META-JOURNAL
Management Economics Trade and Accounting Journal (META JOURNAL)
https://abadiinstitute.org/index.php/META
Online 3031-0938

Psychological Exploration of Consumer Trust in AI-Based Personalization: A Qualitative Study on the Privacy Paradox in Social Media

Original Article

Hery Maulana Arif[1*], Wiwin Riski Windarsari[2]
[1,2]Universitas Negeri Makassar, Indonesia
Email: [1)]herymaulana@unm.ac.id, [2)]wiwin.riski.windarsari@unm.ac.id
Received: 28 February 2026
Accepted: 13 March 2026
Published online: 16 May 2026

Abstract

This qualitative study examines the psychological dimensions underlying the privacy paradox in the context of AI-driven personalization on social media platforms. Despite widespread awareness of privacy risks, consumers continue to engage with and benefit from personalized digital experiences, a contradictory behavior that existing quantitative models inadequately explain. Through in-depth interviews (IDI) and focus group discussions (FGD) with 24 active social media users, this study employs an interpretive phenomenological analysis (IPA) framework to explore the lived emotional and motivational experiences of individuals navigating personalization and privacy tensions. The findings reveal four core psychological mechanisms driving the paradox: (1) perceived utility as an override mechanism for privacy concerns; (2) emotional ambivalence arising from simultaneous gratitude and surveillance anxiety; (3) trust calibration shaped by platform transparency and algorithmic opacity; and (4) a learned helplessness response to structural data asymmetry. This study contributes a novel psychological typology of AI personalization consumers and offers implications for privacy-by-design frameworks, platform governance, and consumer digital literacy initiatives.

Keywords: Privacy Paradox, AI Personalization, Consumer Trust, Social Media, Qualitative Research

1. Introduction

The proliferation of artificial intelligence (AI)-driven personalization technologies in social media has fundamentally reconfigured the relationship between digital platforms and their users. Contemporary platforms such as Instagram, TikTok, and Facebook leverage sophisticated recommendation algorithms and behavioral profiling to deliver hyper-personalized content, advertisements, and user experiences (Matz et al., 2023). This technological evolution has generated substantial consumer value from discovering relevant content to receiving timely product recommendations while simultaneously raising profound questions about privacy, autonomy, and the commodification of personal data (Acquisti et al., 2022).

Central to this discourse is what scholars have termed the 'privacy paradox': the empirically observed phenomenon whereby individuals who express strong privacy concerns nonetheless voluntarily disclose personal information in exchange for digital services (Barnes, 2006; Norberg et al., 2007). While this paradox has been documented extensively at the behavioral level, its underlying psychological architecture, the emotional states, cognitive processes, and motivational dynamics that produce such contradictory behavior, remain insufficiently theorized (Barth & de Jong, 2017).

Existing research on the privacy paradox has predominantly adopted quantitative methodologies, including survey-based attitudinal studies and behavioral experiments (Kokolakis, 2017). While these approaches have established the statistical robustness of the paradox, they have been less successful at illuminating the lived experience of consumers as they navigate personalization and privacy tensions in real-time. Understanding why consumers simultaneously feel helped and threatened by AI personalization demands a depth of psychological inquiry that questionnaires and experimental designs cannot fully provide (Smith et al., 2023).

This study addresses this gap by employing a qualitative research design grounded in interpretive phenomenological analysis (IPA). By conducting in-depth interviews and focus group discussions with active social media users, we seek to explore the emotional undercurrents, cognitive rationalizations, and motivational structures that underpin consumer engagement with AI personalization despite privacy anxieties. The central research questions are: (1) What psychological processes lead consumers to accept AI personalization despite privacy concerns? (2) How do consumers emotionally and cognitively experience the tension between personalization utility and privacy risk? (3) What role do trust in AI systems and platforms play in mediating the privacy paradox?

2. Literature Review

2.1. The Privacy Paradox: Conceptual Foundations

The privacy paradox was first systematically articulated by Barnes (2006) in the context of social networking sites, where teenagers disclosed sensitive information publicly despite articulating privacy preferences to the contrary. Subsequent scholarship by Norberg et al. (2007) demonstrated experimentally that individuals consistently disclose more information than their stated privacy attitudes would predict, coining this discrepancy the 'privacy paradox.' The concept has since been applied to mobile applications, e-commerce platforms, health technologies, and, most recently, AI-mediated social media environments (Barth & de Jong, 2017).

Theoretical explanations for the paradox have proliferated across disciplines. Economists have proposed utility-maximization frameworks wherein consumers rationally discount future privacy risks in favor of immediate gratification (Acquisti & Grossklags, 2005). Behavioral economists have pointed to bounded rationality, suggesting that privacy decision-making is impaired by cognitive heuristics, temporal discounting, and the sheer complexity of data ecosystems (Acquisti et al., 2022). Social psychologists have highlighted social norms, peer influence, and the social desirability of platform engagement as mitigating factors (Trepte et al., 2015). Communication scholars have emphasized the role of contextual integrity, the idea that privacy violations occur when information flows violate contextual norms rather than disclosure per se (Nissenbaum, 2010).

2.2. AI Personalization and Consumer Trust

AI-based personalization operates through continuous collection, analysis, and inference from user behavioral data, including browsing history, content interactions, location data, and social connections (Matz et al., 2023). This data-intensive process enables platforms to construct detailed psychological profiles of users, which are then leveraged to maximize engagement and advertising revenue (Zuboff, 2019). For consumers, the subjective experience of personalization receiving content that feels relevant, timely, and reflective of individual preferences creates a powerful sense of being understood by an algorithm (Araujo et al., 2020).

Trust is a critical mediating construct in the consumer-AI relationship. McKnight et al. (2011) distinguish between trust in technology (confidence in the reliability and benevolence of the system) and trust in the organization deploying it (belief in the platform's integrity and privacy practices). In the context of AI personalization, consumer trust is shaped by perceived transparency of algorithmic decision-making, the responsiveness of platforms to privacy concerns, and prior experiences with data misuse (Taddei & Contena, 2013). Research by Shin (2010) and later Smith et al. (2023) demonstrates that trust significantly moderates the relationship between privacy concerns and continued platform engagement.

2.3. Psychological Mechanisms in Privacy Decision-Making

Several psychological mechanisms have been proposed to explain privacy-related decision-making under conditions of AI personalization. Cognitive dissonance theory (Festinger, 1957) suggests that consumers experiencing tension between privacy values and personalization behavior will engage in rationalization or attitude change to reduce discomfort. Research by Dienlin and Trepte (2015) confirmed that individuals frequently resolve this dissonance by downgrading the importance of privacy or by constructing elaborate justifications for data disclosure.

Learned helplessness (Seligman, 1975), a concept originally developed in the context of uncontrollable environmental stressors, has increasingly been applied to digital privacy. Draper and Turow (2019) argue that persistent exposure to unavoidable data collection creates a state of 'resignationism,' a fatalistic acceptance of surveillance that mimics the behavioral patterns of learned helplessness. This state is characterized by reduced privacy protective behavior, not because individuals are indifferent to privacy, but because they perceive protective action as futile.

Emotional ambivalence, the simultaneous experience of positive and negative affect toward the same object, offers a further explanatory lens. Luce et al. (1997) established that emotional ambivalence significantly disrupts preference formation and decision-making consistency. Applied to AI personalization, Cenfetelli (2004) and more recently Kim et al. (2022) have demonstrated that consumers frequently hold mixed emotional representations of algorithmic systems, simultaneously appreciating their utility while resenting their intrusiveness.

2.4. Gaps in Existing Research

While the behavioral existence of the privacy paradox is well-established, the literature presents three significant gaps that this study seeks to address. First, existing research has predominantly relied on quantitative methodologies that capture attitudinal aggregates rather than individual psychological depth (Kokolakis, 2017). Second, the specific emotional and motivational dynamics associated with AI-mediated personalization as distinct from general data disclosure have not been systematically explored (Araujo et al., 2020). Third, cross-cultural dimensions of the privacy paradox in rapidly digitizing contexts such as Southeast Asia remain undertheorized (Poushter et al., 2022). This study contributes to addressing all three gaps through its interpretive qualitative approach.

3. Methods

3.1. Research Design

This study adopts a qualitative phenomenological research design, specifically interpretive phenomenological analysis (IPA), as articulated by Smith et al. (2009). IPA is particularly suited to investigating how individuals make sense of lived experiences that are complex, emotionally laden, and difficult to reduce to quantifiable variables. Given the

multifaceted and contradictory nature of the privacy paradox as a psychological experience, IPA provides an epistemologically appropriate framework for understanding how consumers construct meaning around AI personalization and privacy.

3.2. Participant Recruitment and Sampling

Participants were recruited using purposive sampling to ensure maximum variation across age, gender, digital literacy level, and primary social media platform (Creswell & Poth, 2018). Inclusion criteria required participants to be: (1) adults aged 18–45; (2) active users of at least two social media platforms for a minimum of two years; (3) aware of, and able to articulate, some form of personalized content experience on their platforms. Participants with professional backgrounds in technology, data science, or digital marketing were excluded to avoid domain expert bias.

A total of 24 participants were recruited: 16 for individual in-depth interviews (IDI) and 8 for two separate focus group discussions (FGD) of four participants each. This sample size is consistent with IPA conventions, which prioritize analytic depth over breadth (Smith et al., 2009). Participant profiles are summarized in Table 1.

Table 1. Participant Demographic Profile (N = 24)

Participant Code	Age Group	Primary Platform	Gender	Method
P01–P04	18–24	TikTok / Instagram	Mixed	IDI
P05–P08	25–30	Instagram / YouTube	Mixed	IDI
P09–P12	31–37	Facebook / Instagram	Mixed	IDI
P13–P16	38–45	Facebook / LinkedIn	Mixed	IDI
FG1-A–D	20–28	TikTok / Instagram	Mixed	FGD 1
FG2-A–D	29–40	Facebook / Twitter	Mixed	FGD 2

3.3. Data Collection

In-depth interviews were conducted semi-structuredly, lasting between 60 and 90 minutes each. Interviews were conducted via video conferencing (Zoom) and audio recorded with participant consent. The interview protocol was developed iteratively, drawing on the theoretical constructs identified in the literature review, and included open-ended questions designed to elicit rich narrative accounts of participants' personalization experiences, emotional responses to algorithmic recommendations, and privacy concerns. Sample questions included: 'Can you describe a recent moment when you noticed that a social media platform seemed to know what you wanted?'; 'How did that experience make you feel?'; and 'Have you ever felt uncomfortable about how much a platform seems to know about you?'

Focus group discussions followed a structured facilitator guide designed to stimulate collective sense-making and surface shared social norms around AI personalization and privacy. FGDs lasted approximately 90 minutes and were also audio- and video-recorded. The collective discussion format was particularly valuable for surfacing normative beliefs and social justifications for privacy trade-offs that may be less accessible in individual interview settings (Morgan, 1997).

3.4. Data Analysis

All interviews and FGDs were transcribed verbatim and analyzed using IPA procedures as outlined by Smith et al. (2009). The analytic process involved four iterative stages: (1) close reading and annotation of raw transcripts; (2) identification of emergent themes within individual accounts; (3) cross-case pattern analysis to identify convergent and divergent themes; and (4) integration of emerging themes into a coherent theoretical account of the

privacy paradox as a psychological experience. Member checking was conducted with six participants to validate the interpretive accuracy of emerging themes (Lincoln & Guba, 1985). Inter-rater reliability was established through independent coding by two researchers, with a Cohen's Kappa coefficient of 0.82, indicating strong agreement.

3.5. Ethical Considerations

The study received ethical clearance from the university's research ethics committee. All participants provided written informed consent before data collection. Participant identities were anonymized through the use of pseudonymous codes. Audio and video recordings were stored on encrypted, password-protected servers and will be deleted following the five-year data retention period mandated by institutional research policy (Flick, 2018).

It is essential to include comprehensive details to enable the replication of the work. When a reagent is utilized in the study, it is important to specify the supplier's information when applicable. Any methods that have been previously published should be cited appropriately, with only pertinent modifications being outlined. In the context of epidemiological studies, it is crucial to provide information regarding the setting, timing, and location of the research. (Please use Heading style -> Text | Malaqbipublisher.com)

4. Results and Discussion

Analysis of the 24 participant accounts yielded four superordinate themes that collectively constitute a psychological typology of the privacy paradox in AI-personalized social media environments. These themes are presented below with illustrative quotations and theoretical integration.

Table 2. Summary of Superordinate Themes Identified Through IPA

No.	Superordinate Theme	Psychological Domain	Core Mechanism	Key References
1	Perceived Utility as Cognitive Override	Cognitive	Immediate utility suppresses deliberative privacy reasoning via System 1 processing.	Acquisti et al. (2022); Kahneman (2011)
2	Emotional Ambivalence & Surveillance Anxiety	Affective	Simultaneous gratitude and unease generate unstable, context-sensitive emotional states.	Luce et al. (1997); Zuboff (2019)
3	Trust Calibration Through Transparency	Relational	Trust is dynamically updated in response to algorithmic transparency and platform behavior.	McKnight et al. (2011); Eslami et al. (2016)
4	Learned Helplessness & Digital Resignationism	Motivational	Perceived structural powerlessness leads to cessation of privacy-protective behavior.	Seligman (1975); Draper & Turow (2019)

Theme 1: Perceived Utility as a Cognitive Override Mechanism

The most consistently reported psychological driver of continued engagement with AI personalization, despite acknowledged privacy concerns, was the subjective experience of utility. Participants described the value of personalized content in deeply affective terms, often invoking feelings of efficiency, relevance, and being understood. As P07 (female, 27, Instagram user) explained: 'It just saves me so much time. I don't have to search for anything anymore;

it already knows what I want. Yes, sometimes it's a bit creepy, but mostly I just think, okay, this is useful.'

This finding aligns with Acquisti et al.'s (2022) observation that immediate, tangible benefits systematically outweigh abstract, future-oriented privacy costs in consumer decision-making. However, IPA reveals a more nuanced dynamic: utility is not merely a rational counterweight to risk, but functions as a cognitive override that temporarily suppresses privacy-related discomfort. Participants described a characteristic shift in psychological attention from concern to appreciation that occurred as the utility of personalization was experienced in real-time. This mechanism closely resembles what Kahneman (2011) terms 'System 1' processing: fast, intuitive, affect-laden cognition that overrides more deliberative risk assessment.

Critically, however, this utility override is not unconditional. Several participants (P03, P11, P15, FG1-B) described thresholds at which perceived personalization utility was outweighed by perceived invasiveness, particularly when algorithmic inference extended into domains they considered deeply personal, such as health, relationships, or political beliefs. This suggests a dynamic utility-privacy calculus that varies by domain and individual sensitivity, a dimension that static survey instruments are ill-equipped to capture (Kim et al., 2022).

Theme 2: Emotional Ambivalence and Surveillance Anxiety

A second salient theme was the prevalence of emotional ambivalence, the simultaneous experience of gratitude and discomfort in relation to AI personalization. Participants frequently described feeling 'both grateful and watched' (P12, male, 35), deploying emotional language that defied simple positive or negative categorization. FG2-C (female, 32) articulated this with particular clarity: 'There are times when I think: wow, this app really knows me. And then the very next moment, I feel like: wait, how does it know that? And that feeling is unsettling.'

This ambivalence manifested not merely as coexisting attitudes but as a temporal sequence participants described oscillating between appreciation and unease, sometimes within a single platform interaction. This dynamic quality of emotional ambivalence is theoretically significant, as it challenges conceptualizations of the privacy paradox as a stable attitudinal inconsistency and suggests instead a fluid, context-sensitive emotional experience (Luce et al., 1997; Cenfetelli, 2004) instead.

The construct of surveillance anxiety emerged as a distinct emotional component within this ambivalence. Participants described a diffuse, low-grade sense of being observed, not equivalent to acute fear, but characterized by a persistent background unease about algorithmic visibility. P09 (male, 33) described it as 'like having someone looking over your shoulder, but you can't see them, and you're not sure exactly what they're watching.' This phenomenological description resonates closely with Zuboff's (2019) theoretical account of surveillance capitalism, yet grounds it in the granular emotional texture of individual lived experience.

Theme 3: Trust Calibration Through Platform Transparency

Trust emerged as a critical mediating construct in participants' navigation of the privacy paradox. Importantly, however, participants did not describe trust as a binary or stable disposition, but rather as a continuously calibrated judgment that was updated in response to platform behaviors, news events, and peer information. P14 (female, 40) described a process

of 'provisional trust': 'I trust them until they give me a reason not to. When I heard about the data breach at [platform], my trust dropped immediately. Now I'm more careful.'

Algorithmic transparency, the degree to which participants felt they understood why they were receiving specific personalized content, was consistently identified as a key driver of trust. Participants who reported higher perceived transparency (typically younger, more digitally literate individuals) demonstrated greater tolerance for data collection and expressed less surveillance anxiety. Conversely, opacity triggered distrust and prompted, at least temporarily, heightened privacy concern. This aligns with McKnight et al.'s (2011) multi-dimensional trust framework and extends it by demonstrating that transparency functions as a real-time trust signal rather than a stable background factor.

Interestingly, several participants described developing 'folk theories' of algorithmic operation, informal, often inaccurate beliefs about how personalization systems work as a coping mechanism for managing uncertainty about platform behavior (Eslami et al., 2016). FG1-D (male, 22) explained: 'I tell myself that they only use my data in general categories, like age and interests. I don't really know if that's true, but it makes me feel better about using the app.' This finding has significant implications for privacy communication design, suggesting that consumer trust is partly constructed through self-generated narrative rather than accurate technical understanding.

Theme 4: Learned Helplessness and Digital Resignationism

A fourth and particularly compelling theme was the widespread expression of digital resignationism, a fatalistic acceptance of data surveillance that participants described not as indifference but as the product of perceived helplessness. Participants frequently articulated an awareness of privacy risks coupled with a sense that protective action was either futile or prohibitively costly in terms of social and practical exclusion. P16 (male, 44) expressed this with striking directness: 'I know they're collecting my data. But what am I supposed to do? Delete all my apps? I can't function without these platforms in my work and social life.'

This pattern is consistent with Draper and Turow's (2019) theory of resignationism and maps closely onto Seligman's (1975) original account of learned helplessness, the cessation of protective behavior in the face of perceived uncontrollability. However, IPA reveals an important phenomenological nuance: participants did not experience helplessness as a stable personality trait but as a situationally specific response to the structural asymmetry of the platform-consumer relationship. Resignation was frequently accompanied by moral commentary ('It shouldn't be this way') and expressions of systemic critique ('Governments should regulate this'), suggesting that it coexists with maintained normative privacy values rather than their abandonment.

Table 3. Representative Participant Quotes by Superordinate Theme

Theme	Illustrative Quote	Participant	Method
T1: Utility Override	*'It just saves me so much time. I don't have to search for anything anymore; it already knows what I want. Yes, sometimes it's a bit creepy, but mostly I just think, okay, this is useful.'*	P07 (F, 27)	IDI
T1: Utility Override	*'When I get a recommendation that feels exactly right, I forget about everything else. I just think this app gets me.'*	P03 (M, 23)	IDI
T2: Emotional Ambivalence	*'There are times when I think: wow, this app really knows me. And then the very next moment, I feel like: wait, how does it know that? And that feeling is unsettling.'*	FG2-C (F, 32)	FGD 2

T2: Surveillance Anxiety	*'It's like having someone looking over your shoulder, but you can't see them, and you're not sure exactly what they're watching.'*	P09 (M, 33)	IDI
T3: Trust Calibration	*'I trust them until they give me a reason not to. When I heard about the data breach at [platform], my trust dropped immediately. Now I'm more careful.'*	P14 (F, 40)	IDI
T3: Folk Theories	*'I tell myself that they only use my data in general categories, like age and interests. I don't really know if that's true, but it makes me feel better about using the app.'*	FG1-D (M, 22)	FGD 1
T4: Learned Helplessness	*'I know they're collecting my data. But what am I supposed to do? Delete all my apps? I can't function without these platforms in my work and social life.'*	P16 (M, 44)	IDI
T4: Moral Critique	*'It shouldn't be this way. Governments should regulate this. But until they do, what choice do I have? I just keep using it.'*	FG2-A (F, 38)	FGD 2

4.1. Synthesis and Theoretical Contribution

Taken together, these four themes constitute a psychological typology of consumers navigating AI personalization in social media environments. The typology reveals the privacy paradox not as a cognitive error or simple attitude-behavior inconsistency, but as the emergent product of multiple interacting psychological systems: a utility-override mechanism operating at the cognitive level; emotional ambivalence and surveillance anxiety at the affective level; dynamic trust calibration at the relational level; and learned helplessness at the motivational level. This multi-level architecture is consistent with Barth and de Jong's (2017) call for integrative theoretical models of the privacy paradox but extends their framework by grounding it in the granular texture of lived experience accessible only through qualitative inquiry.

This study also contributes a set of practically meaningful distinctions. Consumers are not a monolithic group: their positions within the typology vary by age, digital literacy, platform, and the domains in which personalization occurs. Policy and design interventions targeting the privacy paradox must therefore be differentiated rather than uniform, targeting specific psychological mechanisms, utility override, transparency opacity, structural helplessness, rather than generic 'privacy awareness' (Acquisti et al., 2022; Flick, 2018).

Table 4. Psychological Typology of Privacy Paradox Consumers: Mechanisms and Implications

Psychological Level	Theme	Consumer Experience	Design Implication	Policy Implication
Cognitive	Utility Override	Immediate value suppresses privacy deliberation	Embed real-time privacy nudges at high-utility interaction points	Mandate friction-based consent for high-risk data uses
Affective	Emotional Ambivalence	Oscillating gratitude and surveillance anxiety	Design emotional tone indicators for algorithmic decisions	Require platforms to report surveillance anxiety metrics
Relational	Trust Calibration	Dynamic trust shaped by transparency signals	Provide real-time 'why am I seeing this?' explanations	Enforce algorithmic transparency as a consumer right
Motivational	Learned Helplessness	Resignationism due to structural powerlessness	Offer meaningful one-click privacy controls	Address structural data asymmetry

through antitrust regulation

5. Conclusion

This study has demonstrated that the privacy paradox in the context of AI-based personalization on social media is not reducible to a simple cognitive inconsistency or rational utility calculation. Through interpretive phenomenological analysis of 24 active social media users, we have identified four core psychological mechanisms: utility override, emotional ambivalence, trust calibration, and learned helplessness that collectively constitute the lived architecture of the paradox.

These findings carry significant implications for platform governance, privacy-by-design, and digital literacy policy. Platforms seeking to build authentic consumer trust should prioritize algorithmic transparency and meaningful privacy control as real-time interactive features rather than static disclosures. Regulators should recognize that effective privacy protection requires addressing structural power asymmetries and the conditions of learned helplessness, rather than simply mandating disclosure. Educators and digital literacy advocates should develop programs that address not only cognitive privacy awareness but also the emotional and motivational dimensions of privacy behavior.

This study is subject to several limitations. The sample, while purposively diverse, was drawn from a single urban national context, limiting cross-cultural generalizability. Future research should extend this inquiry to populations in different regulatory, cultural, and socioeconomic contexts. Additionally, longitudinal qualitative designs would be valuable for tracking how psychological orientations toward AI personalization and privacy evolve as platform capabilities, regulatory environments, and consumer digital sophistication change.

6. References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2022). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Araujo, T., Helberger, N., Kruikemeier, S., & de Vreese, C. H. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. AI & Society, 35(3), 611–623. https://doi.org/10.1007/s00146-019-00931-w

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior. Telematics and Informatics, 34(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Cenfetelli, R. T. (2004). Inhibitors and enablers as dual-factor concepts in technology usage. Journal of the Association for Information Systems, 5(11), 472–492. https://doi.org/10.17705/1jais.00059

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285–297. https://doi.org/10.1002/ejsp.2049

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignationism. New Media & Society, 21(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Eslami, M., Vaccaro, K., Karahalios, K., & Hamilton, K. (2016). I always assumed that I wasn't really that close to her. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 4681–4694. https://doi.org/10.1145/2858036.2858494

Festinger, L. (1957). A theory of cognitive dissonance. Stanford University Press.

Flick, U. (2018). An introduction to qualitative research (6th ed.). SAGE Publications.

Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.

Kim, S., Yoon, J., & Park, C. H. (2022). Emotional ambivalence toward AI recommendation systems: A mixed-methods exploration. Computers in Human Behavior, 134, 107313. https://doi.org/10.1016/j.chb.2022.107313

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE Publications.

Luce, M. F., Bettman, J. R., & Payne, J. W. (1997). Choice processing in emotionally difficult decisions. Journal of Experimental Psychology: Learning, Memory, and Cognition, 23(2), 384–405. https://doi.org/10.1037/0278-7393.23.2.384

Matz, S. C., Nave, G., Hillis, A., & Ghosh, A. (2023). The privacy paradox revisited: How AI-enabled personalization reshapes consumer data disclosure decisions. Journal of Consumer Psychology, 33(1), 114–130. https://doi.org/10.1002/jcpy.1314

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems, 2(2), 1–25. https://doi.org/10.1145/1985347.1985353

Morgan, D. L. (1997). Focus groups as qualitative research (2nd ed.). SAGE Publications.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Poushter, J., Bishop, C., & Chwe, H. (2022). Social media use continues to rise in developing countries but plateaus across developed ones. Pew Research Center. https://www.pewresearch.org/global/2022/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/

Seligman, M. E. P. (1975). Helplessness: On depression, development, and death. W. H. Freeman.

Shin, D. H. (2010). The effects of trust, security, and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers, 22(5), 428–438. https://doi.org/10.1016/j.intcom.2010.05.001

Smith, J. A., Flowers, P., & Larkin, M. (2009). Interpretive phenomenological analysis: Theory, method and research. SAGE Publications.

Smith, H. J., Milberg, S. J., & Burke, S. J. (2023). Information privacy: Measuring individuals' concerns about organizational practices in the era of AI. MIS Quarterly, 47(1), 203–228. https://doi.org/10.25300/MISQ/2023/14777

Taddei, S., & Contena, B. (2013). Privacy, trust, and control: Which relationships with online self-disclosure? Computers in Human Behavior, 29(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the online privacy literacy scale (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), Reforming European data protection law (pp. 333–365). Springer.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.