and perceptions of institutional privacy practices are closely intertwined, as both shape individuals' privacy judgments on algorithm-driven social media. Users who are more knowledgeable about how platforms collect, store, and use data, such as data-sharing practices, security measures, and institutional policies, tend to develop heightened perceptions of potential privacy risks. These perceptions often translate into stronger social privacy concerns, as individuals become more vigilant about the ways their personal information may be exposed or misused by algorithms and third parties (Mutimukwe et al., 2020; Smith et al., 1996).

From the perspective of CPM theory, this relationship can be explained through the notion of privacy boundaries. When individuals perceive that institutional actors have significant access to and control over their personal information, they assume that their privacy boundaries are vulnerable to intrusion. These perceptions activate greater concern about boundary permeability and potential turbulence, particularly when algorithms or external entities might exploit personal data beyond the individual's control (Petronio & Kovach, 1997). Empirical evidence supports this theoretical link: Studies show that users who perceive greater transparency in institutional privacy practices also tend to report stronger concerns about privacy risks, as heightened perceptions of data regulations make them more conscious of possible violations (Handa et al., 2024; Mutimukwe et al., 2020). In short, institutional privacy perceptions sharpen individuals' recognition of risks, which manifests as greater social privacy concerns. We posit:

H3: Users' perceptions of institutional privacy practices will be positively associated with their social privacy concerns over algorithm-driven social media platforms.

Ethical Considerations

We also examine how ethical considerations about algorithm-driven social media shape users' privacy-related perceptions, which, in turn, influence their trust and engagement with health content curated by these platforms. Ethical considerations in this context encompass users' concerns about whether algorithmic personalization is conducted fairly, transparently, and in ways that respect individual autonomy (Zarouali et al., 2021). Fairness refers to whether algorithmic processes treat users equitably without discrimination. Transparency pertains to the extent to which algorithmic decision making is understandable and accountable to users. Autonomy reflects whether algorithms respect individuals' ability to make independent choices, rather than subtly manipulating or constraining their decision-making power.

When users begin to question the fairness, transparency, or autonomy of algorithmic practices, they are more likely to anticipate risks such as data misuse, bias, or manipulative exposure of personal information. From the perspective of CPM theory, such concerns arise when individuals perceive that their

https://doi.org/10.65476/7tp42020

privacy boundaries are not respected by others—be it social contacts, unknown third parties, or the algorithms themselves (Petronio & Kovach, 1997). As a result, users develop stronger social privacy concerns, particularly about the potential loss of control over their data to peers, advertisers, or unintended audiences. Prior studies have shown that individuals with greater algorithmic or technological literacy, often reflected in heightened sensitivity to the ethical implications of algorithmic systems, tend to adopt privacy-protective strategies, such as limiting access to their browsing histories, interaction records, or personal identifiers (Craig, 2025; Meng, 2024). This suggests that users with stronger ethical considerations of algorithms are more predisposed to harbor elevated levels of social privacy concerns.

Ethical considerations also influence how users perceive institutional privacy practices. When individuals question the ethical integrity of algorithmic systems, they become more attentive to how platforms collect, store, and use personal data. In CPM terms, this reflects a form of boundary coordination, where users closely monitor institutional practices to safeguard their privacy. Research has shown that individuals who value ethical principles, such as fairness, transparency, and accountability, are more attuned to organizational privacy practices, including data collection, sharing, and security protocols (Koene et al., 2015). Accordingly, users with greater ethical considerations about algorithms are not only more vigilant about potential privacy risks but also more likely to be aware of and scrutinize institutional privacy policies and safeguards. Therefore, we propose:

H4: Users' ethical consideration about algorithm-driven social media will be positively associated with their (a) social privacy concerns and (b) perceptions of institutional privacy practices implemented by such platforms.

Association Between Trust and Engagement

Individuals' trust in health information disseminated via algorithm-driven social media platforms plays a pivotal role in shaping their engagement with such content, including actions such as forwarding, liking, and commenting on relevant posts (Guo et al., 2021; Wongkitrungrueng & Assarut, 2020). From the perspective of CPM, trust reduces perceptions of privacy boundary turbulence and legitimizes information-related behaviors, such as disclosure and sharing (Petronio & Kovach, 1997). In algorithm-driven social media, when users trust the health information they encounter, they perceive fewer risks of privacy violations and manipulation, fostering a willingness to interact with and disseminate such content. This process aligns with prior findings showing that trust encourages active participation in online health communities. For instance, research demonstrates that users with high levels of trust in online health communities not only adopt the information provided but also contribute their own knowledge, thus reinforcing mutual engagement (Connolly et al., 2023). Similarly, studies in live streaming environments such as TikTok show that trust in broadcasters and products promotes rapid formation of social bonds, which translates into greater user engagement behaviors like purchasing, commenting, and sharing (Guo et al., 2021). Therefore, we hypothesize:

H5: Users' trust in health information from algorithm-driven social media will be positively associated with their engagement with it.

https://doi.org/10.65476/7tp42020

Mediation Effects

We further investigated the serial mediating roles of social privacy concerns, perceptions of institutional privacy practices, and trust in the relationship between ethical considerations and users' engagement with health information on algorithm-driven social media platforms. Specifically, we propose that users' ethical evaluations of algorithmic practices shape their engagement with content through a sequential pathway involving heightened social privacy concerns, greater perceptions of privacy practices, and, ultimately, trust in algorithm-recommended health information.

This rationale is grounded in the stimulus–organism–response (SOR) framework, which posits that environmental stimuli (e.g., media affordances and ethical cues) indirectly influence behavioral responses through intervening psychological processes such as cognitive appraisal (Mehrabian, 1980). Within this framework, users' ethical considerations serve as the initial stimulus, heightening their privacy concerns. These concerns then activate perceptions of privacy practices, which shape users' appraisal of how platforms safeguard their data. This appraisal process directly affects trust in algorithm-recommended health content, which, in turn, determines users' willingness to engage with it. Prior studies support this sequential mechanism. For instance, research shows that privacy concerns can undermine trust in algorithmic systems, thereby reducing engagement (Xu et al., 2011). Conversely, effective privacy practices and transparent communication by platforms may alleviate these concerns, strengthen trust, and encourage users to interact with the content despite initial reservations (Handa et al., 2024). Capturing this complexity, we posit that ethical considerations influence engagement not directly but through this multistage mediating chain of privacy concerns, perceptions, and trust. Therefore, we propose:

RQ1: Do social privacy concerns, perceptions of institutional privacy practices, and trust in health information on algorithm-driven social media serially mediate the relationship between ethical considerations and user engagement?

Methods

After receiving ethical approval from the Institutional Review Board at a university, we engaged Sojump, a professional survey company, to conduct an online survey in mainland China from October to November 2023. Sojump, a reputable and widely used online data services platform with more than 3 million active users, has been employed in numerous peer-reviewed studies (e.g., Zheng et al., 2024). To ensure a demographically diverse sample, Sojump implemented sampling quotas based on key demographic variables, including age, gender, education level, and geographic region. The final sample thus included participants from all major provinces and across varying demographic categories. Eligible participants were adults aged 18 years and above who were active users of algorithm-driven social media and had previously encountered or accessed health information recommended by these platforms.

A total of 3,734 participants were invited to take part in the online survey, with 1,051 participants completing the survey, yielding a response rate of 28.14%. The survey asked participants about their personal experiences with health-related information recommended by algorithm-driven social media, as well as their privacy concerns about using these platforms. The survey took approximately 10 minutes to

https://doi.org/10.65476/7tp42020

complete, and participants were compensated with 9 CNY. Of the participants, 38.34% were male and 61.66% were female, with ages ranging from 18 to 60 years old (M = 31.90, SD = 7.35). The median education level was a bachelor's degree, and half of the participants reported a monthly household income of less than 10,000 CNY. On average, participants spent 9.47 hours per week using algorithm-driven social media.

Measures

Measurements for each variable examined in this study were adapted from previously validated research instruments or established scales. The item wording, descriptive statistics, and corresponding references for all measures are presented in Table 1. Unless otherwise stated, all items were measured using 5-point Likert scales ranging from 1 (strongly disagree) to 5 (strongly agree) to provide sufficient granularity for respondents to express differentiated opinions.

https://doi.org/10.65476/7tp42020

Table 1. Item Wording and Descriptive Statistics.

Variables	Items		*M*(*SD*)	Loading	Cronbach's *a*	AVE	CR	MSV	ASV	References
Social privacy concern	a)	"I am not concerned that my online behavioral data on algorithm-driven social media could be misused by other users." [reverse-coded]	3.98(1.16)	.72	.70	.51	.76	.16	.12	Malhotra et al. (2004)
	b)	"I believe that my online behavioral data on algorithm-driven social media could threaten my privacy."	3.39(1.12)	.76						
	c)	"I am concerned that any users on algorithm-driven social media may access my online behavioral data."	3.36(1.12)	.66						
Perceived institutional privacy practices	a)	"Algorithm-driven social media companies are transparent in disclosing how user data is collected, processed, and used."	4.08(.87)	.78	.71	.52	.76	.13	.02	Malhotra et al. (2004)
	b)	"Privacy policies of algorithm-driven social media platforms as clear and easy to understand."	4.09(.90)	.65						
	c)	"Social media platforms provide me with sufficient information about how my personal data is handled."	4.29(.81)	.72						

Trust in health information from algorithm-driven social media	a)	"I trust the recommended health information by algorithm-driven social media."	3.77(.76)	.69	.73	.51	.76	.24	.11	Wai Lai & Liu (2020)
	b)	"Recommended health information through the algorithmic processes on social media is credible."	3.84(.92)	.72						
	c)	"The health information recommended on algorithm-driven social media is trustworthy."	3.64(.90)	.73						
Ethical considerations over the algorithm-driven social media	a)	"It is not always transparent why algorithms decide to show me certain health information on social media."	3.59(.93)	.86	.75	.62	.83	.16	.05	Zarouali et al. (2021)
	b)	"The health information that algorithms recommend to me on social media can be subjected to human biases (e.g., prejudices and stereotypes)."	3.39(1.14)	.77						
	c)	"Algorithms using my personal data to recommend health information on social media has negative consequences for me."	3.70(1.04)	.89						
Engagement in health	a)	"I often like and comment on others' posts regarding health	3.61(1.02)	.78	.83	.56	.83	.24	.10	Khan (2017); Lim

https://doi.org/10.65476/7tp42020

information from algorithm-driven social media		content on algorithm-driven social media."			et al. (2015)
	b)	"I often express my feelings about others' posts regarding health content on algorithm-driven social media."	3.46(1.16)	.80	
	c)	"I interact with others regarding health content on algorithm-driven social media."	3.59(1.09)	.76	
	d)	"Anything related to health content on algorithm-driven social media grabs my attention."	3.63(1.02)	.64	

Note. AVE = Average Variance Extracted; CR = Composite Reliability; MSV = Maximum Shared Variance; ASV = Average Shared Squared Variance; M = Mean Score; SD = Standard Deviation.

https://doi.org/10.65476/7tp42020

Data Analytical Approach

Structural equation modeling (SEM) was conducted using JASP (Love et al., 2019). SEM enables simultaneous testing of both measurement and structural relationships among latent variables, providing a comprehensive assessment of how observed indicators reflect theoretical constructs and how these constructs interrelate. First, a confirmatory factor analysis (CFA) was performed to evaluate the measurement model—that is, how well the observed items represent their underlying latent constructs (e.g., ethical concern, privacy concern, trust, and engagement). CFA assesses convergent validity (the degree to which items measuring the same construct are correlated) and discriminant validity (the extent to which conceptually distinct constructs are empirically distinguishable). Next, the structural model was tested to examine the hypothesized relationships among the latent variables, while statistically controlling for participants' age, gender, income, and education. Model fit was evaluated based on Hu and Bentler's (1999) established guidelines, which suggest that a well-fitting model should have a Tucker–Lewis Index (TLI) and Comparative Fit Index (CFI) above .90, a Root Mean Square Error of Approximation (RMSEA) below .05, and a Standardized Root Mean Square Residual (SRMR) below .08.

Finally, mediation analyses were conducted within the SEM framework using 5,000 bootstrap samples with 95% confidence intervals to test indirect effects. This approach provides robust estimates of mediation paths, capturing the mechanisms through which ethical and privacy concerns influence trust and engagement with algorithmically recommended health information. Statistical significance was assessed using a two-tailed test with an alpha level of 0.05, following conventional standards in social science research.

Results

The measurement model demonstrated good fit: $\chi^2 = 181.20$, $df = 89$, $p < .001$, CFI = .96, TLI = .95, $\chi^2/df = 2.04$, RMSEA = .05, SRMR = .05 (see Table 2). The full structural model also demonstrated an acceptable fit: $\chi^2 = 436.72$, $df = 151$, $p < .001$, CFI = .95, TLI = .94, $\chi^2/df = 2.89$, RMSEA = .04, SRMR = .06 (see Table 2). Factor loadings for all measurement items exceeded 0.60, with most between 0.70 and 0.90. The composite reliability (CR) and Cronbach's alpha of each variable were above 0.70, and the Average Variance Extracted (AVE) for all variables was above 0.50, indicating good reliability and convergent validity (Hair, 2010; see Table 2). Additionally, we found that the Maximum Shared Variance (MSV) value and the Average Shared Squared Variance (ASV) value were both lower than the AVE for all the measured constructs. Hence, the constructs in our model were distinct, confirming discriminant validity (Hair, 2010). Five pairs of items measuring the same latent variables were correlated, as suggested by modification indices, to improve model fit. The full model explained 48.1% of the variance in user engagement with health information from algorithm-driven social media.

Table 2. Model Fit for the Measurement Model and Structural Model.

Model fit	χ^2	*Df*	CFI	TLI	RMSEA	SRMR	χ^2/df
Measurement Model	181.20	89	.96	.95	.05	.05	2.04
Structural Model	436.72	151	.95	.94	.04	.06	2.89

Specifically, results showed that users' social privacy concerns about algorithm-driven social media were negatively associated with their trust in *(β* = −.55, *p* < .001) and engagement with (*β* = −.12, *p* = .011) health-related information on these platforms, thus supporting H1a and H1b. Additionally, users' perceptions of institutional privacy practices were positively associated with their trust in health-related information from the platforms (*β* =.35, *p* < .001), supporting H2a. However, perceptions of institutional privacy practices were not significantly related to their engagement with this information (*β* = .02, *p* = .59), meaning H2b was not supported. In contrast, perceptions of institutional privacy practices were positively associated with social privacy concerns (*β* = .18, *p* < .001), supporting H3. Individuals' ethical considerations about algorithm-driven social media were positively associated with both social privacy concerns (*β* = .56, *p* < .001) and perceptions of institutional privacy practices (*β* = .22, *p* < .001; see Figure 1), supporting H4a and H4b. Lastly, trust in health-related information from the algorithm-driven social media was positively related to engagement with it (*β* = .58, *p* < .001), thus supporting H5. The results of the structural equational modeling were displayed in Figure 2. The power analysis, conducted using G*Power 3.1, indicates that our sample size (*N* = 1,051) provides adequate statistical power (> .85) to detect small-to-medium effect sizes (*ω* = .10–.30) at an alpha level of .05 with 151 degrees of freedom, which clarifies the sensitivity and robustness of our analyses.

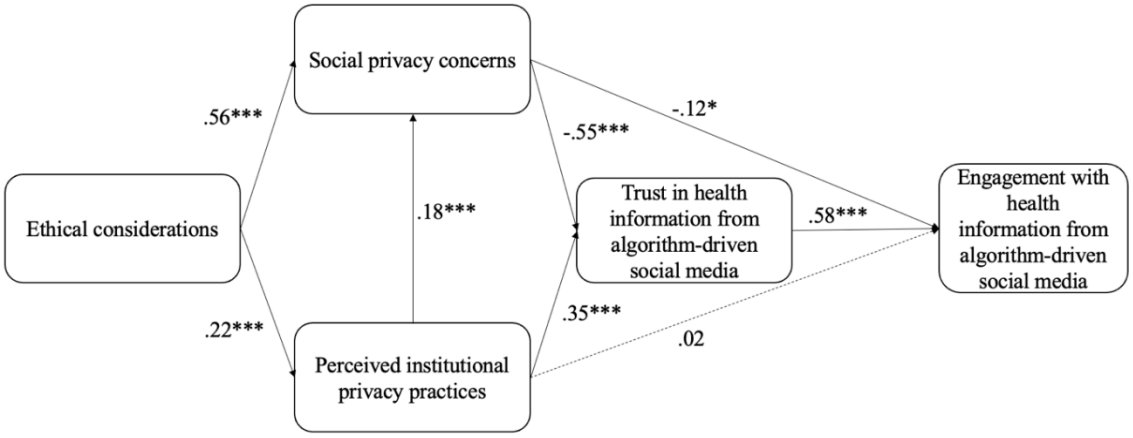

Figure 2. Results of the structural model.

Note. *N* = 1,051; *p* < .05*, *p* < .01**, *p* < .001***; Solid lines represent statistically significant paths and dotted lines represent statistically nonsignificant paths.

The mediation analysis revealed that trust in health-related information from algorithm-driven social media significantly mediated the relationship between social privacy concerns and engagement with health-related information (*b* = −.54, *p* < .001, 95% CI [−.68, −.40]). Additionally, trust in health-related information also mediated the association between perceptions of institutional privacy practices and engagement with health-related information (*b* = .34, *p* < .001, 95% *CI* [.23, .46]). Furthermore, the pathway from social privacy concerns to trust in health information recommended by algorithm-driven social media serially mediated the relationship between ethical considerations and engagement with this content (*b* = −.26, *p* < 0.001, 95% *CI* [−.33, −.19]). Similarly, the pathway from perceptions of institutional privacy practices to trust in algorithm-recommended health information also serially mediated the relationship

https://doi.org/10.65476/7tp42020

between ethical considerations and engagement (b = .06, p < 0.001, 95% *CI* [.03, .10]). Lastly, the pathway from perceptions of institutional privacy practices, through social privacy concerns, to trust in algorithm-recommended health information serially mediated the relationship between ethical considerations and engagement (b = −.02, p = .002, 95% *CI* [−.03, −.01]; see Table 3).

Table 3. Results of Mediation Analysis.

Paths: Indirect effects	*b*	*p p*	*β*	95%*CI*
Social privacy concern → Trust → Engagement	−.54	< .001	−.32	[−.68, −.40]
Perceptions of institutional privacy practices → Trust → Engagement	.34	< .001	.20	[.23, .46]
Ethical consideration → Social privacy concern → Trust → Engagement	−.26	< .001	−.18	[−.33, −.19]
Ethical concerns → Perceptions of institutional privacy practices → Trust → Engagement	.06	< .001	.04	[.03, .10]
Ethical concerns → Perceptions of institutional privacy practices → Social privacy concern → Trust → Engagement	−.02	.002	−.01	[−.03, −.01]

Discussion

Informed by CPM theory, we proposed a model to examine how users' ethical considerations about algorithm-driven social media influence their trust in and engagement with recommended health content, with social privacy concerns and perceptions of institutional privacy practices as mediators. An online survey of algorithmic social media users revealed that ethical concerns were positively associated with both social privacy concerns and perceptions of institutional privacy practices. Social privacy concerns were negatively related to trust, whereas perceptions of institutional privacy practices were positively related. In turn, trust positively impacted engagement. We found a negative indirect effect of ethical considerations on engagement via social privacy concerns and trust, and a positive indirect effect via perceptions of institutional privacy practices and trust. These findings highlight the distinct roles of different privacy concerns, with social privacy concerns deterring trust and engagement and perceptions of institutional practices fostering them.

We found that users' ethical considerations about algorithm-driven social media were positively related to their perceptions of institutional privacy practices. This aligns with previous research showing that users concerned with ethical issues like data fairness, transparency, and accountability are more vigilant about their privacy (e.g., Mittelstadt et al., 2016; Wu, 2024). Ethical considerations lead users to question how their data are managed, resulting in greater perceptions of privacy practices. Similarly, ethical considerations positively influence social privacy concerns, as users become more cautious about exposing personal information (Handa et al., 2024; Shin et al., 2022). These findings highlight the need for transparency, user control, and ethical responsibility in algorithm-driven platforms, which can help reduce privacy concerns and foster trust and engagement.

https://doi.org/10.65476/7tp42020

We also uncovered distinct effects of different privacy-related perceptions on trust in health content recommended by algorithm-driven social media platforms: Social privacy concerns were negatively related to trust, while perceptions of institutional privacy practices were positively related. This finding aligns with previous research showing that when users perceive risks in social sharing and feel a lack of control over who can see their information, their trust in the platform diminishes, affecting their willingness to engage with content shared or recommended by it (Handa et al., 2024; Jozani et al., 2020). In our study's context, users' concerns about visibility and peer interactions likely reduce their trust in recommended health content, as they may doubt the platform's ability to adequately protect their data and privacy preferences.

Conversely, users with heightened perceptions of institutional privacy practices focus on how well the platform itself safeguards data through secure storage, transparent data policies, and responsible data sharing. Research suggests that when platforms are perceived as responsible and transparent in their data handling, they can foster user trust (Jozani et al., 2020; Shin et al., 2022). Therefore, users who are aware of the platform's institutional privacy practices may feel reassured and more inclined to trust the health information recommended by the platform, viewing it as a credible source. The differing effects of social privacy concerns and perceptions of institutional privacy practices on trust highlight the need for platforms to adopt a comprehensive privacy strategy—one that builds institutional trust while addressing social privacy concerns. However, while perceptions of privacy practices were positively related to trust in social media–recommended content, they did not lead to increased user engagement. This suggests that even though users may trust the content more because of their perceptions of privacy practices, this trust does not necessarily translate into active engagement with or use of the content. This may be because trust alone is not sufficient to drive user engagement. Other factors, such as content relevance or user interest, also play crucial roles in determining whether users engage with recommended information (Wahid & Gunarto, 2022).

The finding that ethical considerations influence engagement with algorithm-recommended health content through two opposing pathways—that is, negatively via social privacy concerns and trust and positively via perceptions of institutional privacy practices and trust. This offers a nuanced understanding of how different types of privacy concerns shape user behavior. On one hand, social privacy concerns can erode trust, thereby reducing engagement with recommended health content, particularly when ethical concerns amplify users' sensitivity to social privacy risks (Jozani et al., 2020). On the other hand, when platforms demonstrate privacy practices protecting personal data, users' perceptions of such practices can reinforce their trust in such platforms, as they feel their data are securely managed at an organizational level. This heightened trust, in turn, positively impacts engagement, as users view the platform as a credible and safe source of health information. These opposing indirect effects underscore the importance of addressing both social privacy concerns and perceptions of institutional privacy practices to foster a trust-based user experience. Algorithm-driven platforms could enhance user trust and engagement with health content by balancing robust institutional privacy practices with greater user control over social privacy settings, thereby effectively addressing ethical concerns.

Implications and Limitations

This study has several theoretical implications. First, it extends the scope of CPM theory by incorporating ethical considerations as a precursor to how individuals navigate privacy boundaries in the

https://doi.org/10.65476/7tp42020

context of health information consumption on algorithm-driven social media. By positioning ethical concerns about social media algorithms as contextual factors influencing privacy perceptions, this study highlights their impact on users' engagement with health information. Specifically, individuals who are more concerned about the transparency and accountability of the algorithms governing these platforms are likely to experience heightened social privacy concerns, which, in turn, reduce their trust in and engagement with recommended health content. This perspective underscores the pivotal role of algorithmic ethics in shaping health information consumption behaviors.

Second, this study advances a nuanced understanding of the dual effects of privacy-related perceptions in the context of algorithm-driven social media. It demonstrates that while social privacy concerns undermine users' trust and engagement with health content, perceptions of institutional privacy practices exert a counterbalancing, positive influence. These contrasting pathways extend CPM theory by highlighting the dynamic push-and-pull of privacy negotiations, showing that users' behaviors are shaped by the simultaneous tension between protective concerns and reassurances of institutional safeguards. In doing so, the findings refine CPM's explanatory power by revealing how different types of privacy perceptions can coexist and interact to influence disclosure and engagement decisions.

Third, this research broadens the scope of CPM theory by applying it to the emerging domain of algorithm-driven social media. Unlike traditional online health communication contexts, algorithm-driven platforms personalize information flow and blur boundaries between private and public spheres. By situating CPM in this novel setting, the study underscores the theory's relevance for understanding how individuals negotiate privacy boundaries and make engagement decisions in highly personalized environments. This application not only validates CPM's adaptability but also extends its theoretical reach to the challenges posed by contemporary algorithmic communication systems.

This study also offers several practical implications. First, as social privacy concerns diminish trust in algorithm-recommended health information, platform developers should design mechanisms that give users granular control over the visibility, sharing, and use of their personal data. Implementing user-friendly privacy dashboards, default privacy-by-design settings, and clear notifications about data usage can effectively alleviate user anxiety and foster greater trust. Second, the positive association between perceptions of institutional privacy practices and trust underscores the importance of organizational transparency. Platforms should regularly communicate their data-handling protocols, algorithmic decision processes, and third-party data-sharing policies—particularly about health-related content—through accessible and plain-language disclosures. Third, the contrasting effects of social versus institutional privacy concerns suggest that multilayered privacy strategies are needed: User-centered interpersonal controls (e.g., limiting social visibility of health interactions) should complement transparent institutional governance frameworks. Fourth, as users' ethical considerations about algorithms heighten both privacy concerns and trust expectations, policy makers and regulators should establish clearer standards for algorithmic accountability, mandating explainability and independent auditing of health-related recommendation systems. Finally, collaboration among developers, health authorities, and regulators is crucial for building a trustworthy digital health ecosystem, helping to balance personalization with protection, innovation with responsibility, and engagement with ethical integrity.

https://doi.org/10.65476/7tp42020

Our study has several limitations. First, its cross-sectional design limits our ability to observe how ethical considerations may elicit privacy concerns and influence users' trust and engagement with social media–recommended content over time, as well as to establish causal relationships between these variables. Future research could employ longitudinal or experimental designs to explore these causal dynamics more effectively. Second, participants were recruited through an online panel provided by a professional survey company, which may not fully represent the broader Chinese population. Although quota sampling was used to ensure diversity in age, gender, education, and geographic region, potential sampling biases and a relatively low response rate remain possible, as many individuals screened by the platform did not meet the eligibility criteria for inclusion (i.e., being active users of algorithm-driven social media who had previously encountered health information recommended by these platforms). Additionally, although we ensured that participants were drawn from multiple provinces across China, we did not track whether they resided in rural or urban areas. Given that digital disparities persist between regions, particularly in access to and comprehension of health information on social media, the findings should be interpreted with caution and may not be fully generalizable to all segments of the population.

Third, we did not consider other variables that may affect user engagement with social media–recommended health content beyond privacy concerns, such as the perceived benefits of acquiring health content via social media (Jozani et al., 2020) and privacy self-efficacy (Chen, 2018). Future studies on user engagement with recommended content on social media could investigate these additional factors, as they have been shown to be significant in influencing engagement. Lastly, this study examined health information on algorithm-driven social media in general, without differentiating between types of health information. The effects of privacy concerns on engagement may vary substantially across content types (e.g., diet, lifestyle, exercise, mental health, or information about infectious or fatal diseases). Future research could investigate how algorithms recommend different categories of health information and how these distinctions influence user engagement.

References

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66–84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1–21. https://doi.org/10.1016/j.im.2015.08.001

Bright, L. F., Lim, H. S., & Logan, K. (2021). "Should I post or ghost?": Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing, 38*(10), 1712–1722. https://doi.org/10.1002/mar.21499

https://doi.org/10.65476/7tp42020

Brinson, N., Amini, B., Lemon, L., & Bawole, C. (2024). Electronic performance monitoring: The role of reactance, trust, and privacy concerns in predicting job satisfaction in the post-pandemic workplace. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18*(5), Article 10. https://doi.org/10.5817/CP2024-5-10

Cain, J. A., & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society, 24*(12), 2705–2724. https://doi.org/10.1177/14614448211000327

Chen, H. T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist, 62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691

Connolly, R., Sanchez, O. P., Fundacao, G. V., Compeau, D., Tacco, F., & Fundacao Getulio,V. (2023). Understanding engagement in online health communities: A trust-based perspective. *Journal of the Association for Information Systems, 24*(2), 345–378. https://doi.org/10.17705/1jais.00785

Craig, M. J. (2025). Human-machine communication privacy management, privacy fatigue, and the conditional effects of algorithm awareness on privacy co-ownership in the social media context. *Computers in Human Behavior, 173*, *108786*. https://doi.org/10.1016/j.chb.2025.108786

Culnan, M. J., & Bies, R. J. (1999). Managing privacy concerns strategically: The implications of fair information practices for marketing in the twenty-first century. In C. J. Bennett & R. Grant (Eds.), *Visions of privacy* (pp. 149–167). Toronto: University of Toronto Press.

De Wolf, R. (2016). Group privacy management strategies and challenges in Facebook: A focus group study among Flemish youth organizations. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), Article 5. https://doi.org/10.5817/CP2016-1-5

DiStaso, M. W., & Bortree, D. S. (2012). Multi-method analysis of transparency in social media practices: Survey, interviews and content analysis. *Public Relations Review, 38*(3), 511–514. https://doi.org/10.1016/j.pubrev.2012.01.003

Duong, H. L., Tran, M. T., Vo, T. K. O., & Tran, T. K. C. (2024). Social media and privacy concerns: Exploring university student's privacy concerns in TikTok platform in Vietnam. *Journal of Information, Communication and Ethics in Society, 22*(4), 392–418. https://doi.org/10.1108/JICES-04-2024-0045

Foxman, E. R., & Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing, 12*(1), 106–119. https://doi.org/10.1177/074391569501200111

Guo, L., Hu, X., Lu, J., & Ma, L. (2021). Effects of customer trust on engagement in live streaming commerce: Mediating role of swift guanxi. *Internet Research, 31*(5), 1718–1744. https://doi.org/10.1108/INTR-02-2020-0078

Hair, J. F. (Ed.). (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Handa, M., Bhalla, R., & Ahuja, P. (2024). My privacy at risk – my guard is on: A study of SNS use among young adults. *Vilakshan - XIMB Journal of Management, 21*(1), 126–140. https://doi.org/10.1108/XJM-05-2023-0108

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*, 106260. https://doi.org/10.1016/j.chb.2020.106260

Khan, M. L. (2017). Social media engagement: What motivates user participation and consumption on YouTube? *Computers in Human Behavior, 66*, 236–247. https://doi.org/10.1016/j.chb.2016.09.024

Kim, K., & Moon, S. I. (2021). When algorithmic transparency failed: Controversies over algorithm-driven content curation in the South Korean digital environment. *American Behavioral Scientist, 65*(6), 847–862. https://doi.org/10.1177/0002764221989783

Koene, A., Perez, E., Carter, C. J., Statache, R., Adolphs, S., O'Malley, C., Rodden, T., & McAuley, D. (2015). Research ethics and public trust, preconditions for continued growth of internet mediated research: Public confidence in internet mediate research. In *ICISSP 2015: Proceedings of the 1st International Conference on Information Systems Security and Privacy* (pp. 163–168). ESEO, Angers, Loire Valley, France: Science and Technology Publications. https://doi.org/10.5220/0005331501630168

Kotilainen, S., Okkonen, J., Vuorio, J., & Leisti, K. (2020). Youth media education in the age of algorithm-driven social media. In D. Frau-Meigs, S. Kotilainen, M. Pathak-Shelat, M. Hoechsmann, & S. R. Poyntz (Eds.), *The handbook of media education research* (1st ed., pp. 131–139). Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/9781119166900.ch10

Lim, J. S., Hwang, Y., Kim, S., & Biocca, F. A. (2015). How social media engagement leads to sports channel loyalty: Mediating roles of social presence and channel commitment. *Computers in Human Behavior, 46*, 158–167. https://doi.org/10.1016/j.chb.2015.01.013

https://doi.org/10.65476/7tp42020

Love, J., Selker, R., Marsman, M., Jamil, T., Dropmann, D., Verhagen, J., Ly, A., Gronau, Q. F., Smíra, M., Epskamp, S., Matzke, D., Wild, A., Knight, P., Rouder, J. N., Morey, R. D., & Wagenmakers, E.-J. (2019). JASP: Graphical statistical software for common statistical designs. *Journal of Statistical Software, 88*(2), 1–17. https://doi.org/10.18637/jss.v088.i02

Lutz, C., & Ranzini, G. (2017). Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media + Society, 3*(1), 1–12. https://doi.org/10.1177/2056305117697735

Lutz, C., & Tamo-Larrieux, A. (2020). The robot privacy paradox: Understanding how privacy concerns shape intentions to use social robots. *Human-Machine Communication, 1*, 87–111. https://doi.org/10.30658/hmc.1.6

Majjate, H., Bellarhmouch, Y., Jeghal, A., Yahyaouy, A., Tairi, H., & Zidani, K. A. (2025). Assessing the impact of ethical aspects of recommendation systems on student trust and engagement in e-learning platforms: A multifaceted investigation. *Education and Information Technologies, 30*(3), 3953–3977. https://doi.org/10.1007/s10639-024-12979-3

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. https://doi.org/10.1287/isre.1040.0032

Matei, S., Rughinis, C., & Rughinis, R. (2017). Big data, old users, personal worlds: A survey of challenges and resistance to big data analytics in the EU. In *2017 21st International Conference on Control Systems and Computer Science (CSCS)* (pp. 175–181). Bucharest, Romania: IEEE. https://doi.org/10.1109/CSCS.2017.31

Mehrabian, A. (1980). *Basic dimensions for a general psychological theory: Implications for personality, social, environmental, and developmental studies*. Cambridge, MA: Oelgeschlager, Gunn & Hain.

Meng, X. (2024). From interpersonal privacy to humantechnological privacy: Communication privacy management theory revisited. *Technical Communication, 71*(2), 72–88. https://doi.org/10.55177/tc304825

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21. https://doi.org/10.1177/2053951716679679

https://doi.org/10.65476/7tp42020

Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government Information Quarterly, 37*(1), 101413. https://doi.org/10.1016/j.giq.2019.101413

Nguyen, T. T., Backes, M., & Stock, B. (2022). Freely given consent?: Studying consent notice of third-party tracking and its violations of GDPR in Android apps. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2369–2383). Los Angeles, CA: ACM. https://doi.org/10.1145/3548606.3560564

Nguyen, T. T., Tran, V. T. T., & Tran Hoang, M. T. (2024). How peer privacy concerns affect active and passive uses of social networking sites: A dual peer privacy calculus model. *Social Science Computer Review, 42*(6), 1440–1463. https://doi.org/10.1177/08944393231224539

Ou, M., Zheng, H., Kim, H. K., & Chen, X. (2023). A meta-analysis of social media fatigue: Drivers and a major consequence. *Computers in Human Behavior, 140*, 107597. https://doi.org/10.1016/j.chb.2022.107597

Ozdemir, Z. D., Jeff Smith, H., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642–660. https://doi.org/10.1057/s41303-017-0056-z

Petronio, S., & Kovach, S. (1997). Managing privacy boundaries: Health providers' perceptions of resident care in Scottish nursing homes. *Journal of Applied Communication Research, 25*(2), 115–131. https://doi.org/10.1080/00909889709365470

Petronio, S., & Sargent, J. (2011). Disclosure predicaments arising during the course of patient care: Nurses' privacy management. *Health Communication, 26*(3), 255–266. https://doi.org/10.1080/10410236.2010.549812

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A., & Ling, R. (2020). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. *Media Psychology, 23*(6), 840–864. https://doi.org/10.1080/15213269.2019.1648218

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. https://doi.org/10.1080/10447318.2021.1994211

Shin, D., Kee, K. F., & Shin, E. Y. (2022). Algorithm perceptions: Why user perceptions is critical for personal privacy in the adoption of algorithmic platforms? *International Journal of Information Management, 65*, 102494. https://doi.org/10.1016/j.ijinfomgt.2022.102494

https://doi.org/10.65476/7tp42020

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196. https://doi.org/10.2307/249477

Trifiro, B. M. (2023). Breaking your boundaries: How TikTok use impacts privacy concerns among influencers. *Mass Communication and Society, 26*(6), 1014–1037. https://doi.org/10.1080/1520543

Wahid, R. M., & Gunarto, M. (2022). Factors driving social media engagement on Instagram: Evidence from an emerging market. *Journal of Global Marketing, 35*(2), 169–191. https://doi.org/10.1080/08911762.2021.1956665

Wai Lai, I. K., & Liu, Y. (2020). The effects of content likeability, content credibility, and social media engagement on users' acceptance of product placement in mobile social networks. *Journal of Theoretical and Applied Electronic Commerce Research, 15*(3), 1–19. https://doi.org/10.4067/S0718-18762020000300102

Wells, J. D., Valacich, J. S., & Hess, T. J. (2011). What signal are you sending? How website quality influences perceptions of product quality and purchase intentions. *MIS Quarterly, 35*(2), 373–396. https://doi.org/10.2307/23044048

Wilson, S. R., Hintz, E. A., MacDermid Wadsworth, S. M., Topp, D. B., Southwell, K. H., & Spoont, M. (2021). Female US military veterans' (non) disclosure of mental health issues with family and friends: Privacy rules and boundary management. *Health Communication, 36*(4), 412–423. https://doi.org/10.1080/10410236.2019.1693128

Wongkitrungrueng, A., & Assarut, N. (2020). The role of live streaming in building consumer trust and engagement with social commerce sellers. *Journal of Business Research, 117*, 543–556. https://doi.org/10.1016/j.jbusres.2018.08.032

Wu, C. (2024). Data privacy: From transparency to fairness. *Technology in Society, 76*, 102457. https://doi.org/10.1016/j.techsoc.2024.102457

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Zarouali, B., Boerman, S. C., & De Vreese, C. H. (2021). Is this recommended by an algorithm? The development and validation of the algorithmic media content perceptions scale (AMCA-scale). *Telematics and Informatics, 62*, 101607. https://doi.org/10.1016/j.tele.2021.101607

https://doi.org/10.65476/7tp42020

Zhang, X., Wen, D., Liang, J., & Lei, J. (2017). How the public uses social media WeChat to obtain health information in China: A survey study. *BMC Medical Informatics and Decision Making, 17*(S2), 71–79. https://doi.org/10.1186/s12911-017-0470-0

Zheng, H., Zhao, L., Luo, C., Fu, S., Chen, X., & Liang, S. (2024). Understanding user engagement in mobile health applications from a privacy management perspective. *Health Promotion International, 39*(4), daae103. https://doi.org/10.1093/heapro/daae103

https://doi.org/10.65476/7tp42020