Sarcouncil Journal of Entrepreneurship and Business Management

ISSN(Online): 2945-3720

Volume- 05| Issue- 11| 2026

Research Article **Received:** 15-10-2026 | **Accepted:** 10-11-2026 | **Published:** 24-11-2026

Personalization, Privacy and Consumer Trust in Digital Marketing: An Integrative Framework for Data-Driven Customer Relationships

Ashish Kumer Ghosh

Department of Marketing, Australian National Institute of Management and Commerce (IMC) Perth 6000, Australia.

Abstract: Digital marketing depends on personal data. Firms use browsing records, purchase histories and profile information to tailor offers, and consumers value relevance but worry about how much is known about them. Research on this tension has grown in separate streams, with marketing studies on privacy practices, information systems studies on the privacy calculus and behavioural studies on how privacy choices are made. This paper brings them together. Drawing on an integrative review of work in marketing, information systems and consumer psychology, it develops a framework in which a firm's personalization and privacy practices shape consumers' perceived benefit and perceived privacy risk, which act on trust and through trust on purchase intention, loyalty and advocacy. Seven propositions specify the roles of contextual fit, control-giving practices, transparency, prior experience of intrusive targeting and managerial adoption of privacy-protective practices. The framework adds a managerial adoption layer, taken from technology acceptance research, to the consumer-side literature, and it states boundary conditions in a form that can be tested. A mixed-methods agenda is proposed, combining a survey analysed with partial least squares structural equation modelling, a controlled experiment and interviews with marketing managers. The paper offers practical guidance on how much to personalize, how much control to give and how to disclose data practices in a way that builds trust.

Keywords: Personalization; privacy; consumer trust; digital marketing; buyer behaviour; data-driven marketing; e-commerce.

INTRODUCTION

Digital marketing runs on personal data. Retailers follow browsing and purchase histories to tailor offers, advertisers match messages to profiles, and platforms adjust what each user sees. Consumers gain when the result is relevant, and many accept some data collection in return. The same practices can also leave consumers feeling watched. Dwivedi *et al.,* (2021) observe that the internet and social media have changed consumer behaviour and the way companies do business, and they list ethical issues among the topics that need further study. Bleier *et al.,* (2020) treat consumer privacy and data-based innovation in marketing as linked questions.

Research on this tension has developed in separate streams. Marketing work examines how privacy practices affect customer and firm performance (Martin *et al.,*, 2017; Martin & Murphy, 2017). Information systems work examines the privacy calculus, in which consumers weigh the benefits of disclosure against its risks (Dinev & Hart, 2006; Smith *et al.,*, 2011), and it asks how transparency shapes willingness to be profiled (Awad & Krishnan, 2006). Behavioural work shows that privacy preferences depend on context and are easily shifted (Acquisti *et al.,*, 2015). Measurement work treats privacy concern as a multidimensional construct (Malhotra *et al.,*, 2004), and Nissenbaum (2004) supplies the idea of contextual integrity, under which information flows should match the norms of the setting in which they occur. Each stream explains part of the picture. Few studies integrate the firm's data practices, the consumer's perceptions and the trust that follows into one connected chain, and fewer still ask whether managers will actually adopt the practices that the evidence recommends.

This paper treats data-driven personalization as a chain of linked decisions. The firm decides how much data to collect and use, how much control to give consumers and how openly to disclose what it does. Those choices shape how the consumer judges the personalized offer, in particular how useful it seems and how risky. The judgement feeds trust, and trust feeds purchase and loyalty, which return to the firm as further data. Seen this way, personalization is a decision about information as well as a marketing tactic, which brings it within the scope of information management and data-driven decision-making.

Three research questions guide the paper. RQ1: How do a firm's personalization and privacy practices shape consumers' perceptions of benefit and risk? RQ2: Through which mechanism do those perceptions reach purchase intention and loyalty? RQ3: Which conditions strengthen or weaken that path, including the extent to which managers adopt privacy-protective practices?

The paper makes three contributions. It links firm-side practices and consumer-side perceptions in a single chain. It adds a managerial adoption layer,

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Ashish Kumer Ghosh

DOI-https://doi.org/10.5281/zenodo.24492292

drawn from technology acceptance research, to explain why privacy-protective practices are applied unevenly across firms. And it states seven propositions, with their boundary conditions, in a form that can be tested with the design set out in Section 6. The rest of the paper reviews the background literature, explains the review approach, presents the framework and propositions, discusses implications, and sets out a research agenda.

THEORETICAL BACKGROUND

Personalization as an Information Decision

Decision-making research has long held that people choose under limits on information, time and attention (Simon, 1955). Personalization responds to those limits on the consumer side by turning a large assortment into a short list of relevant options. On the firm side it responds by turning behavioural data into decisions about what to show, to whom and when. Both parties decide with incomplete information, and each depends on what the other discloses. The consumer decides how much to reveal, and the firm decides how much to ask for and how to use it.

Dwivedi *et al.,* (2021) bring together expert views on digital and social media marketing. They conclude that online channels have altered consumer behaviour and firm practice, and they include mobile marketing, electronic word of mouth and ethical issues among the areas that need more research. Martin and Murphy (2017) review the role of data privacy in marketing and set out an agenda for the field, while Bleier *et al.,* (2020) discuss how consumer privacy concerns and privacy regulation bear on data-based innovation in marketing. Together these works frame the problem as one that firms cannot leave to the legal department. How a firm collects and uses data is part of how it markets.

Privacy Concerns, the Calculus and the Paradox

Smith *et al.,* (2011) review information privacy research across disciplines and organize it as a sequence running from the antecedents of privacy concern to its outcomes. Within that sequence, the privacy calculus is the most widely used idea in e-commerce research. Dinev and Hart (2006) extend the calculus for e-commerce transactions, in which consumers weigh the benefits of disclosing information against its risks. The idea is simple, and it fits personalization well because the benefit and the risk come from the same data. Xu *et al.,* (2011) extend the calculus to location-aware marketing and report that personalization shapes risk and benefit beliefs differently depending on whether it is covert or overt. Kokolakis (2017) reviews the privacy paradox literature and attributes its mixed findings to differences in methods, contexts and definitions.

Fairness and transparency enter this calculus. Culnan and Armstrong (1999) studied how perceived procedural fairness in a firm's information practices relates to privacy concerns and trust, and Awad and Krishnan (2006) examined information transparency and consumers' willingness to be profiled online for personalization. Acquisti *et al.,* (2015) add a behavioural warning. They describe privacy preferences as context dependent and malleable, so what consumers say they want and what they do can diverge, and small changes in how a request is framed can shift the outcome. The so-called personalization-privacy paradox, in which consumers value tailoring yet resist the data collection behind it, is better read as a product of these features than as plain inconsistency. Brandimarte *et al.,* (2013) add a caution about control: giving people more perceived control over their information can make them more willing to disclose sensitive information, which may leave them more exposed.

Control, Transparency and Personalization Outcomes

A smaller group of studies asks what firms can do about the tension. Tucker (2014) reports a field experiment on a social network in which giving users more control over their personal information made personalized advertising more effective. Aguirre *et al.,* (2015) examine how information collection and trust-building strategies shape the effectiveness of personalized online advertising. Martin *et al.,* (2017) examine how firms' data privacy practices affect customer and firm performance, with customers' sense of vulnerability and control at the centre of the account. Tam and Ho (2006) found that web users are receptive to personalized content and use it as an aid to decisions, while White *et al.,* (2008) show that highly personalized email solicitations can provoke reactance. The common thread is that personalization works better when consumers feel the firm is open about what it does and leaves them some say.

Read together, the privacy calculus and transparency studies point the same way. The calculus implies that the effect of personalization

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

on trust depends on the balance between perceived benefit and perceived privacy risk (Dinev & Hart, 2006), and transparency about how data will be used shapes consumers' willingness to accept that trade (Awad & Krishnan, 2006). How data are gathered, and whether consumers feel the firm has been open about it, in turn shapes how far trust extends (Aguirre *et al.*,, 2015; Martin *et al.*,, 2017). On this reading, trust in a personalizing firm is better treated as a judgement that consumers revise in the light of experience than as a fixed attitude, a point developed in Section 4.3.

Trust, Relationship Marketing and Managerial Adoption

Trust is the hinge between what a firm does with data and what consumers do next. Mayer *et al.*, (1995) define trust as the willingness of one party to be vulnerable to the actions of another and identify ability, benevolence and integrity as the characteristics that drive it. Morgan and Hunt (1994) place trust and commitment at the centre of relationship marketing and treat them as mediating variables between relationship investments and cooperative outcomes. In online shopping, Gefen *et al.*, (2003) integrated trust with technology acceptance and showed that trust matters for purchase intention alongside perceived usefulness and ease of use. Personalization asks the consumer to be vulnerable in a specific way by sharing data and acting on tailored suggestions, so these ideas apply directly.

The firm side has its own adoption problem. Davis (1989) showed that perceived usefulness and perceived ease of use shape the acceptance of information technology, and Venkatesh *et al.*, (2003) later brought earlier models together in a unified account that adds social influence and facilitating conditions. Research on personalization and privacy has paid little attention to this layer, yet it matters. Two firms may adopt the same privacy policy on paper and apply it very differently because one set of managers sees the practices as useful and workable while the other treats them as a compliance burden. In integrated marketing communications the problem is sharper, because consumers meet the firm across email, web, mobile and social channels, and a privacy promise made in one channel and ignored in another damages trust in all of them.

REVIEW APPROACH

The paper follows an integrative conceptual review approach. The aim is to build a framework and derive testable propositions, so the review is selective and argument-driven rather than an attempt to estimate average effect sizes. Sources were identified primarily from leading marketing journals (Journal of Marketing, Journal of the Academy of Marketing Science, Journal of Retailing, International Journal of Research in Marketing, Journal of Marketing Research), information systems journals that address privacy, trust and technology acceptance (MIS Quarterly, Information Systems Research), and behavioural science outlets. Key search terms included combinations of personalization, privacy, consumer trust, transparency, privacy paradox and technology acceptance. A source was retained when it was peer reviewed, offered either an explicit framework or empirical evidence, and bore directly on a firm's data practices or on a consumer response to them. No formal systematic search protocol or quality appraisal checklist was applied, and the selection reflects the author's judgement of theoretical relevance. This limitation is acknowledged in Section 7.

Constructs and relationships were extracted from each source and mapped onto the chain of decisions described in the introduction. A proposition was written when at least one well-cited study supplied a mechanism and at least one further source supported the direction of the effect. Where the evidence rests on a single platform or setting, the proposition is stated as a conditional and flagged for wider testing.

CONCEPTUAL FRAMEWORK AND PROPOSITIONS

Figure 1 summarizes the framework. A chain of effects runs from firm data practices to consumer perceptions, from perceptions to trust and from trust to buyer behaviour, and three moderators condition it. Firm data practices comprise collection and use practices, namely the depth and contextual fit of personalization, and control-giving practices, namely the control offered to consumers over what is collected and how it is used. These practices shape two consumer perceptions, perceived personalization benefit and perceived privacy risk. Both perceptions act on consumer trust, and trust then shapes buyer behaviour. Transparency about data collection and use is treated separately from these practices: it is modelled not as an antecedent of the perceptions but as a moderator. Transparency and prior negative privacy experience condition the paths from perception to trust. Managerial adoption, in turn, moderates the paths from firm data practices

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

to consumer perceptions (P1 and P2), because it determines whether privacy-protective and control-giving practices are implemented as intended; it is not treated as a separate antecedent of those practices.

Key constructs are defined as follows. Personalization depth is the extent to which a firm uses individual-level data to tailor an offer, and contextual fit is the degree to which that use matches what the consumer would expect in the situation at hand. Expectations concern not only how much data is used but also its provenance (whether it was supplied by the consumer or obtained elsewhere), whether it is used across contexts or shared with third parties, and whether the firm relies on attributes it has inferred rather than ones the consumer disclosed. Control-giving practices are the mechanisms through which a firm lets consumers shape collection and use, such as opt-outs, access to and deletion of personal data, and preference settings. Perceived personalization benefit is the consumer's belief that the offer is relevant and saves effort. Perceived privacy risk is the consumer's expectation of harm or loss of control arising from the firm's use of personal data. Perceived control is the consumer's belief that they can shape what is collected and how it is used. Transparency covers disclosure of what data are collected, how they are used and with whom they are shared. Prior negative privacy experience is a consumer's earlier exposure to intrusive or poorly targeted personalization. Implementation fidelity is the degree to which privacy-protective and control-giving practices are applied as designed and consistently across channels. Consumer trust is understood in the sense of Mayer *et al.*, (1995) as willingness to be vulnerable, encompassing perceptions of ability, benevolence and integrity. The framework treats trust primarily as an overall judgement while recognizing these dimensions.

The framework is presented as a linear chain for clarity. In practice, buyer behaviour feeds data back to the firm, creating the possibility of learning, trust repair and revised practices over time. Modelling this feedback loop is left for future research.

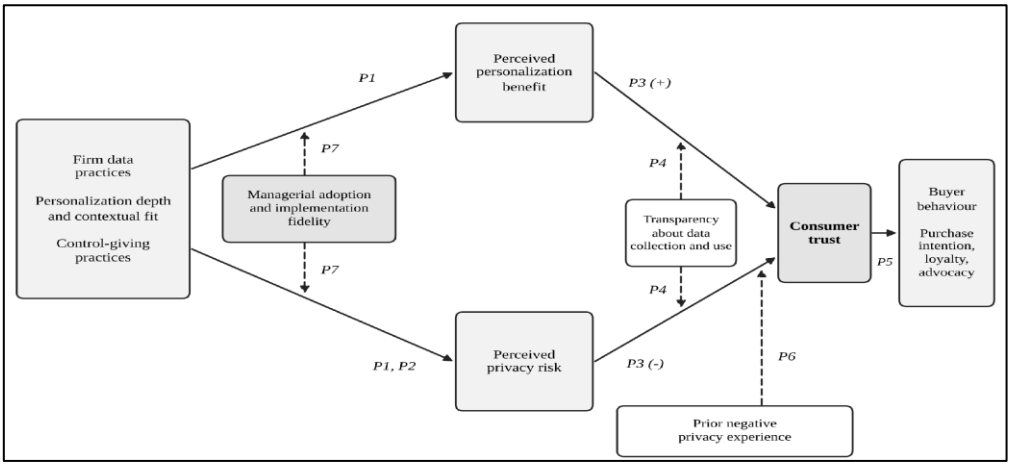

Figure 1. Conceptual framework of personalization, privacy and consumer trust in digital marketing.

Solid arrows show direct effects; dashed arrows show moderation. Managerial adoption and implementation fidelity (P7) moderate the paths from firm data practices to consumer perceptions (P1 and P2); they are not a direct antecedent of firm data practices. Perceived control is the mechanism through which control-giving practices lower perceived privacy risk (P2). Transparency (P4) moderates both perception-to-trust paths, and prior negative privacy experience (P6) moderates the perceived privacy risk-to-trust path.

Firm Data Practices

The privacy calculus implies that benefit and risk rise together with the amount of data used (Dinev & Hart, 2006). The behavioural evidence adds that the weight consumers give to each depends on context (Acquisti *et al.,* 2015). A recommendation based on items a shopper has just viewed on the same site is likely to feel natural. The same recommendation based on data bought from a third party, or on activity in another setting, may feel like surveillance, and so may an offer that reveals an attribute the consumer never disclosed but the firm has inferred. Contextual fit, including where the data came from and how it was derived, therefore matters as much as depth. Lambrecht and Tucker (2013) report that product-specific retargeted advertisements performed worse than generic brand advertisements unless a consumer's browsing suggested that preferences had become

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

more specific, and Mothersbaugh *et al.,* (2012) examine the role of information sensitivity in online disclosure.

P1. *Perceived privacy risk increases when a firm's data collection and use exceed consumers' expectations for the context, in particular when personalization draws on data of unexpected provenance (for example data obtained from third parties rather than supplied by the consumer), uses data across contexts or shares it with third parties, or relies on attributes inferred rather than disclosed. When collection and use remain within those expectations, greater personalization depth is expected to increase perceived personalization benefit without a corresponding increase in perceived privacy risk.*

Control is the second practice. Tucker (2014) found that more control made personalized advertising more effective, and Martin *et al.,* (2017) place control and vulnerability at the centre of how data practices affect performance. Culnan and Armstrong (1999) point to fair procedures as a related route to lower concern.

P2. *Control-giving practices (for example opt-outs, access to and deletion of personal data, and preference settings) increase consumers' perceived control over their data. Perceived control in turn reduces perceived privacy risk and thereby supports consumer trust (P3), without reducing perceived personalization benefit. The effect is expected to be strongest when control is easy to exercise.*

Consumer Evaluation and Trust

Firm practices reach consumers as an experience, such as an offer that feels relevant or one that feels intrusive. Two perceptions carry most of the weight in the literature reviewed here, perceived personalization benefit and perceived privacy risk. Kim *et al.,* (2008) found that trust and perceived risk strongly shape consumers' purchase decisions and that privacy and security concerns affect trust in a website, and McKnight *et al.,* (2002) propose a multidimensional typology of trust measures for e-commerce.

P3. *Perceived personalization benefit increases consumer trust in the firm, while perceived privacy risk decreases it; the relative strength of these opposing effects determines overall trust. Both effects are expected to be conditioned by transparency (P4) and the risk effect by prior negative privacy experience (P6).*

Transparency is the lever most often proposed for tipping that balance (Awad & Krishnan, 2006; Martin *et al.,*, 2017). It is not a guaranteed remedy, because a long or vague disclosure can draw attention to data collection that consumers would otherwise ignore.

P4. *Transparency about data collection and use is expected to strengthen the positive effect of perceived personalization benefit on trust and to weaken the negative effect of perceived privacy risk on trust, particularly when disclosures are specific and credible. The effect is not automatic, and poorly designed transparency can heighten privacy salience.*

Trust matters because of what it produces. In commitment-trust theory, trust drives commitment and cooperative behaviour (Morgan & Hunt, 1994), and in the model of Mayer *et al.,* (1995), it determines willingness to accept vulnerability. In online shopping it works alongside usefulness and ease of use to shape purchase intention (Gefen *et al.,* 2003). In the present context it translates into willingness to share data, to act on tailored offers and to stay with the brand.

P5. *Consumer trust mediates the effects of perceived personalization benefit and perceived privacy risk on purchase intention, loyalty, and advocacy.*

Experience and Recalibration

Trust is not set once. Consumers carry what they learn from earlier encounters into later ones, and Aguirre *et al.,* (2015) show that how information is collected changes the way personalized advertising performs, with covert collection heightening consumers' sense of vulnerability. Martin *et al.,* (2017) likewise place vulnerability at the centre of how data practices affect customer responses. A consumer who has met an offer that seemed to know too much or that used information the consumer did not knowingly give has direct evidence that the risks of data use can materialize. For that consumer, a given level of perceived privacy risk is likely to weigh more heavily in the trust judgement than it would for a consumer without such an experience. Prior negative experience is therefore treated here as a condition that amplifies the link between perceived privacy risk and trust, rather than as a separate direct cause of lower trust.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

P6. *Prior negative privacy experience, meaning earlier exposure to intrusive or poorly targeted personalization, strengthens the negative effect of perceived privacy risk on consumer trust. The strengthening is expected to be greater when the consumer believes data were used beyond what they had agreed to. Visible control is proposed as one factor that may attenuate this amplification, although a prompt to adjust settings could also remind consumers of the data held about them. This element is flagged as speculative and a priority for experimental testing.*

Managerial Adoption

Everything above assumes that managers apply the practices as designed. Technology acceptance research suggests the assumption often fails. Perceived usefulness and ease of use shape acceptance (Davis, 1989), as do social influence and facilitating conditions (Venkatesh *et al.,*, 2003).

P7. *Managers' adoption of privacy-protective and control-giving practices, shaped by perceived usefulness, perceived ease of use, social influence and facilitating conditions, and the implementation fidelity with which those practices are applied, moderate the effects proposed in P1 and P2. The effects of firm data practices on consumer perceptions are expected to be stronger when adoption and implementation fidelity are high. Where adoption is low or practices are applied inconsistently across channels, the predicted effects are unlikely to materialize.*

Table 1. Summary of propositions

No.	Proposition (short form)	Key constructs	Main anchoring sources
P1	Data collection and use that exceed contextual expectations (unexpected provenance, cross-context or third-party use, inferred attributes) raise perceived privacy risk; depth within expectations raises perceived benefit without matching risk	Personalization depth; contextual fit; data provenance; cross-context/third-party use; inferred attributes; perceived benefit; perceived privacy risk	Dinev & Hart (2006); Acquisti *et al.*, (2015); Aguirre *et al.*, (2015)
P2	Control-giving practices (opt-outs, data access/deletion, preference settings) increase perceived control, which reduces perceived privacy risk and supports trust without reducing perceived personalization benefit	Control-giving practices; perceived control; perceived privacy risk; perceived personalization benefit; trust	Tucker (2014); Martin *et al.*, (2017); Culnan & Armstrong (1999)
P3	Benefit raises trust; risk lowers it; the relative strength of these opposing effects determines overall trust	Perceived benefit; perceived privacy risk; trust	Awad & Krishnan (2006); Dinev & Hart (2006); Culnan & Armstrong (1999)
P4	Transparency is expected to strengthen the benefit effect and weaken the risk effect when disclosures are specific and credible	Transparency about data collection and use	Awad & Krishnan (2006); Martin *et al.*, (2017); Culnan & Armstrong (1999)
P5	Trust mediates effects on purchase intention, loyalty and advocacy	Trust; purchase intention; loyalty; advocacy	Morgan & Hunt (1994); Mayer *et al.*, (1995); Gefen *et al.*, (2003)
P6	Prior negative privacy experience strengthens the negative effect of perceived privacy risk on trust, more so when data were used beyond agreement; control may attenuate this amplification (speculative)	Prior negative privacy experience (moderator); perceived privacy risk; trust; data use beyond agreement; perceived control	Aguirre *et al.*, (2015); Martin *et al.*, (2017)
P7	Managerial adoption and implementation fidelity moderate the effects of firm data practices on consumer perceptions (P1, P2)	Usefulness; ease of use; social influence; facilitating conditions; implementation fidelity	Davis (1989); Venkatesh *et al.*, (2003)

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

DISCUSSION

Theoretical Implications

First, the framework links two literatures that rarely speak to each other. Marketing studies of data privacy usually take the firm's perspective, and information systems studies of the privacy calculus usually take the consumer's. The chain from practice to perception to trust to behaviour gives each a place and shows where evidence is missing.

Second, it treats contextual fit as a design variable. The calculus literature tends to speak of the amount of data used. The behavioural evidence suggests that the match between data use and context may matter as much as the amount, and P1 states that expectation in a testable form.

Third, it brings managerial adoption into the picture. A privacy practice that exists in a policy document has no effect on consumers until managers apply it, which is why P7 treats adoption and implementation fidelity as moderators of the practice-to-perception paths in P1 and P2.

Implications for Practice

Marketing leaders can use the framework as a working checklist. A first step is to map each personalization use against the context in which consumers meet it and ask whether the data used would be expected there. Uses that rely on data from other settings, or on inferences the consumer never supplied, are the strongest candidates for redesign or for explicit consent.

Control should come early and be easy to use. The evidence reviewed suggests that giving consumers a real say does not weaken personalization and may strengthen it (Tucker, 2014). The propositions also imply that telling consumers what data are used should help trust, provided the message is specific enough to be believed. Generic privacy statements are unlikely to do this work. At the same time, transparency is not costless. Disclosure can heighten privacy salience or produce transparency fatigue for some consumers, so firms should treat disclosure design as an empirical question rather than an automatic remedy. Firms should also treat intrusive or irrelevant offers as a trust signal. A small number of visible failures can matter more than a high average relevance score, so complaint review and quick correction belong in the operating process.

Adoption also requires investment. Training, workflow integration and clear accountability for data practices address the facilitating conditions that technology acceptance research identifies as important (Venkatesh *et al.,* 2003). Consistency across channels deserves particular attention in integrated marketing communications. For brand and reputation management, it is plausible that trust in how a brand handles data cannot be separated from trust in the brand itself, since the integrity dimension in Mayer *et al.,* (1995) applies to how a firm treats personal information. That point is an argument developed here and has not been tested in the sources reviewed.

Governance and Regulation

Martin and Murphy (2017) and Bleier *et al.,* (2020) both place privacy regulation and consumer concern at the centre of the future of data-based marketing, and the expert contributions assembled by Dwivedi *et al.,* (2021) place ethical issues within the research agenda for digital marketing. Goldfarb and Tucker (2011) found that display advertising became less effective at raising stated purchase intent after European privacy laws limited data collection for targeting, so regulation also changes what personalization can achieve. The framework touches these issues in two places. Perceived privacy risk is a modelled construct in P3, and control-giving practices (P2) and transparency (P4) are the means through which firms can respond to regulation as well as to consumer concern. Formal governance, including periodic reviews of data use and records of consent, would give firms evidence that their stated practices are applied in fact. Regulatory regimes differ across jurisdictions, so firms that operate internationally cannot assume that one policy suits every market.

RESEARCH AGENDA AND PROPOSED EMPIRICAL DESIGN

The propositions can be tested with a combination of methods. A sequence of three studies is proposed.

Study 1 is a cross-sectional survey of online consumers who regularly receive personalized offers from retailers or platforms. Measures of perceived personalization benefit, perceived privacy risk, perceived control, transparency, trust, prior experience of intrusive targeting, purchase intention and loyalty would be adapted from validated scales. Partial least squares structural equation modelling is suitable for a model with multiple mediators and moderators (Hair *et al.,* 2019), and sample size would be determined by power analysis. This study can establish

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

associations and measurement properties for the consumer-side constructs (P1 to P6) but cannot support strong causal claims.

Study 2 is a between-subjects experiment in a simulated shopping environment. It manipulates the contextual fit of the data used for personalization (within or beyond what the shopper would expect), the availability of control (none or preference settings) and the specificity of the data explanation (generic or specific). A staged intrusive offer before the main task, crossed with these manipulations, allows a direct test of whether prior negative privacy experience strengthens the effect of perceived privacy risk on trust (P6). Random assignment supplies causal evidence on the consumer-side mechanisms in a retail setting. The design does not manipulate managerial adoption and therefore cannot test P7.

Study 3 comprises semi-structured interviews with marketing managers about how privacy and consent practices are decided, applied and monitored across channels, and about the barriers to applying them. These interviews inform the firm-side propositions (P1, P2 and P7), where quantitative evidence is currently thinnest. Interview insights can be paired with firm-level indicators such as consent rates, complaint volumes and campaign outcomes where available. Qualitative data alone cannot establish the statistical boundary-condition effects proposed in P7.

Two extensions would strengthen the program. The first is cross-national comparison. Attitudes to data sharing and the regulatory setting differ across markets, and the framework gives international marketing researchers a structure for testing such differences, particularly in emerging markets, which are underrepresented in the sources reviewed here. The second is a longitudinal design that follows consumers over repeated interactions, which would allow the feedback loop noted in Section 4 to be modelled.

LIMITATIONS

The paper is conceptual. The propositions come from a selective review and have not been tested, and the choice of sources reflects the author's judgement of theoretical relevance rather than a reproducible systematic protocol. Some of the empirical findings cited come from a single platform or setting, and their transfer to other channels and product categories remains an assumption that requires direct testing. The framework combines constructs that are each well studied but rarely modelled together, and interactions among them, for example between transparency and prior experience, may behave differently from the additive logic used here. Trust, transparency and control are multi-dimensional, yet the current propositions treat them primarily as overall constructs. Important boundary conditions are under-specified in the present model, including product category and perceived risk, brand reputation, consumer privacy literacy, cultural context and the regulatory environment. The proposed empirical agenda addresses some of these gaps but cannot test the full firm and consumer feedback loop in a single design.

CONCLUSION

This paper has treated personalization in digital marketing as a question of information and trust that spans the firm and the consumer. The framework proposes that contextual fit and control-giving practices shape how consumers weigh the benefit and the risk of personalized offers, that those perceptions reach buyer behaviour through trust, and that transparency and earlier experience condition that path. It adds that none of this reaches consumers unless managers apply the practices consistently and with fidelity. Seven propositions turn these claims into hypotheses for testing. For researchers, the agenda offers a route from conceptual argument to survey and experimental evidence. For practitioners, it offers a way to decide how much to personalize, how much control to give and how to speak about data in a way that keeps the trust on which personalization depends.

REFERENCES

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. "Privacy and human behavior in the age of information." *Science* 347.6221 (2015): 509-514.
2. Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. "Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness." *Journal of retailing* 91.1 (2015): 34-49.
3. Awad, N. F., & Krishnan, M. S. "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization1." *MIS quarterly* 30.1 (2006): 13-28.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

4. Bleier, A., Goldfarb, A., & Tucker, C. "Consumer privacy and the future of data-based innovation and marketing." *International Journal of Research in Marketing* 37.3 (2020): 466-480.
5. Brandimarte, L., Acquisti, A., & Loewenstein, G. "Misplaced confidences: Privacy and the control paradox." *Social psychological and personality science* 4.3 (2013): 340-347.
6. Culnan, M. J., & Armstrong, P. K. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation." *Organization science* 10.1 (1999): 104-115.
7. Davis, F. D. "Perceived usefulness, perceived ease of use, and user acceptance of information technology." *MIS quarterly* (1989): 319-340.
8. Dinev, T., & Hart, P. "An extended privacy calculus model for e-commerce transactions." *Information systems research* 17.1 (2006): 61-80.
9. Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., & Wang, Y. "Setting the future of digital and social media marketing research: Perspectives and research propositions." *International journal of information management* 59 (2021): 102168.
10. Gefen, D., Karahanna, E., & Straub, D. W. "Trust and tam in online shopping: An integrated model1." *MIS quarterly* 27.1 (2003): 51-90.
11. Goldfarb, A., & Tucker, C. E. "Privacy regulation and online advertising." *Management science* 57.1 (2011): 57-71.
12. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. "When to use and how to report the results of PLS-SEM." *European business review* 31.1 (2019): 2-24.
13. Kim, D. J., Ferrin, D. L., & Rao, H. R. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents." *Decision support systems* 44.2 (2008): 544-564.
14. Kokolakis, S. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon." *Computers & security* 64 (2017): 122-134.
15. Lambrecht, A., & Tucker, C. "When does retargeting work? Information specificity in online advertising." *Journal of Marketing research* 50.5 (2013): 561-576.
16. Malhotra, N. K., Kim, S. S., & Agarwal, J. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." *Information systems research* 15.4 (2004): 336-355.
17. Martin, K. D., Borah, A., & Palmatier, R. W. "Data privacy: Effects on customer and firm performance." *Journal of marketing* 81.1 (2017): 36-58.
18. Martin, K. D., & Murphy, P. E. "The role of data privacy in marketing." *Journal of the Academy of Marketing Science* 45.2 (2017): 135-155.
19. Mayer, R. C., Davis, J. H., & Schoorman, F. D. "An integrative model of organizational trust." *Academy of management review* 20.3 (1995): 709-734.
20. McKnight, D. H., Choudhury, V., & Kacmar, C. "Developing and validating trust measures for e-commerce: An integrative typology." *Information systems research* 13.3 (2002): 334-359.
21. Morgan, R. M., & Hunt, S. D. "The commitment-trust theory of relationship marketing." *Journal of marketing* 58.3 (1994): 20-38.
22. Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. "Disclosure antecedents in an online service context: The role of sensitivity of information." *Journal of service research* 15.1 (2012): 76-98.
23. Nissenbaum, H. "Privacy as contextual integrity." *Wash. L. Rev.* 79 (2004): 119.
24. Simon, H. A. "A behavioral model of rational choice." *The quarterly journal of economics* (1955): 99-118.
25. Smith, H. J., Dinev, T., & Xu, H. "Information privacy research: An interdisciplinary review1." *MIS quarterly* 35.4 (2011): 989-A27.
26. Tam, K. Y., & Ho, S. Y. "Understanding the impact of web personalization on user information processing and decision Outcomes1." *MIS quarterly* 30.4 (2006): 865-890.
27. Tucker, C. E. "Social networks, personalized advertising, and privacy controls." *Journal of marketing research* 51.5 (2014): 546-562.
28. Morris, M. G., Venkatesh, V., Davis, F. D., & Davis, G. B. "User acceptance of information technology: toward a unified view." *MIS quarterly* 27.3 (2003): 425.
29. White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. "Getting too personal: Reactance

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

to highly personalized email solicitations." *Marketing Letters* 19.1 (2008): 39-50.

30. Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing." *Decision support systems* 51.1 (2011): 42-52.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Ghosh, A. K. "Personalization, Privacy and Consumer Trust in Digital Marketing: An Integrative Framework for Data-Driven Customer Relationships" *Sarcouncil Journal of Entrepreneurship and Business Management* 5.11 (2026): pp 12-21.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher