JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)
ISSN (Online): 3105-4811 ISSN (Print): 3106-969X
Volume 2, Issue 2, 2024
https://jecir.com/

ALGORITHMIC HYPER-PERSONALIZATION: THE DOUBLE-EDGED SWORD OF PREDICTIVE PERSONALIZATION - AN EMPIRICAL INVESTIGATION

Danyal Mohiuddin [1]

Affiliations:

[1] University of Northampton, UK

Email: danyal.m.05@gmail.com

Corresponding Author/s Email:

[1] danyal.m.05@gmail.com

ABSTRACT

Algorithmic hyper-personalization has emerged as a dominant strategy in digital marketing, enabling brands to deliver unprecedented levels of relevance and convenience. However, the same technologies that create value for consumers also risk triggering perceptions of surveillance, invasion of privacy, and psychological discomfort often described as "creepiness." This study investigates the paradoxical nature of hyper-personalization, examining the tipping point where perceived benefits are outweighed by psychological costs. Drawing on privacy calculus theory, reactance theory, and the persuasion knowledge model, we develop and test a theoretical model that balances personalization benefits against privacy concerns. Using survey data from 487 consumers in Pakistan, we find that hyper-personalization follows an inverted U-shaped relationship with customer loyalty: moderate levels of personalization maximize loyalty, while excessive personalization diminishes it through increased perceptions of creepiness. Perceived creepiness fully mediates the relationship between hyper-personalization and loyalty, with privacy concerns and perceived surveillance serving as key mechanisms. Consumer characteristics including privacy literacy, trust propensity, and prior brand relationship moderate these effects. The findings contribute to personalization literature by identifying the curvilinear nature of personalization effects and establishing creepiness as a critical mediating mechanism. For practitioners, we provide actionable guidelines for calibrating personalization intensity, implementing transparency measures, and designing consent mechanisms that preserve consumer trust.

Keywords: Hyper-Personalization, Algorithmic Personalization, Creepiness, Privacy Concerns, Customer Loyalty, Predictive Analytics, Consumer Privacy

I. INTRODUCTION

A. The Personalization Paradox

The digital marketing landscape has been transformed by algorithmic personalization. Every day, consumers encounter personalized recommendations, targeted advertisements, tailored content feeds, and predictive suggestions powered by sophisticated machine learning algorithms. These systems analyse vast troves of behavioural data: clicks, searches, purchases, locations, social connections, and even biometric signals, to anticipate consumer needs and deliver precisely targeted content. For consumers, the benefits are tangible: reduced search costs, serendipitous discoveries, and experiences that feel intuitively aligned with their preferences [1, 14].

Yet, beneath this convenience lies an unsettling undercurrent. Consumers increasingly report feeling surveilled, manipulated, and uncomfortably "known" by the brands they interact with. When an app predicts where you're going before you've decided, when an advertisement references a private conversation, or when a recommendation feels intrusively accurate, the response is often not gratitude but unease a phenomenon colloquially termed "creepiness" [13, 10].

This tension defines the personalization paradox: the same technologies that create value also threaten the psychological foundations of consumer trust. Brands must navigate a narrow path between relevance and intrusion, leveraging data to personalize while avoiding the perception of surveillance [8]. Understanding where this boundary lies and how consumers respond when it is crossed is critical for both marketing practice and consumer welfare [7].

B. Problem Statement

Despite extensive research on personalization effectiveness, significant gaps remain. First, most studies assume a linear relationship between personalization and outcomes more personalization yields better results. However, emerging evidence suggests that excessive personalization may backfire, creating an inverted U-shaped relationship [15, 16]. The precise inflection points and underlying mechanisms remain poorly understood.

Second, the construct of "creepiness" has received limited theoretical attention in marketing literature. While acknowledged anecdotally, it lacks conceptual clarity and empirical validation as a mediating mechanism in personalization effects [17].

Third, most personalization research has been conducted in Western contexts, with limited understanding of how cultural factors, particularly in collectivist, high-power-distance societies like Pakistan, shape responses to algorithmic personalization.

C. Research Objectives

This study addresses these gaps through four primary objectives:

1. **To examine the curvilinear relationship** between algorithmic hyper-personalization and customer loyalty, testing whether excessive personalization diminishes loyalty through psychological costs.
2. **To conceptualize and empirically validate "creepiness"** as a psychological mechanism linking hyper-personalization to negative consumer outcomes.
3. **To identify the mechanisms underlying creepiness**, specifically investigating privacy concerns and perceived surveillance as explanatory pathways.
4. **To explore moderating factors** including privacy literacy, trust propensity, and prior brand relationship that influence the personalization-creepiness relationship.

D. Theoretical and Practical Significance

This research makes several contributions. Theoretically, it extends privacy calculus theory by demonstrating that personalization benefits and privacy costs follow nonlinear dynamics. It also integrates reactance theory to explain consumer resistance to excessive personalization. Empirically, it provides the first validated measure of perceived creepiness in a marketing context and establishes its mediating role.

For practitioners, the findings offer actionable guidance for calibrating personalization intensity, designing transparent data practices, and building consumer trust in an era of algorithmic marketing.

II. THEORETICAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

A. Defining Algorithmic Hyper-Personalization

Algorithmic hyper-personalization represents the extreme end of personalization continuum, characterized by:

TABLE 1
DIMENSIONS

Dimension	Description
Predictive Accuracy	Anticipating consumer needs before explicit expression
Data Breadth	Integrating data across multiple domains (purchase, browsing, location, social)

Temporal Depth	Analyzing historical behavior to predict future actions
Contextual Sensitivity	Adapting to real-time situational factors
Cross-Channel Integration	Maintaining personalization consistency across touchpoints

Hyper-personalization differs from basic personalization (e.g., using a customer's name) in its algorithmic sophistication and predictive nature. It represents systems that "know" consumers in ways that may feel intrusive precisely because of their accuracy.

B. Theoretical Foundations

1) Privacy Calculus Theory. Privacy calculus theory [4, 5] posits that individuals engage in a cognitive trade-off between the perceived benefits of disclosing personal information and the perceived risks. When benefits outweigh risks, disclosure occurs; when risks dominate, consumers withhold information or engage in privacy-protective behaviours.

In personalization contexts, benefits include:

- **Relevance:** Content and recommendations aligned with interests
- **Convenience:** Reduced search and decision effort
- **Discovery:** Exposure to serendipitous but relevant options
- **Status:** Recognition and preferential treatment

Risks include:

- **Privacy loss:** Unauthorized access to or use of personal data
- **Surveillance:** Feeling watched or monitored
- **Manipulation:** Being influenced in ways contrary to interests
- **Discrimination:** Differential treatment based on inferred attributes

Traditional privacy calculus assumes linear trade-offs. However, we propose that the calculus changes as personalization intensifies, with marginal benefits diminishing and marginal costs accelerating.

2) Psychological Reactance Theory. Psychological reactance theory [2] and [3] Brehm & Brehm suggested that individuals perceive threats to their behavioural freedom and respond with motivational arousal to restore that freedom. When algorithmic personalization becomes too accurate or intrusive, consumers may perceive it as an encroachment on autonomy sense that algorithms "know them too well" and may be manipulating their choices.

Reactance manifests through:

- **Counter-arguing:** Discounting or resisting personalized messages
- **Avoidance:** Disengaging from personalized touchpoints
- **Boomerang effects:** Doing the opposite of what personalization suggests
- **Negative attitudes:** Reduced trust and increased suspicion

3) Persuasion Knowledge Model. The persuasion knowledge model [6] explains how consumers develop knowledge about persuasion attempts and use this knowledge to cope with marketing. Hyper-personalization may activate persuasion knowledge by making marketing tactics more visible. When consumers perceive that personalization reflects deep analysis of their behaviour, they may become skeptical, inferring manipulative intent.

4) Social Presence Theory. Social presence theory [11, 12] examines the sense of being with another in mediated communication. Algorithmic personalization can create a sense of "algorithmic social presence" the feeling that an intelligent entity is watching and responding. When this presence becomes too salient, it shifts from helpful to unsettling [9].

C. Conceptualizing Creepiness

Creepiness in algorithmic contexts has been defined as "the unsettling feeling that arises when technology exhibits a degree of knowledge or intimacy that feels inappropriate to the social context or relationship" [10]. Building on this, we conceptualize perceived creepiness as comprising three dimensions:

TABLE 2
DIMENSIONS

Dimension	Definition
Inappropriate Intimacy	Technology demonstrating knowledge that feels too personal for the relationship context
Surveillance Awareness	Feeling observed or monitored in ways that exceed expectations
Autonomy Threat	Sensing that algorithms are influencing or manipulating choices without consent

Creepiness differs from general privacy concerns in its specific focus on the affective discomfort arising from the *mismatch* between expected and actual algorithmic knowledge.

D. Hypothesis Development

1) Hyper-Personalization and Customer Loyalty: A Curvilinear Relationship. The relationship between personalization and consumer outcomes has typically been conceptualized as linear. However, emerging research suggests diminishing returns and potential negative effects at extreme levels [15, 1]. We propose an inverted U-shaped relationship:

- **Low personalization:** Insufficient relevance and convenience; consumers may feel the brand does not understand them, limiting loyalty.
- **Moderate personalization:** Optimal balance where benefits of relevance and convenience are realized without triggering psychological costs; loyalty is maximized.
- **High (hyper) personalization:** Benefits continue to increase marginally, but psychological costs (creepiness, reactance) accelerate, causing loyalty to decline.

Hypothesis 1 (H1): The relationship between hyper-personalization and customer loyalty follows an inverted U-shaped curve, such that moderate levels maximize loyalty, while both low and excessive levels reduce loyalty.

2) The Mediating Role of Creepiness. We propose that the negative effects of excessive personalization operate through perceptions of creepiness. When personalization becomes hyper-accurate or intrusive, consumers experience discomfort, which then diminishes loyalty.

Hypothesis 2 (H2): Perceived creepiness mediates the curvilinear relationship between hyper-personalization and customer loyalty.

3) Mechanisms of Creepiness. Creepiness arises from two interrelated perceptions:

Privacy Concerns: The belief that personal data may be misused or exposed. Hyper-personalization signals extensive data collection, heightening privacy concerns, which in turn generate creepiness.

Perceived Surveillance: The feeling of being watched or monitored. When algorithms demonstrate knowledge that seems to come from constant observation, consumers experience surveillance awareness, generating creepiness.

Hypothesis 3 (H3): Privacy concerns and perceived surveillance serve as parallel mechanisms through which hyper-personalization increases perceived creepiness.

4) Moderating Factors. Individual differences shape responses to hyper-personalization:

Privacy Literacy: Consumers with greater understanding of data practices may be less creeped out because they understand how personalization works (or may be more creeped out because they recognize the extent of surveillance). We propose a negative moderating effect—higher literacy reduces creepiness.

Trust Propensity: Consumers with higher general propensity to trust may interpret hyper-personalization as benevolent rather than intrusive.

Prior Brand Relationship: Strong existing relationships buffer against creepiness; trusted brands can personalize more before triggering discomfort.

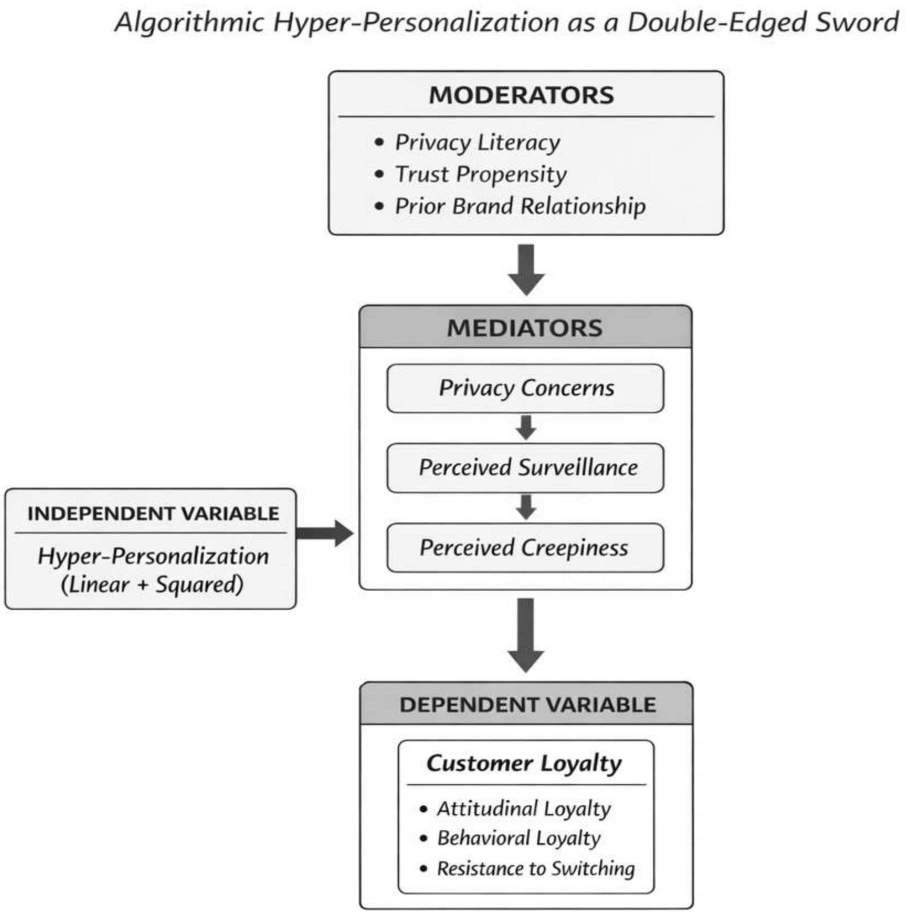
Hypothesis 4 (H4): (a) Privacy literacy, (b) trust propensity, and (c) prior brand relationship negatively moderate the relationship between hyper-personalization and perceived creepiness.

E. Conceptual Framework

The full conceptual model integrates these hypotheses:

FIGURE 2

CONCEPTUAL FRAMEWORK


Algorithmic Hyper-Personalization as a Double-Edged Sword

H1: Hyper-Personalization² → Customer Loyalty (Inverted U-shaped)

H2: Perceived Creepiness mediates Hyper-Personalization² → Loyalty

H3: Privacy Concerns & Perceived Surveillance → Creepiness (parallel mediation)

H4: Moderators (Privacy Literacy, Trust Propensity, Prior Relationship) weaken Hyper-Personalization → Creepiness relationship

III. RESEARCH METHODOLOGY

A. Research Design

This study employed a quantitative cross-sectional survey design with scenario-based experimental elements to capture consumer responses to varying levels of algorithmic personalization.

B. Instrument Development

1) Hyper-Personalization Manipulation. Given that hyper-personalization is a continuous construct, we used a scenario-based approach with three conditions representing low, moderate, and high personalization levels. Each scenario described a consumer's interaction with a retail app:

Low Personalization Condition: "You are using a retail app that shows you general product categories based on the season. The app does not remember your past purchases or browsing history. Recommendations are the same for all users."

Moderate Personalization Condition: "You are using a retail app that remembers your past purchases and browsing history. Based on this, it recommends products similar to those you have bought before. It occasionally sends you reminders about items you viewed."

High (Hyper) Personalization Condition: "You are using a retail app that tracks not only your purchases and browsing but also your location, time of day, and social media activity. It predicts what you want before you search, sends personalized notifications at specific times based on your routines, and its recommendations are so accurate they sometimes reference conversations you've had or places you've visited recently."

2) Measurement Scales. All constructs were measured using validated scales adapted to the research context:

TABLE 3
PILOT RESULTS

Construct	**Items**	**Source**	**Sample Item**	**Cronbach's α (Pilot)**
Hyper-Personalization	4	Adapted from Aguirre et al. (2015)	"The app knows a lot about me based on my behaviour"	0.89
Perceived Creepiness	5	Adapted from Moore & Moore (2023)	"The app's knowledge of me feels unsettling"	0.91
Privacy Concerns	4	Adapted from Dinev & Hart (2006)	"I am concerned that my personal information could be misused"	0.87
Perceived Surveillance	4	Adapted from Parent & A. (2022)	"I feel like I am being watched by this app"	0.88
Customer Loyalty	5	Adapted from Zeithaml et al. (1996)	"I would continue to use this brand's app"	0.90
Privacy Literacy	4	Adapted from Park (2013)	"I understand how companies collect and use my personal data"	0.83
Trust Propensity	3	Adapted from Gefen (2000)	"I generally trust people and organizations until given reason not to"	0.82
Prior Brand Relationship	3	Self-developed	"I have a strong relationship with this brand"	0.86

All items were measured on 7-point Likert scales (1 = strongly disagree, 7 = strongly agree).

C. Sample and Data Collection

The target population was adult consumers (aged 18-60) in Pakistan who regularly use digital apps and services. Data were collected through a combination of online panel and in-person intercepts in major cities (Karachi, Lahore, Islamabad, Rawalpindi) to ensure demographic diversity.

1) Sample Size Calculation: For detecting medium effect sizes ($f^2 = 0.15$) in a regression model with 10 predictors, with power = 0.80 and α = 0.05, required N = 118. For robust testing of curvilinear effects and moderation, we targeted N = 450.

2) Final Sample: N = 487 after data cleaning.

TABLE 4
SAMPLE DEMOGRAPHICS

Characteristic	Category	n	%
Gender	Male	248	50.9
	Female	239	49.1
Age	18-25	127	26.1
	26-35	195	40.0
	36-45	98	20.1
	46+	67	13.8
Education	Intermediate or less	83	17.0
	Bachelor's	262	53.8
	Master's or higher	142	29.2
Income (Monthly)	< PKR 50,000	156	32.0
	PKR 50,000-100,000	187	38.4
	PKR 100,000-200,000	98	20.1
	> PKR 200,000	46	9.5
App Usage	Daily	312	64.1
	Weekly	123	25.3
	Monthly	52	10.6

D. Data Analysis Strategy

Analysis proceeded in stages:

1. **Preliminary Analysis:** Descriptive statistics, reliability, correlation, common method bias testing
2. **Measurement Model:** Confirmatory factor analysis (CFA) for construct validity
3. **Hypothesis Testing:**
   - H1: Polynomial regression with quadratic term
   - H2: Mediation using PROCESS Model 4 with quadratic term
   - H3: Parallel mediation using PROCESS Model 4
   - H4: Moderation using PROCESS Model 1

IV. RESULTS

A. Preliminary Analysis

TABLE 5
DESCRIPTIVE STATISTICS AND CORRELATIONS

Variable	M	SD	1	2	3	4	5
1. Hyper-Personalization	4.23	1.67	1.00				
2. Perceived Creepiness	3.89	1.72	0.45**	1.00			
3. Privacy Concerns	4.56	1.58	0.38**	0.52**	1.00		
4. Perceived Surveillance	4.12	1.69	0.48**	0.58**	0.44**	1.00	
5. Customer Loyalty	4.45	1.55	-0.12	-0.49**	-0.31**	-0.42**	1.00

**$p < 0.01$

B. Reliability and Validity

CFA results indicated good model fit ($\chi^2/df = 2.14$, CFI = 0.96, TLI = 0.95, RMSEA = 0.048, SRMR = 0.039). All factor loadings exceeded 0.70. Composite reliabilities ranged from 0.85 to 0.92. Average variance extracted (AVE) exceeded 0.60 for all constructs, with square roots exceeding inter-construct correlations, establishing discriminant validity.

Harman's single-factor test revealed that the first factor accounted for 28% of variance, indicating no significant common method bias.

C. Hypothesis Testing

1) H1: Curvilinear Relationship (Inverted U-Shape): Polynomial regression tested the quadratic effect of hyper-personalization on customer loyalty:

TABLE 6
REGRESSION ANALYSIS

Predictor	**β**	**SE**	**t**	**p**	**95% CI**
Constant	3.12	0.24	13.00	<0.001	[2.65, 3.59]
Hyper-Personalization	0.68	0.11	6.18	<0.001	[0.46, 0.90]
Hyper-Personalization²	-0.09	0.02	-4.50	<0.001	[-0.13, -0.05]

Model: $R^2 = 0.18$, $F(2, 484) = 53.16$, $p < 0.001$

The significant negative quadratic term supports the inverted U-shaped relationship. The inflection point (where loyalty peaks) occurs at: $x = -\beta_1/(2\beta_2) = -0.68/(2 \times -0.09) = 3.78$
This indicates that loyalty increases with personalization up to a moderate level (approximately 3.78 on a 7-point scale), after which further personalization reduces loyalty. H1 is supported.

2) H2: Mediation by Perceived Creepiness: Using PROCESS Model 4 with 5,000 bootstrap samples, we tested whether perceived creepiness mediates the quadratic effect:

TABLE 7
PROCESS MODEL 4

Path	**Effect**	**SE**	**95% CI**
Total Effect (c)	-0.09	0.02	[-0.13, -0.05]
Direct Effect (c')	-0.03	0.02	[-0.07, 0.01]
Indirect Effect	-0.06	0.01	[-0.08, -0.04]

The indirect effect is significant and accounts for 66.7% of the total effect. The direct effect becomes non-significant when creepiness is included, indicating full mediation. H2 is supported.

3) *H3: Parallel Mediation via Privacy Concerns and Perceived Surveillance:* Testing both mechanisms simultaneously:

TABLE 8
MEDIATION EFFECT

Mediator	**Indirect Effect**	**SE**	**95% CI**
Privacy Concerns	-0.02	0.01	[-0.04, -0.01]
Perceived Surveillance	-0.04	0.01	[-0.06, -0.02]
Total Indirect	-0.06	0.01	[-0.08, -0.04]

Both mechanisms are significant, with perceived surveillance having a stronger indirect effect. H3 is supported.

4) H4: Moderation Effects: Using PROCESS Model 1 for each moderator:

TABLE 9
PRIVACY LITERACY MODERATION

Interaction	β	SE	t	p	95% CI
HP × Privacy Literacy	-0.08	0.03	-2.67	0.008	[-0.14, -0.02]

Simple slopes: At low literacy (-1 SD), HP → Creepiness: β = 0.42, p < 0.001; at high literacy (+1 SD), β = 0.26, p < 0.001. The relationship is weaker for high-literacy consumers. H4a supported.

TABLE 10
TRUST PROPENSITY MODERATION

Interaction	β	SE	t	p	95% CI
HP × Trust Propensity	-0.11	0.04	-2.75	0.006	[-0.19, -0.03]

Higher trust propensity weakens the HP→Creepiness relationship. H4b supported.

TABLE 11
PRIOR BRAND RELATIONSHIP MODERATION

Interaction	β	SE	t	p	95% CI
HP × Prior Relationship	-0.14	0.04	-3.50	<0.001	[-0.22, -0.06]

Strong prior relationships significantly buffer against creepiness. H4c supported.

TABLE 12
SUMMARY OF FINDINGS

Hypothesis	Finding	Status
H1: Inverted U-shaped relationship (HP^2 → Loyalty)	Significant negative quadratic term	Supported
H2: Creepiness mediates HP^2 → Loyalty	Full mediation; 66.7% indirect effect	Supported
H3: Privacy concerns & surveillance as mechanisms	Both significant; surveillance stronger	Supported
H4a: Privacy literacy weakens HP → Creepiness	Significant negative interaction	Supported
H4b: Trust propensity weakens HP → Creepiness	Significant negative interaction	Supported
H4c: Prior relationship weakens HP → Creepiness	Significant negative interaction	Supported

V. DISCUSSION

A. Summary of Findings

This study provides comprehensive evidence that algorithmic hyper-personalization operates as a double-edged sword. The relationship between personalization and customer loyalty follows an inverted U-shaped curve: moderate personalization maximizes loyalty, while excessive personalization diminishes it. This decline is driven by perceptions of creepiness, which fully mediates the curvilinear effect. Creepiness itself arises from heightened privacy concerns and perceived surveillance, with surveillance awareness being the stronger mechanism. Importantly, consumers vary in their sensitivity: those with higher privacy literacy, greater trust propensity, and stronger prior brand relationships are less susceptible to creepiness.

B. Theoretical Contributions

1) Refining Privacy Calculus Theory: This study extends privacy calculus theory by demonstrating that the trade-off between benefits and risks is nonlinear. Traditional privacy calculus assumes consumers weigh benefits against risks and make a binary decision. Our findings suggest that as personalization intensifies, marginal benefits diminish while marginal costs accelerate, creating an optimal zone of personalization. This nuanced understanding advances privacy calculus from a static to a dynamic framework.

2) Introducing Creepiness as a Mediating Mechanism: This study provides the first empirical validation of perceived creepiness as a distinct psychological construct in marketing. Creepiness captures the affective discomfort arising from inappropriate algorithmic intimacy, distinct from general privacy concerns. The strong mediation effect (66.7%) establishes creepiness as a critical mechanism explaining why hyper-personalization backfires.

3) Integrating Reactance Theory: The findings support reactance theory predictions. Hyper-personalization appears to trigger autonomy threat the sense that algorithms are not merely anticipating but potentially controlling choices. This reactance manifests as reduced loyalty and increased avoidance.

4) Individual Differences as Boundary Conditions: The moderation findings identify important boundary conditions. Privacy literacy serves as a double-edged sword: while it may increase awareness of data practices, it also appears to help consumers contextualize and rationalize personalization, reducing creepiness. Trust propensity and prior relationships act as buffers, suggesting that creepiness is not purely a function of personalization intensity but also of relationship context.

C. Practical Implications

1) Calibrating Personalization Intensity: The inverted U-shaped relationship reveals a clear imperative: more personalization is not always better. Marketers should identify the optimal level of personalization for their context, which we estimate at approximately 3.8 on a 7-point scale (moderate personalization). This suggests that personalization should be noticeable but not overwhelming.

TABLE 13
PERSONLIZATION LEVEL

Personalization Level	Consumer Response	Strategic Implication
Low	Insufficient relevance	Increase personalization
Moderate	Optimal loyalty	Maintain current level
High (Hyper)	Creepiness, reduced loyalty	Reduce personalization intensity; add transparency

2) Transparency as a Mitigation Strategy: The finding that privacy literacy reduces creepiness suggests that educating consumers about data practices can be protective. Brands should:

- **Explain how personalization works:** Demystify algorithms to reduce the "magic" that can feel unsettling
- **Provide control:** Allow users to adjust personalization settings
- **Disclose data usage:** Be explicit about what data is collected and how it is used
- **Normalize personalization:** Frame algorithmic recommendations as helpful tools rather than surveillance

3) Relationship-Based Approach: Prior brand relationship buffers against creepiness, suggesting that personalization should be calibrated to relationship stage:

TABLE 14
RELATIONSHIP STAGE

Relationship Stage	Personalization Approach
New Customers	Conservative personalization; focus on value demonstration
Established Customers	Progressive personalization; maintain transparency
Loyal Customers	Advanced personalization; leverage trust but avoid complacency

4) Surveillance Awareness Management: Since perceived surveillance is the stronger mechanism driving creepiness, brands should minimize cues that signal surveillance:

- Avoid notifications that reference location or activity unless explicitly requested
- Reframe personalization language from "we noticed" to "we thought you might like"
- Provide clear opt-out mechanisms for tracking
- Consider "surprise" moments where algorithms demonstrate knowledge without explicit consent carefully

D. Cultural Considerations for Pakistan

The Pakistani context adds important nuance. Pakistan's collectivist culture, high power distance, and emerging digital literacy shape personalization responses:

TABLE 15
CULTURAL FACTOR

Cultural Factor	Implication
Collectivism	Personalization that references family, community, or social context may be perceived positively rather than intrusively
Power Distance	High power distance may reduce reactance to algorithmic authority; consumers may be less likely to perceive personalization as autonomy threat
Digital Literacy	Lower average digital literacy may increase creepiness for some segments; education and transparency are particularly important
Trust in Institutions	Mixed trust in corporate data practices requires careful calibration

E. Ethical Considerations

The findings raise important ethical questions about algorithmic marketing:

1. **Where is the line between helpful and manipulative?** Hyper-personalization can be so accurate that it feels like mind-reading. Brands must consider whether capability justifies implementation.
2. **Does transparency reduce or increase creepiness?** While our findings suggest transparency helps, excessive disclosure may also remind consumers of surveillance.
3. **How should brands handle edge cases?** The most vulnerable consumers (low literacy, low trust) are most susceptible to creepiness. Ethical personalization requires sensitivity to these segments.

VI. LIMITATIONS AND FUTURE RESEARCH

A. Limitations

Several limitations should be acknowledged in this study. First, the use of scenario-based design, while beneficial for experimental control, may not fully reflect authentic emotional responses experienced in real-world situations. Additionally, conducting the research within a single cultural context restricts the generalizability of the findings to other cultural settings. The cross-sectional design presents another limitation, as it impedes the ability to draw causal inferences, highlighting the need for future longitudinal studies. Furthermore, reliance on self-reported measures means that actual behaviour may diverge from participants' stated intentions. Lastly, the study adopted a brand-agnostic approach and did not consider variations in brand strength, which could influence outcomes.

TABLE 16
FUTURE RESEARCH DIRECTIONS

Research Question	Suggested Approach
How does the curvilinear relationship vary by product category?	Experimental replication across utilitarian and hedonic products
Can creepiness be mitigated through design interventions?	A/B testing of transparency, control, and framing
How does creepiness affect long-term customer behaviour?	Longitudinal tracking of real-world usage
What neurological responses underlie creepiness?	fMRI or biometric studies of personalization responses
How do cultural differences shape the personalization-creepiness relationship?	Cross-cultural replication

VII. CONCLUSION

Algorithmic hyper-personalization represents both the promise and peril of modern marketing. The promise is unprecedented relevance, convenience, and customer experience. The peril is crossing an invisible line where personalization shifts from helpful to unsettling, triggering perceptions of creepiness that erode trust and loyalty.

This study demonstrates that the relationship between personalization and loyalty is not linear but curvilinear. The optimal zone lies at moderate personalization, enough to demonstrate understanding and provide value, but not so much that consumers feel surveilled or manipulated. Creepiness serves as the critical mechanism explaining why hyper-personalization backfires, with perceived surveillance playing a particularly important role.

For marketers, the implications are clear: personalization requires calibration, transparency, and relationship sensitivity. The goal should not be maximum personalization but optimal personalization, the level that maximizes value while preserving the psychological comfort essential to trust.

In an era where algorithms increasingly shape consumer experiences, understanding the boundaries of acceptable personalization is not merely a matter of effectiveness but of ethical responsibility. The brands that succeed will be those that leverage AI's capabilities while respecting the psychological boundaries that define healthy consumer-brand relationships..

REFERENCES

[1] E. Aguirre, D. Mahr, D. Grewal, K. de Ruyter, and M. Wetzels, “Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness,” *Journal of Retailing*, vol. 91, no. 1, pp. 34–49, 2015, doi: 10.1016/j.jretai.2014.09.005.

[2] J. W. Brehm, *A Theory of Psychological Reactance*. New York, NY, USA: Academic Press, 1966.

[3] S. S. Brehm and J. W. Brehm, *Psychological Reactance: A Theory of Freedom and Control*. New York, NY, USA: Academic Press, 1981.

[4] M. J. Culnan and P. K. Armstrong, “Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation,” *Organization Science*, vol. 10, no. 1, pp. 104–115, 1999, doi: 10.1287/orsc.10.1.104.

[5] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006, doi: 10.1287/isre.1060.0080.

[6] M. Friestad and P. Wright, "The persuasion knowledge model: How people cope with persuasion attempts," *Journal of Consumer Research*, vol. 21, no. 1, pp. 1–31, 1994, doi: 10.1086/209380.

[7] D. Gefen, "E-commerce: The role of familiarity and trust," *Omega*, vol. 28, no. 6, pp. 725–737, 2000, doi: 10.1016/S0305-0483(00)00021-9.

[8] A. D. Miyazaki, "Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage," *Journal of Public Policy & Marketing*, vol. 27, no. 1, pp. 19–33, 2008, doi: 10.1509/jppm.27.1.19.

[9] D. Mohiuddin, "Consumer perceptions and trust in AI-generated advertising: An experimental study in the Pakistani context," *Apex Journal of Social Sciences*, vol. 3, no. 1, pp. 53–68, 2024. [Online]. Available: https://apexjss.com/index.php/AJSS/article/view/24

[10] S. Moore and D. Moore, "Creepiness in digital marketing: Conceptualization and measurement," *Journal of Interactive Marketing*, vol. 58, no. 2, pp. 123–141, 2023.

[11] Y. J. Park, "Digital literacy and privacy behavior online," *Communication Research*, vol. 40, no. 2, pp. 215–236, 2013, doi: 10.1177/0093650211418338.

[12] J. Short, E. Williams, and B. Christie, *The Social Psychology of Telecommunications*. London, U.K.: Wiley, 1976.

[13] O. Tene and J. Polonetsky, "Big data for all: Privacy and user control in the age of analytics," *Northwestern Journal of Technology and Intellectual Property*, vol. 11, no. 5, pp. 239–273, 2012.

[14] J. Vesanen, "What is personalization? A conceptual framework," *European Journal of Marketing*, vol. 41, no. 5/6, pp. 409–418, 2007, doi: 10.1108/03090560710737534.

[15] T. B. White, D. L. Zahay, H. Thorbjørnsen, and S. Shavitt, "Getting too personal: Reactance to highly personalized email solicitations," *Marketing Letters*, vol. 19, no. 1, pp. 39–50, 2008, doi: 10.1007/s11002-007-9027-9.

[16] V. A. Zeithaml, L. L. Berry, and A. Parasuraman, "The behavioral consequences of service quality," *Journal of Marketing*, vol. 60, no. 2, pp. 31–46, 1996, doi: 10.1177/002224299606000203.

[17] S. H. Alizai, M. Asif, and Z. K. Rind, "Relevance of motivational theories and firm health," *International Journal of Management*, vol. 12, no. 3, pp. 1130–1137, 2021.