Impact of AI-Driven Digital Marketing on Data Privacy and Consumer Behavior: An SEM Study

Asma Anjum and Manju Priya R***

AI-driven digital marketing has yielded both opportunities and obstacles, leading to its impact on consumer data privacy. While consumer data aids marketers in creating effective marketing strategies, it is imperative to ethically handle consumer data as it might lead to a negative influence on consumer behavior towards businesses. The current study is a quantitative analysis that examines, through existing literature, the multifaceted impact of AI-driven digital marketing on consumer data privacy and its resultant impact on consumer behavior towards businesses. A structured questionnaire was used to get insights from 200 randomly selected respondents and Structural Equation Model (SEM) approach was employed to elucidate the complex relationship between AI-driven marketing strategies and privacy concerns among consumers. The findings of the study emphasize the significance of striking a balance between promoting innovation in marketing and safeguarding consumer privacy rights, to ensure ethical application of AI in digital marketing.

Introduction

AI has revolutionized the realm of digital marketing by transforming the way businesses engage with the target market. It has significantly minimized manual intervention by automating various marketing processes, thereby helping businesses enhance marketing campaigns and efficiently engage with potential customers. AI-powered tools such as sentiment analysis, natural language processing and predictive analytics enable marketers to anticipate customer needs and optimize personalized advertising strategies in real-time (George *et al.*, 2024). Thus, to stay consistent in the market, it is crucial to incorporate effective AI-driven marketing strategies that enhance consumer engagement; this can be accomplished by gathering and analyzing consumer data. Data is the key aspect of understanding consumer preferences and trends, which enables marketers to provide personalized campaigns that promote consumer engagement and customer satisfaction (Van Esch and Stewart, 2021).

* Research Scholar, JAIN (Deemed to be University), Bengaluru, Karnataka, India; and is the corresponding author. E-mail: Asma.ninetysix@gmail.com

** Associate Professor, School of Commerce, JAIN (Deemed to be University), Bengaluru, Karnataka, India. E-mail: r.manjupriya@jainuniversity.ac.in

Through robust algorithms and machine learning techniques, AI enables marketers to swiftly and precisely analyze extensive customer data accurately and build deeper connections with the target market. AI in digital marketing has a tremendous success rate, however, digital marketers are oblivious to the method of applying AI in their business operations which can lead to disruptions in various networking channels. AI in marketing is deeply intertwined with data privacy as it heavily relies on the collection, analysis, and utilization of personal data to tailor advertising strategies and enhance consumer engagement (Nair and Gupta, 2021). Thus, it certainly brings forth profound concerns regarding data privacy among customers, which thereby leads to negative attitude of customers towards businesses (Carmody *et al.*, 2021). Though customers normally provide consent to data collection for marketing purposes, they certainly have concerns about the extent of data that can be collected without their awareness leading to privacy hindrances. Furthermore, privacy is a growing concern as the potential for unauthorized access, data breaches, and privacy violations has grown exponentially (Bhadouria, 2022). Presthus and Sørum (2019) ascertained that the General Data Protection Regulation (GDPR) aims at strengthening consumer rights to data privacy in the wake of AI. Therefore, it becomes imperative to study the surge in AI-driven digital marketing leading to ethical concerns in data privacy, as it can help in identifying potential threats to personal data and develop measures to mitigate the risks and protect individuals' privacy rights.

Literature Review

Increasing Relevance of AI-Driven Digital Marketing

AI has rapidly emerged as a game-changer in various sectors, and digital marketing has greatly benefitted from its advancements, resulting in major implications for companies and their digital marketing approaches (Gkikas and Theodoridis, 2019). AI-based propensity modeling gathers and processes large datasets of consumer data effortlessly, helping them discover valuable insights into consumer behavior, preferences, and trends (Theodoridis and Gkikas, 2019). Furthermore, machine learning (ML), a branch of AI, deals with the creation of algorithms that let computers learn from data and improve their functionality without the need for manual programming. ML algorithms in digital marketing examine historical customer data to discover patterns, preferences, and behaviors. These algorithms extract valuable insights from the data, allowing businesses to make informed decisions and customize their marketing strategies accordingly. ML techniques, such as classification, regression, clustering and recommendation systems, have become quite prevalent in the field of digital marketing. The application of this knowledge enables the optimization of marketing campaigns, customization of content, and anticipation of future customer behavior (Chaitanya *et al.*, 2023). According to Ziakis and Vlachopoulou (2023), AI and ML algorithms are now essential components of digital marketing, with techniques like deep learning and neural networks playing a significant part in predictive analytics and customization of marketing tactics (Ruan and Siau, 2019). Marketers also make use of data mining techniques to predict customer behavior and improve customer satisfaction. AI has empowered numerous organizations to forecast extensive consumer data to meet customer requirements and offer personalized products and services (Zaman, 2022). AI emulates human cognitive functions and integrates them into digital marketing. It utilizes input data from analytic reports, websites, sales, and social media insights to generate efficient, productive, and highly optimal outcomes (Suleiman *et al.*, 2021). Hassan (2021) adds that AI also facilitates sentiment analysis, a crucial component of social media tools used to gauge the customer's attitude towards a product, service, or brand, enabling marketers to understand customer behavior, campaign performance, and social listening (Conick, 2017). AI continues to evolve, and its integration into digital marketing strategies promises to redefine the industry landscape, offering unparalleled opportunities for businesses to optimize their marketing efforts and stay ahead in today's competitive market. However, there certainly are ethical challenges to be faced by organizations (Pereira *et al.*, 2023). A study by Mehmood *et al.* (2016) stated, "Marketers are hungry for personal information such that they may more effectively use their money towards targeted advertising. People may be harmed by data collection and yet not realize it, or even anticipate the level of damage. Indeed, the results can prove to be costly and potentially embarrassing, and certainly extend beyond what one might imagine." There is a risk of data breaches or unauthorized access to sensitive information, further exacerbating privacy concerns (Quach *et al.*, 2022). In sum, AI algorithms rely heavily on vast amounts of consumer data to generate insights (Ferrell, 2017). However, this collection and utilization of personal data raise serious questions about privacy infringement and data misuse. The intricate profiling capabilities of AI may result in the creation of highly detailed and potentially invasive consumer profiles, raising concerns about individual privacy rights and autonomy.

Significance of Protecting Consumer Privacy

The present digital world, where information flows freely and personal data is collected at every click, the protection of customer data has become paramount, particularly within the dynamic landscape of digital marketing. Safeguarding privacy is not just a legal requirement but a moral imperative (Pamela, 2023). Evans *et al.* (2023) argued that people generally prefer to keep their personal information private and storing consumer data can cause serious privacy concerns for end-users. According to Kesan *et al.* (2015), privacy is a fundamental right rather than a moral obligation. Privacy issues are a major concern for individuals and can even result in cases of submitting inaccurate information online, resulting in identity theft (Srivastava and Jeet, 2023). Privacy concerns have become more profound as our lives are regularly exposed on social media platforms (Budak *et al.*, 2016). Several social media platforms strive to generate user profiles for monitoring preferences and interests, often accumulating excessive or irrelevant data. Unauthorized access can result in unauthorized manipulation or modification, posing a risk to data integrity and potentially resulting in financial losses and a decline in customer trust (Muneer *et al.*, 2018). With the increasing prevalence of digitalization, it is crucial to safeguard systems and networks, as repercussions are beyond human imagination (Tang *et al.*, 2021). Saeed (2023) highlighted that privacy concerns are a major issue because Internet users have limited technical knowledge and therefore, it becomes imperative to emphasize the significance of protecting consumer data privacy, and safeguarding this information is crucial to maintaining trust between businesses and consumers (Vaghashia and Ganatra, 2015). Protection of privacy fosters a sense of security and confidence among consumers, encouraging them to engage more freely in digital transactions and interactions (Binjubeir *et al.*, 2019). In essence, protecting data privacy is not just a matter of legal obligation but a cornerstone of building and sustaining mutually beneficial relationships in the digital realm (Hammouchi *et al.,* 2019). Moreover, in an era where data breaches and cyberattacks are prevalent, effective data privacy measures serve as a shield against potential threats, safeguarding both individuals and organizations from the adverse consequences of unauthorized data access and exploitation.

Data Privacy Concerns Arising from AI-driven Practices

Many AI-driven marketing practices operate in opaque ways, making it challenging for users to understand how their data is used (Stevenson, 2016). Users may not be aware of the extent of data collected or how it is being utilized for marketing, undermining their privacy rights (Brookman *et al*., 2017). For instance, a participant from a study conducted by Rainie and Duggan (2016) on privacy said, "I share data every time I leave the house, whether I want to or not. The data is not really the problem. It is who gets to see and use that data that creates problems." Users want to maintain the confidentiality and safety of their interpersonal communication, however, this seems unattainable because social networking channels and messaging apps record interactions with friends and family, while smart devices with built-in microphones capture their in-person discussions. However, Cheng *et al*. (2015) argued that confidential data is always secured and inaccessible to irrelevant individuals and organizations. A unique technique known as trapdoor technique is used to ensure the encryption of confidential information. However, even with advanced techniques, there are many instances of data breaches where sensitive information is leaked on the dark web. For instance, in May 2021, Air India, the official airline of India, disclosed a data breach that impacted almost 4.5 million customers. The breach disclosed personal data, including passport information, credit card details, and contact information, as a result of a cyberattack on the airline's data processor. The primary issue is that the disclosure of personal information can have extensive repercussions for individuals, including financial detriment, identity theft, and exposure to legal and security hazards. This underscores the significance of implementing robust data protection measures and strict cybersecurity processes to protect sensitive personal information from unauthorized access and misuse (Cimpanu, 2021). Another such instance of data breach occurred in August 2021: Juspay, a payment gateway provider that administers more than 4 million transactions daily, amounting to ₹1,000 cr, experienced a data breach on various e-commerce platforms, including Amazon, Swiggy, and Ola. This breach resulted in the exposure of personal data belonging to over 100 million customers. The data dump was uncovered in early January by cybersecurity researcher, Rajshekhar Rajaharia. Credit card information and CVV codes, among other sensitive payment data, were stored on a Juspay server that was illegally accessed during the incident. The potential consequence of this could be substantial financial damages for several customers, amounting to millions. Breaches and data exposures have become common. What is more concerning in this specific instance is the significant delay between the incident and Juspay's public acknowledgment of it (Tsaaro, 2021). Therefore, it is crucial for companies to publicly acknowledge any data breaches they experience. When organizations refuse to do this, customers will remain uninformed and will not be able to take the necessary precautions to protect their information. By acknowledging a data breach, companies can help ensure that customers are informed and able to protect their data from being compromised. Data breaches can occur through various means, and they often involve unauthorized access to sensitive information and stem from extensive collection, analysis, and utilization of personal data (Meral, 2021). AI-driven marketing algorithms frequently gather extensive amounts of data from many sources, such as browsing histories, social media engagements, and purchasing patterns. This data collection can create intricate user profiles that may contain sensitive information, such as health status, political beliefs, or financial situation, raising concerns about privacy invasion (Bhardwaj, 2021). According to Trusov *et al.* (2016), AI algorithms create highly detailed profiles of individuals by analyzing their online behavior over time. This continuous monitoring and tracking of user activities raise concerns about privacy invasion, leading to manipulation or exploitation based on this detailed profiling.

In a technological world where everyone is connected through social media, data sharing becomes inevitable. According to Khatri (2021), "When we open social media platforms like Facebook or Instagram, we often see the products that we have talked to someone about, or we have seen somewhere and wanted to buy or we are thinking of something and it appears in front of us; this is all because of AI. But the question is how? This means that the data is analyzed using AI techniques, but did we provide the data?" The answer is No; privacy is the primary casualty in this situation. The unauthorized utilization of customer data, without their consent or authorization, may lead to potential complications in the future (Newman, 2019).

Furthermore, customers' data is stored as Big Data to understand, predict, and influence consumer behavior (Jin, 2018). Nevertheless, a significant challenge that big data encounters revolves around the issue of data privacy. The expanding repositories of big data have become a major focus for hackers and scammers. Data manipulation can lead to privacy concerns, such as collection of user information for undisclosed commercial objectives by an organization (Khanan *et al.*, 2019).

Ultimately, the integration of AI into various practices raises valid privacy concerns. Resolving these concerns necessitates a collaborative approach from marketers, regulators, and technology providers. It is crucial to prioritize user privacy, establish strong security measures, and foster transparency and accountability in digital marketing.

Impact of Data Privacy Breach on Consumer Behavior

Businesses frequently use customer data to enhance their marketing efforts; however, this framework compels one business to share its customer data with another, putting it at risk for privacy violations that could result in serious losses of competitive advantage, customer trust, and brand value, as well as legal repercussions for noncompliance (Schneider *et al*., 2017). Organizations often sell customer data to other businesses through various data brokerage firms or data exchanges (Rostow, 2017). These entities act as intermediaries to collect valuable consumer information from multiple sources, such as online purchases, browsing history, social media interactions, and demographic data. Once aggregated, this data is anonymized and packaged into datasets, which are then sold or exchanged among digital marketers and advertisers (Schneider *et al.*, 2017). The sharing of consumer data with third-party brokers is a widespread practice across various industries, driven by the desire to enhance marketing efforts, generate revenue, and gain valuable insights into consumer behavior. Rodenhausen *et al.* (2023) proposed that customers expect their data to be utilized to create concise, informative, and captivating marketing content, or to help businesses understand their preferred product advancements. However, they express apprehension when it comes to their data being shared with other companies, and strongly oppose the idea of their data being sold. Data sharing raises significant concerns regarding privacy, security, and ethical considerations, prompting calls for stricter regulations and greater transparency in data-sharing practices (Jai and King, 2016). However, in the modern Internet era, where there are no boundaries on the volume of information shared, privacy becomes a concern (Wu *et al.,* 2012). When personal information falls into the wrong hands due to a breach, customers feel a profound sense of violation and vulnerability (Ablon *et al.*, 2016). This can profoundly result in cynical consumer behavior towards the business, which can furthermore lead to a breach of trust, with individuals becoming more cautious and selective about the companies they engage with online. When consumers lose trust in a business, it may have adverse effects on a firm's reputation (Ho *et al.*, 2023). This loss of customer confidence can have long-lasting effects (Lulandala, 2020). If a customer no longer chooses to use a business service, they probably will not want to return to the same business; this will lead to potential revenue loss for businesses (Jumah and Alnsour, 2022). Trust is fundamental to any relationship, whether it is between stakeholders or customers. A data breach can lead to a significant breakdown in confidence, making it challenging for the affected organization to regain trust and rebuild its reputation (Strzelecki and Rizun, 2022). Customers predominantly lose trust in a company when it fails to promptly announce a data breach. One of the major concerns with data breaches is the announcement made by the companies informing the customers about the breach. The timely disclosure of a breach has an enormous impact on efforts to rebuild trust (Muzatko and Bansal, 2018). When the announcement of a breach is delayed, it makes it difficult to restore trust to its initial levels (Muzatko and Bansal, 2023). Furthermore, timely disclosure is essential for consumers to take necessary precautions to protect their personal information. When a company delays announcing a breach, consumers may perceive it as hiding information, which thereby leads to a change in consumer behavior (Angelis *et al.*, 2022). Lack of transparency can irreversibly damage the company's reputation, resulting in loss of customer loyalty and trust (Strzelecki and Rizun, 2022). The negative repercussions on consumer attitude towards businesses have become increasingly prevalent in today's digital landscape mainly due to unprecedented data breaches.

When personal information is compromised, cybercriminals may use this data to craft convincing phishing messages tailored to the victims. These messages often appear legitimate, leveraging stolen information to establish trust and increase the likelihood of success (Thomas *et al*., 2017). For example, attackers may use stolen email addresses or account details to impersonate reputable organizations or individuals, making their phishing attempts appear more authentic (Nurse, 2018). The effect on customers can be profound, as falling victim to phishing can lead to further data compromise, financial loss, identity theft, or other forms of cybercrime (Sumner and Yuan, 2019). Moreover, phishing attacks can erode trust in legitimate communications, leaving customers wary of engaging with legitimate businesses and organizations (Abroshan *et al*., 2018). Overall, the intersection of data breaches and phishing poses a significant threat to customer security and underscores the importance of robust cybersecurity measures and proactive education to mitigate risks and protect individuals' sensitive information (Suzuki and Monroy, 2022). Businesses that fail to prioritize data protection risk tarnishing their reputation and losing the trust of their customer base, ultimately facing financial and operational setbacks. Therefore, safeguarding data privacy is not just a legal obligation but also a crucial aspect of maintaining consumer trust and fostering positive relationships with customers.

Regulations Governing Consumer Privacy

General Data Protection Regulation (GDPR)

GDPR has been recognized as a significant milestone in safeguarding data privacy, setting a new benchmark for data protection regulations. The GDPR of the European Union is widely recognized as a highly comprehensive legal framework for safeguarding the personal data of individuals and granting them various rights. Many countries around the world have developed their own data protection laws, drawing inspiration from the GDPR framework. It is a comprehensive regulation that governs the processing of personal data. It establishes mandatory requirements for obtaining consent, including special considerations for consent from minors. The regulation additionally defines special categories of personal data and outlines the rights of individuals whose data is being processed. Non-compliance with GDPR laws can result in significant penalties. Additionally, the GDPR has set up an independent supervisory authority to ensure compliance and handle grievances (Shastri, 2023).

California Consumer Privacy Act (CCPA)

The CCPA regulates the operations of companies and individuals involved in the collection and processing of consumers' private data. It is required by law for companies to prioritize the protection and proper handling of data, while also granting consumers the authority to manage and oversee the collection, usage, and sharing of their personal information. With CCPA, consumers have the authority to delete any information that has been collected about them and can also put a stop to the sale of their personal data to third-parties (Goldman, 2020). Both GDPR and CCPA aim to strengthen consumer rights, and businesses will have to allocate a significant amount of their limited resources—including money, time, and effort—to ensure they comply with laws that may be similar but have distinct requirements (Alexander, 2019).

Digital Personal Data Protection (DPDP)

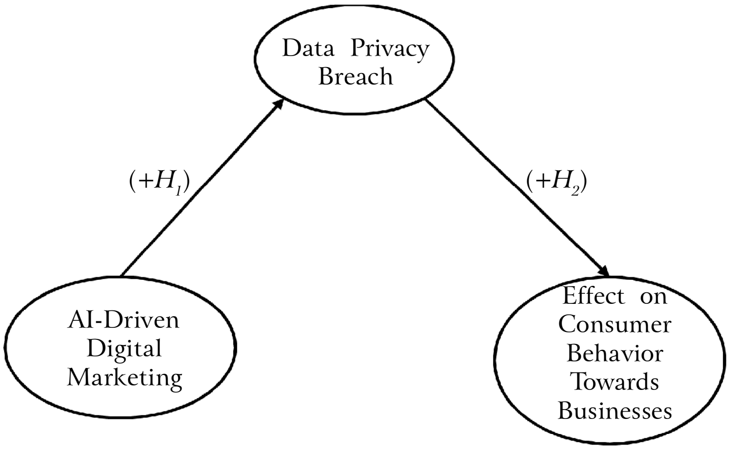
India has been diligently working on a comprehensive data privacy regulation that aligns with global standards, ensuring the utmost protection for its citizens. Although the Information Technology Act of 2000 still stands as the primary legislation addressing data privacy in India, DPDP has undeniably transformed the landscape of data protection in the country. This act permits the processing of personal data for any lawful purpose. An organization processing data must obtain consent from the individual involved or use it for "legitimate purposes," as defined by the law. It is important to only collect the data that is essential for the intended purpose. Consumers must be provided with a clear notice that includes all the necessary details, such as the rights of the individual involved and the process for addressing grievances. People have the option to withdraw their consent if it is the basis for processing their data (Burman, 2023).

In summary, the regulations vary in terms of their scope, enforcement mechanisms, and specific provisions. However, they all have a common objective of protecting individuals' privacy rights, encouraging responsible data practices, and ensuring that data controllers and processors are held accountable. Having a deep understanding of these regulations is crucial for organizations operating in a global digital economy to successfully navigate compliance requirements and maintain ethical standards in data handling practices.

Conceptual Framework and Hypothesis Formulation

The framework shown in Figure 1 is conceptualized from the literature review.

Figure 1: Conceptual Framework


Data Privacy Breach
(+H_1)
(+H_2)
AI-Driven Digital Marketing
Effect on Consumer Behavior Towards Businesses

H_1: Use of AI-driven digital marketing has a higher probability of perceived breach of data privacy

H_2: The higher the frequency of data privacy breaches, the higher the negative impact on consumer behavior towards businesses

Data and Methodology

The approach involved constructing theories by thoroughly reviewing existing literature and carefully examining the gaps or limitations. The current study has employed a structured questionnaire (see Appendix) for quantitative information. The participants in the interview were selected based on structured snowballing and random sampling. As far as statistical technique was concerned, SEM approach was considered. However, this model was customized to the need of the present study.

For this study, a set of 11 Likert-based questions was created. Participants were asked to rate their level of agreement on a scale of 1 to 5, with 1 representing Strongly Disagree and 5 representing Strongly Agree. For data collection, the authors conducted interviews with 200 respondents. These respondents were randomly selected individuals who purchase products online. The authors used a structured online questionnaire to gather information from them. A basic random technique was used to gather the data. The period of the study was from March 2024 to August 2024.

Results

The pertinent items, 'standardized loading' (correlation coefficients), composite reliability, and Cronbach's alpha results are shown in Table 1. The hypothesized measurement model—which comprises three dimensions, viz., AI-driven digital marketing, data privacy breaches, and the impact of customer behavior towards businesses—was validated using the Confirmatory Factor Analysis (CFA) technique. Furthermore, Table 1 provides the loading of items below each dimension.

To assess the questionnaire's psychometric qualities, we first calculated the Cronbach's alpha reliability coefficient. Cronbach's alpha has a value between 0 and 1, where a higher number denotes more consistency and stability. Nonetheless, a cut-off value of 0.60 is frequently employed for fundamental research (Nunnally, 1978; and Kalthom *et al.,* 2012). Table 1 displays the results of Cronbach's alpha, indicating that the instrument's consistency and stability are satisfactory. Additionally, Table 1 makes it clear that a significant number of the components had loading values higher than 0.50 while examining the composite reliability, which offers strong support for commonality. Furthermore, all dimensions' Cronbach's alpha values are higher than the generally accepted 0.60 threshold. Table 2 displays the discriminant validity result, which shows that there is no statistical overlap between the latent variables. This is indicated by the inter-item correlation values being less than the square root of the AVE value. Furthermore, the constructs are not affected by multicollinearity.

Table 1: Reliability and Item Loadings of AI-Driven Digital Marketing Constructs Impacting Breach of Data Privacy and Consumer Behavior Towards Businesses

Factor	Item/Indicators	Loading	CR	CA	AVE
AI-Driven Digital Marketing (AI_DM)	I find AI-driven digital marketing strategies helpful when making purchase decisions (AI_DM_1)	0.711	0.752	0.753	0.432
	AI-driven digital marketing strategies improve my overall shopping experience (AI_DM_2)	0.637			
	I am more engaged with the brands that use AI for personalized marketing (AI_DM_3)	0.683			
	I prefer receiving AI-driven marketing recommendations over generic marketing messages (AI_DM_4)	0.592			
Breach of Data Privacy (DAT_PRV)	I feel AI-driven digital marketing poses a risk to my personal data (DAT_PRV_1)	0.662	0.780	0.780	0.470
	I feel companies are not transparent about how they use my data, which can cause a breach of privacy (DAT_PRV_2)	0.713			
	I feel that I have no control over my personal data when it is used in AI-driven marketing practices (DAT_PRV_3)	0.672			
Effect on Consumer Behavior Towards Businesses (CON_BHV)	I feel that my data is not adequately protected when used in AI-driven digital marketing (DAT_PRV_4)	0.694	0.720	0.721	0.463
	Concerns about data privacy affect my trust in businesses using AI-driven digital marketing strategies (CON_BHV_1)	0.715			
	I am more likely to avoid businesses that I perceive as mishandling consumer data through AI-driven marketing (CON_BHV_2)	0.726			
	I avoid doing business/purchases with companies that have had data breaches or privacy issues (CON_BHV_3)	0.593			

Note: CR – Composite Reliability, CA – Cronbach Alpha, AVE – Average Variance Explained.

Table 2: Discriminant Validity of the Measurement Model

	AI_DM	DAT_PRV	CON_BHV
AI_DM	**0.657***		
DAT_PRV	0.613	**0.686***	
CON_BHV	0.523	0.649	**0.680***

Note: * Square Root of AVE values.

SEM Analysis Result

SEM analysis was used to test the hypotheses following the CFA which evaluated the items' validity and reliability. Table 3 and Figure 2 present the results.

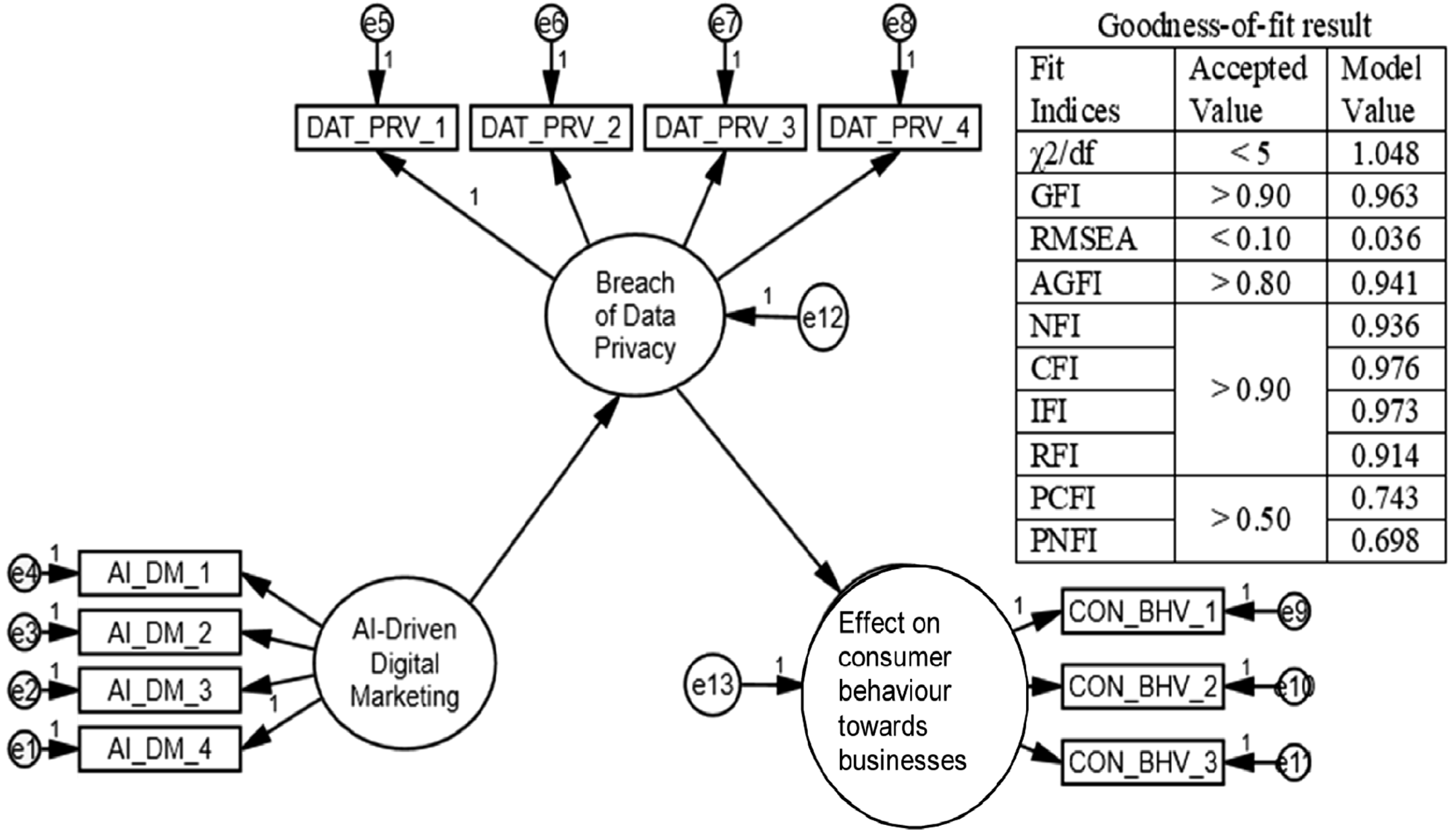
The results of the SEM analysis revealed that the model demonstrated a close match to the required model fit, as evidenced by a chi-square/df value of 1.048 (Figure 2). The CFI and GFI are close to standard cut-off of above 0.90. RMSEA with a value of 0.036 fulfilled the threshold value of 0.10. Regression analysis results are depicted in Table 3, which shows AI-driven digital marketing has a significant (with p-value of 0.000, $p < 0.05$) influence on breach of data privacy. Thus, hypothesis H_1 is accepted at 95% level of confidence. The regression ($\beta = 0.724$) indicates that for every additional 10 respondents who favor digital marketing, an average of seven respondents are likely to agree on the data privacy breach dimension. Similarly, breach of data privacy has significant impact on consumer behavior towards businesses and the hypothesis is accepted at 5% level of significance. Likewise, breach of data privacy has about 66% ($\beta = 0.661$) impact on consumer behavior towards businesses, at a statistically significant level of 5%. This implies that six out of ten consumers perceive a risk of data breach towards businesses which can lead to a huge loss of ROI.

Table 3: Standardized Regression Coefficients for the Direct Correlation Between Dimensions

			Standard Estimate	CR	p	Remark
Breach of Data Privacy	←	AI-Driven Digital Marketing	0.724	5.831	0.000*	H_1 supported
Effect on Consumer Behavior	←	Breach of Data Privacy	0.661	6.035	0.000*	H_2 supported

Note: * Significant at 5% level.

Figure 2: SEM Result of AI-Driven Digital Marketing Constructs Impacting Breach of Data Privacy and Consumer Behavior Towards Businesses



Goodness-of-fit result

Fit Indices	Accepted Value	Model Value
χ2/df	< 5	1.048
GFI	> 0.90	0.963
RMSEA	< 0.10	0.036
AGFI	> 0.80	0.941
NFI	> 0.90	0.936
CFI		0.976
IFI		0.973
RFI		0.914
PCFI	> 0.50	0.743
PNFI		0.698

Discussion

The present study offers practical recommendations for customers and marketers to prevent privacy issues and data breaches. Implementing these recommendations can greatly decrease the likelihood of data breaches, safeguard customer information, and maintain trust, additionally leading to an improved ROI. It promotes consumer engagement and uninterrupted sales. Similarly, individuals can be proactive in protecting their personal information and reducing the potential harm caused by any security breaches.

Below are a few significant practices that can be enforced by organizations to protect the consumer database:

Taking User Consent Before Sharing Data with Third Parties: The study found that organizations often share consumer data with third-party organizations through data brokers for marketing purposes and targeted advertising. Customers value their privacy and expect organizations to handle their data responsibly and ethically. When organizations share consumer data with data brokers, especially without transparent disclosure, it undermines consumer trust and damages reputation which can lead to privacy violations. Customers may feel that their personal information is being exploited for profit and may worry about possible consequences such as identity theft or unauthorized use of their information. Therefore, obtaining user consent before sharing information with third parties is of utmost importance. It respects individual autonomy and rights to privacy and recognizes their ownership and control of their data.

Complying with Government Standards: Strict measures must be taken to follow the government protocols in every organization. Compliance with government regulations such as GDPR and DPDP is significantly important as it protects consumer data. Adherence to these standards safeguards individual privacy rights by setting clear guidelines for the collection, processing, and storage of personal data. Compliance with government standards not only protects the fundamental rights of individuals to privacy but also helps organizations mitigate various privacy risks. It also helps organizations avoid legal consequences and hefty fines and demonstrates their commitment to upholding ethical standards and respecting individual privacy preferences.

Companies Should Invest in Cybersecurity: Organizations are data keepers, not data owners. This shift in perspective underscores the responsibility organizations bear in safeguarding sensitive information entrusted to them by customers, employees, and stakeholders. By acknowledging their role as data keepers, companies can better appreciate the importance of implementing robust cybersecurity. Investing in robust cybersecurity measures not only helps mitigate these risks but also strengthens resilience against potential threats, ensuring the continuity of business operations and protecting sensitive data from unauthorized access or misuse as it allows organizations to fulfill their duty of care towards the data they manage, preserving trust, integrity, and privacy.

The Data Should Always Be Encrypted: Embracing Transport Layer Security (TLS) 1.3 as the encryption standard reflects a proactive approach to cybersecurity, safeguarding sensitive data and mitigating risks associated with cyber threats. It ensures that eavesdroppers and hackers are unable to see what is transmitted. It is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence. By upgrading to TLS 1.3, organizations can benefit from improved performance and reduced latency, while ensuring data confidentiality and integrity during transmission across networks. Embracing encryption as a cybersecurity best practice demonstrates a commitment to safeguarding data integrity and confidentiality, fostering trust among customers, partners, and stakeholders.

Organizations Should Enforce Multi-Factor Authentication for Administrators Who Access Consumer Data: Organizations today face ever-evolving cybersecurity threats, particularly concerning the protection of consumer data. One pivotal measure in fortifying their defence is the enforcement of multi-factor authentication (MFA) for administrators who access consumer data. MFA adds an additional layer of security beyond traditional password-based authentication, significantly reducing the risk of unauthorized access and potential data breaches. By requiring administrators to authenticate themselves through multiple factors such as passwords, biometrics, or one-time codes, MFA mitigates the vulnerabilities associated with password theft or phishing schemes.

Access to Database Servers Should Be Restricted to Specific Administrators Through Role-Based Access Control (RBAC) Policies: Employing RBAC policy is a prudent approach to manage and restrict access to specific administrators based on their roles and responsibilities. With RBAC, administrators are assigned roles defining their level of access, ensuring that they only interact with data and functionalities relevant to their tasks. For instance, a database administrator may have full access to database management functions, while a customer support representative may only have access to customer-related data. By implementing RBAC, organizations can enforce the principle of least privilege, granting administrators the minimum level of access required to perform their duties effectively. This not only reduces the risk of unauthorized access and potential data breaches but also enhances accountability and traceability in data management practices. Overall, leveraging RBAC policies to restrict access to database servers ensures a robust and secure data environment, safeguarding sensitive information and preserving organizational integrity.

Data Breach Has to Be Reported by Organizations Immediately: In the digital age, where data breaches pose significant risks to privacy and security, prompt and transparent reporting is crucial. It is imperative that companies adhere to regulations mandating the reporting of data breaches to both the relevant government authorities and affected end-users within specified timeframes. Such regulations establish accountability and promote swift action in the event of a breach, enabling authorities to investigate and mitigate the impact, while empowering users to take necessary precautions to protect themselves. Timely reporting not only helps contain the fallout of a breach but also fosters transparency, trust, and confidence among stakeholders. By promptly notifying both regulatory bodies and affected individuals, companies demonstrate their commitment to data protection and accountability, paving the way for swift remediation efforts and ensuring the integrity of digital ecosystems.

As for consumers, to mitigate data privacy issues, they may need to consider the following:

Consumers Should Never Use Identical Passwords and Pins Across Different Channels: Due to the inherent risks associated with such practices, using the same credentials across multiple platforms increases the vulnerability of personal accounts to potential security breaches. If one account is compromised, hackers can easily access other accounts that share the same login credentials, leading to widespread data theft or identity fraud. By using unique passwords and PINs for each channel, consumers can mitigate the impact of a security breach on their other accounts, minimizing the risk of unauthorized access and protecting their sensitive information.

Users Should Provide Only Required Information and Not Unwarranted Information: Users should exercise caution and discretion when providing personal information, ensuring that they only disclose the necessary details and refrain from sharing unwarranted information. This prudent approach helps mitigate risks associated with data privacy breaches, identity theft, and unauthorized access. By limiting the disclosure of personal information to only what is required for a specific transaction or interaction, users can minimize their exposure to potential threats and protect their privacy rights. Adhering to the principle of sharing only required information aligns with best practices for data protection and privacy, promoting a safer and more secure online environment for users.

Users Must Not Save Passwords on Websites, Notepads or Logbooks: Users must refrain from saving passwords on websites or storing them in easily accessible locations such as notepads due to significant security risks. Saving passwords directly on websites exposes them to potential breaches, as these passwords may be compromised if the website's security is compromised. Cybercriminals actively target such easily accessible repositories of passwords, posing a serious threat to users online security and privacy. Similarly, storing passwords in logbooks increases the risk of physical theft or unauthorized access. Instead, users should adopt secure password management practices, such as using reputable password managers. Password managers offer encrypted storage for passwords, ensuring that they remain secure and inaccessible to unauthorized individuals. Additionally, users should create strong, unique passwords for each online account and enable multi-factor authentication whenever possible to add an extra layer of security.

Review Data Sharing Option: Consumers have the power to safeguard their data privacy by actively choosing to limit data sharing. Many online platforms and services provide users with settings or preferences that allow them to control how their personal information is shared with third-parties. By accessing these settings, consumers can review and adjust permissions related to data sharing, choosing to limit or opt out of sharing their information with external entities. Choosing to restrict data sharing serves as a practical measure for consumers to assert control over their data privacy, enhance online security, and promote responsible data handling practices among service providers.

Practice Safe Browsing Habits and Beware of Phishing and Other Spam Attacks: Often, cybercriminals employ deceptive tactics, such as phishing emails or fake pop-up notifications to lure users into downloading malicious software or providing sensitive information. Phishing attempts involve fraudulent emails, messages, or websites designed to deceive recipients into divulging sensitive information such as passwords, credit card numbers, or personal data. These attacks often impersonate trusted entities, such as banks, government agencies, or reputable organizations, to trick users into taking actions that compromise their security. By avoiding the temptation to click links or download files from suspicious sources, users can safeguard themselves against malware infections, data breaches, and other cyber threats. Instead, users should rely on official channels, such as Apple App Stores or Google Play Store to obtain any updates for their applications.

Privacy Setting Review: It is important to regularly review and adjust privacy settings on social media platforms, apps, and online services in order to have control over the information shared and who can access it. Adjusting privacy settings helps mitigate the risk of data exposure and potential privacy violations by limiting the amount of information shared with third-party entities or advertisers. By taking proactive steps to manage privacy settings, users can safeguard their digital identities.

Conclusion

AI significantly enhances personalization for individual customers; however, it relies heavily on data collection to function effectively, thereby raising concerns about privacy and security. Digital marketing strategies using AI collect data from various sources, including social media, browsing history, purchase history, and even real-time location data. While this data-driven approach enables more effective marketing strategies, it also means that large volumes of personal data are stored and processed, potentially exposing consumers to risks if data breaches occur.

There is a growing concern among consumers regarding the limited transparency and control they have over their personal information. Issues such as unauthorized data sharing, inadequate data protection measures, and the potential for misuse of personal information have become prominent, exacerbated by instances of high-profile data breaches and misuse of consumer data by companies.

Marketers must carefully consider the advantages of AI-driven strategies, while also prioritizing the protection of consumer data, adherence to regulatory requirements, and preservation of consumer trust. Through the use of advanced technology and a commitment to openness and protection, organizations can address privacy issues and unlock the complete capabilities of AI in the realm of digital marketing.

Adhering to privacy regulations can be a challenging and expensive endeavor, and not meeting these requirements can lead to significant penalties and harm to one's reputation. Striking the perfect balance between personalization and privacy poses a significant challenge for marketers. Although individuals appreciate personalized marketing that caters to their preferences, they also highly value their privacy.

In conclusion, the future of AI in digital marketing will likely see continued advancements in both personalization and data privacy protection. As AI technologies evolve, they will offer more sophisticated tools for data analysis while simultaneously incorporating stronger privacy-preserving features. Marketers must stay informed about technological developments and regulatory changes to effectively navigate the landscape of AI-driven digital marketing.

Limitations: The domain of AI-driven digital marketing is undergoing tremendous advancements, and the technology and methodologies addressed in this paper may swiftly become outdated. With the ongoing progress of AI, it is expected that new privacy issues and suggestions will arise. Continuous research is necessary to stay up-to-date with these advancements and comprehend their consequences for the privacy of consumer data.

References

1. Ablon L, Heaton P, Lavery D C and Romanosky S (2016), *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, Rand Corporation.

2. Abroshan H, Devos J, Poels G and Laermans E (2018), "Phishing Attacks Root Causes", Risks and Security of Internet and Systems: 12th International Conference, *CRiSIS 2017,* pp. 187-202, Dinard, France, September 19-21, 2017, Revised Selected Papers 12, Springer International Publishing.

3. Alexander C B (2019), "The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations", *Loy. Consumer L. Rev*., Vol. 32, No. 2, p. 199. https://lawecommons.luc.edu/lclr/vol32/iss2/2

4. Angelis J N, Murthy R S, Beaulieu T and Miller J C (2022), "Better Angry Than Afraid: The Case of Post Data Breach Emotions on Customer Engagement", *IEEE Transactions on Engineering Management,* Vol. 71, pp. 2593-2605.

5. Bhadouria A S (2022), "Study of Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches", *International Journal of Scientific and Research Publications*, DOI:10.29322/IJSRP.X.2022.p091095

6. Bhardwaj K (2021), "AI for Data Driven Digital Marketing", Doctoral dissertation, Delhi Technological University.

7. Binjubeir M, Ahmed A A, Ismail M A B *et al.* (2019), "Comprehensive Survey on Big Data Privacy Protection", *IEEE Access*, Vol. 8, pp. 20067-20079.

8. Brookman J, Rouge P, Alva A and Yeung C (2017), *Cross-Device Tracking: Measurement and Disclosures*, Proceedings on Privacy Enhancing Technologies.

9. Budak C, Goel S, Rao J and Zervas G (2016), "Understanding Emerging Threats to Online Advertising", ACM Conference on Economics and Computation, pp. 561-578.

10. Burman A (2023), "Understanding India's New Data Protection Law-Carnegie India", https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624. Accessed March 24, 2024.

11. Carmody J, Shringarpure S and Van de Venter G (2021), "AI and Privacy Concerns: A Smart Meter Case Study", *Journal of Information, Communication and Ethics in Society*, Vol. 19, No. 4, pp. 492-505.

12. Chaitanya K, Saha G C, Saha H *et al*. (2023), "The Impact of Artificial Intelligence and Machine Learning in Digital Marketing Strategies", *European Economic Letters (EEL)*, Vol. 13, No. 3, pp. 982-992.

13. Cheng H, Rong C, Hwang K *et al.* (2015), "Secure Big Data Storage and Sharing Scheme for Cloud Tenants", *China Communications*, Vol. 12, No. 6, pp. 106-115.

14. Cimpanu C (2021), "Air India Says Data Breach Impacts 4.5 million Former Passengers", May 24. https://therecord.media/air-india-says-data-breach-impacts-4-5-million-former-passengers

15. Conick H (2017), "The Past, Present and Future of AI in Marketing", *Marketing News*, Vol. 51, No. 1, pp. 26-35.

16. Evans R, Hajli N and Nisar T M (2023), "Privacy Enhancing Factors and Consumer Concerns: The Moderating Effects of the General Data Protection Regulation", *British Journal of Management*, Vol. 34, No. 4, pp. 2075-2092.

17. Ferrell O C (2017), "Broadening Marketing's Contribution to Data Privacy", *Journal of the Academy of Marketing Science*, Vol. 45, pp. 160-163.

18. George S M, Sasikala B, Gowthami T *et al.* (2024), "Role of Artificial Intelligence in Marketing Strategies and Performance", *Migration Letters*, Vol. 21, No. S4, pp. 1589-1599.

19. Gkikas D C and Theodoridis P K (2019), "Artificial Intelligence (AI) Impact on Digital Marketing Research", Springer Proceedings in Business and Economics, in Androniki Kavoura, Efstathios Kefallonitis and Apostolos Giovanis (Ed.), *Strategic Innovative Marketing and Tourism*, pp. 1251-1259, Springer International Publishing.

20. Goldman E (2020), "An Introduction to the California Consumer Privacy Act (CCPA)", Santa Clara Univ. Legal Studies Research Paper.

21. Hammouchi H, Cherqi O, Mezzour G *et al.* (2019), "Digging Deeper into Data Breaches: An Exploratory Data Analysis of Hacking Breaches Over Time", *Procedia Computer Science*, Vol. 151, pp. 1004-1009.

22. Hassan A (2021), "The Usage of Artificial Intelligence in Digital Marketing: A Review", *Applications of Artificial Intelligence in Business, Education and Healthcare*, pp. 357-383.

23. Ho F N, Ho-Dac N and Huang J S (2023), "The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence", *SAGE Open,* Vol. 13, No. 3, 21582440231181395.

24. Jai T M C and King N J (2016), "Privacy Versus Reward: Do Loyalty Programs Increase Consumers' Willingness to Share Personal Information with Third-Party Advertisers and Data Brokers?", *Journal of Retailing and Consumer Services*, Vol. 28, No. C, pp. 296-303.

25. Jin G Z (2018), "Artificial Intelligence and Consumer Privacy", in *The Economics of Artificial Intelligence: An Agenda,* pp. 439-462, University of Chicago Press.

26. Juma'h A H and Alnsour Y (2020), "The Effect of Data Breaches on Company Performance", *International Journal of Accounting & Information Management*, Vol. 28, No. 2, pp. 275-301.

27. Kalthom A, Jan M T and Manaf N H A (2012), "A Structural Equation Modelling Approach to Validate the Dimensions of SERVPERF in the Airline Industry of Malaysia", *International Journal of Engineering and Management Sciences*, Vol. 3, No. 2, pp. 134-141.

28. Kesan J P, Hayes C M and Bashir M N (2015), "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy", *Ind. LJ*, Vol. 91, p. 267.

29. Khanan A, Abdullah S, Mohamed A H H *et al.* (2019), "Big Data Security and Privacy Concerns: A Review", Smart Technologies and Innovation for a Sustainable Future: Proceedings of the 1st American University in the Emirates International Research Conference, Dubai, UAE 2017, pp. 55-61, Springer International Publishing.

30. Khatri M (2021), "How Digital Marketing Along with Artificial Intelligence is Transforming Consumer Behavior", *International Journal for Research in Applied Science and Engineering Technology*, Vol. 9, No. 7, pp. 523-527.

31. Lulandala E E (2020), "Facebook Data Breach: A Systematic Review of Its Consequences on Consumers' Behaviour Towards Advertising", in P K Kapur, O Singh, S K Khatri and A K Verma (Eds.), *Strategic System Assurance and Business Analytics: Asset Analytics,* Springer, Singapore. https://doi.org/10.1007/978-981-15-3647-2_5

32. Mehmood A, Natgunanathan I, Xiang Y *et al.* (2016), "Protection of Big Data Privacy", *IEEE access*, Vol. 4, pp. 1821-1834.

33. Meral K Z (2021), "Strategic Social Media Marketing and Data Privacy", *Management Strategies to Survive in a Competitive Environment: How to Improve Company Performance,* pp. 187-199, Springer International Publishing, Cham.

34. Muneer Asia, Razzaq Samreen and Farooq Zaineb (2018), "Data Privacy Issues and Possible Solutions in E-Commerce", *Journal of Accounting & Marketing*, Vol. 7. 10.4172/2168-9601.1000294

35. Muzatko S and Bansal G (2018), "Timing of Data Breach Announcement and e-Commerce Trust", The proceedings of Midwest Association for Information Systems Conference.

36. Muzatko S and Bansal G (2023), "It Pays to be Forthcoming: Timing of Data Breach Announcement, Trust Violation, and Trust Restoration", Internet Research.

37. Nair K and Gupta R (2021), "Application of AI Technology in Modern Digital Marketing Environment", *World Journal of Entrepreneurship, Management and Sustainable Development*, Vol. 17, No. 3, pp. 318-328.

38. Newman D (2019), "5 Ways AI Is Transforming the Customer Experience". Retrieved from https://www.forbes.com/sites/danielnewman/2019/04/16/5-ways-ai-is-transforming-the-customer-experience/?sh=55da8158465a

39. Nurse J R (2018), "Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit". arXiv preprint arXiv:1811.06624

40. Nunnally J C (1978), "An Overview of Psychological Measurement", in B B Wolman, (Eds.), *Clinical Diagnosis of Mental Disorders,* pp. 97-146, Springer, Boston, MA.

41. Pamela (2023), "Ethics of Data Privacy in Digital Marketing", *CIO Women Magazine*. https://ciowomenmagazine.com/data-privacy-in-digital-marketing/

42. Pereira L, Tomás D, Dias Á *et al.* (2023), "How Artificial Intelligence Can Improve Digital Marketing", *International Journal of Business Information Systems*, Vol. 44, No. 4, pp. 581-624.

43. Presthus W and Sørum H (2019), "Consumer Perspectives on Information Privacy Following the Implementation of the GDPR", *International Journal of Information Systems and Project Management*, Vol. 7: No. 3, Article 3. https://aisel.aisnet.org/ijispm/vol7/iss3/3.

44. Quach S, Thaichon P, Martin K D *et al.* (2022), "Digital Technologies: Tensions in Privacy and Data", *Journal of the Academy of Marketing Science*, Vol. 50, No. 6, pp. 1299-1323.

45. Rainie L and Duggan M (2016), "Privacy and Information Sharing", Pew Research Center, December 2015, http://www.pewinternet.org/2016/01/14/2016/Privacy-and-Information-Sharing/

46. Rane S (2023), "What is ISO 27001? A Detailed, Simple, and Straightforward Guide", ControlCase. https://www.controlcase.com/what-is-iso-27001/? Accessed on March 24, 2024.

47. Rodenhausen D, Wiener L, Rogers K and Katerman M (2023), "Consumers Want Privacy. Marketers Can Deliver", Digital Marketing.

48. Rostow T (2017), "What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers", *Yale Journal on Regulation*, Vol. 34, No. 2, p. 667.

49. Ruan Z and Siau K (2019), "Digital Marketing in the Artificial Intelligence and Machine Learning Age", The Americas Conference on Information Systems (AMCIS 2019), Cancun, Mexico.

50. Saeed S (2023), "A Customer-Centric View of E-Commerce Security and Privacy", *Applied Sciences*, Vol. 13, No. 2, 1020. https://doi.org/10.3390/app13021020

51. Schneider M J, Jagpal S, Gupta S *et al.* (2017), "Protecting Customer Privacy when Marketing with Second-Party Data", *International Journal of Research in Marketing*, Vol. 34, No. 3, pp. 593-603.

52. Shastri D (2023), "What is GDPR Compliance and Applicability in India?", LegalWiz.in. https://www.legalwiz.in/blog/what-is-gdpr-compliance-and-applicability-in-india

53. Srivastava S and Jeet S (2023), "E-commerce and Privacy Issues", *Russian Law Journal*, Vol. 11, No. 5, pp. 2170-2175.

54. Stevenson D M (2016), "Data, Trust, and Transparency in Personalized Advertising", Doctoral dissertation.

55. Strzelecki A and Rizun M (2022), "Consumers' Change in Trust and Security After a Personal Data Breach in Online Shopping", *Sustainability*, Vol. 14, No. 10, 5866. https://doi.org/10.3390/su14105866

56. Suleiman D A, Awan T M and Javed M (2021), "Enhancing Digital Marketing Performance Through Usage Intention of AI-Powered Websites", *IAES International Journal of Artificial Intelligence*, Vol. 10, No. 4, pp. 810-817.

57. Sumner A and Yuan X (2019), "Mitigating Phishing Attacks: An Overview", Proceedings of the 2019 ACM Southeast Conference, pp. 72-77.

58. Suzuki Y E and Monroy S A S (2022), "Prevention and Mitigation Measures Against Phishing Emails: A Sequential Schema Model", *Security Journal*, Vol. 35, No. 4, pp. 1162-1182.

59. Tang Z, Miller A S, Zhou Z and Warkentin M (2021), "Does Government Social Media Promote Users Information Security Behaviour Towards Covid-19 Scams? Cultivation Effects and Protective Motivations", *Government Information Quarterly,* Vol. 38, No. 2, 101572. https://doi.org/10.1016/j.giq.2021.101572

60. Theodoridis P K and Gkikas D C (2019), "How Artificial Intelligence Affects Digital Marketing", International Conference on Strategic Innovative Marketing and

Tourism 2018 (ICSIMAT), pp. 1319-1327, Springer International Publishing, Athenian Riviera, Greece.

61. Thomas K, Li F, Zand A *et al.* (2017), "Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials", Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1421-1434.

62. Trusov M, Ma L and Jamal Z (2016), "Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting", *Marketing Science*, Vol. 35, No. 3, pp. 405-426.

63. Tsaaro (2021), "Juspay Data Breach", https://tsaaro.com/blogs/juspay-data-breach/

64. Vaghashia H and Ganatra A (2015), "A Survey: Privacy Preservation Techniques in Data Mining", *International Journal of Computer Applications*, Vol. 119, No. 4, pp. 20-26.

65. Van Esch P and Stewart Black J (2021), "Artificial Intelligence (AI): Revolutionizing Digital Marketing", *Australasian Marketing Journal*, Vol. 29, No. 3, pp. 199-203. https://doi.org/10.1177/18393349211037684

66. Wu K W, Huang S Y, Yen D C and Popova I (2012), "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust", *Computers in Human Behavior*, Vol. 28, No. 3, pp. 889-897.

67. Zaman K (2022), "Transformation of Marketing Decisions Through Artificial Intelligence and Digital Marketing", *Journal of Marketing Strategies*, Vol. 4, No. 2, pp. 353-364.

68. Ziakis C and Vlachopoulou M (2023), "Artificial Intelligence in Digital Marketing: Insights from a Comprehensive Review", *Information*, Vol. 14, No. 12, 664. https://doi.org/10.3390/info14120664

Appendix

Questionnaire	
Constructs and Measurement Items	
Influence of AI-Driven Digital Marketing Strategies	1. I find AI-driven digital marketing strategies helpful when making purchase decisions
	2. AI-driven digital marketing strategies improve my overall shopping experience
	3. I am more engaged with the brands that use AI for personalized marketing
	4. I prefer receiving AI-driven marketing recommendations over generic marketing messages
Influence of AI-Driven Digital Marketing Strategies on Consumer Data Privacy	1. I feel AI-driven digital marketing poses a risk to my personal data
	2. I feel companies are not transparent about how they use my data, which can cause a breach of privacy
	3. I feel that I have no control over my personal data when it is used in AI-driven marketing practices
	4. I feel that my data is not adequately protected when used in AI-driven digital marketing
Effect on Consumer Behaviour Towards Businesses	1. Concerns about data privacy affect my trust in businesses using AI-driven digital marketing strategies
	2. I am more likely to avoid businesses that I perceive as mishandling consumer data through AI-driven marketing
	3. I avoid doing business with companies that have had data breaches or privacy issues

Reference # 03J-2024-11-04-01