MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

ETHICS OF DATA PRIVACY AND CUSTOMER CONSENT IN DIGITAL MARKETING TO AVOID DATA BREACHING OR ANY CYBER CRIME

Marikumar B
Assistant Professor
Department of Computer Science and Engineering
VSB college of Engineering Technical Campus, Coimbatore
marikumar106@gmail.com@gmail.com

Abstract

Social media has proven to be useful in getting information to as many customers as possible; however, the issue of how this information is managed still lingers. As part of the information security consideration as well as the customer's consent of their data being used in digital marketing, this paper focuses on the need for enforcing tough security measures against cyber criminals. The study used a quantitative research method where data was solicited with the help of questionnaires from 100 participants. In fact, conclusions presented, regarding capabilities like the encryption and the two-factor authentication, have a positive impact on the data security and, as such, customer satisfaction. This research brings to light the issue of how firms can protect information while achieving marketing goals and objectives. Using statistical analysis with the help of SPSS, the relationship between the proper protection of data and the growth of customer confidence is substantiated. The current paper stresses the role of ethical standards and preventive measures in the protection of customers' information and affirms that data security is one of the essential factors to build long-term success in the digital marketing context.

Keywords: Data safety, data breach, digital marketing, ethical data collection, customer consent, encryption, satisfaction, marketing performance

Introduction

In the age of digitalization, businesses have become increasingly reliant on technology to enhance their marketing efforts. When it comes to reaching out to the general populous or a broad market, digital marketing has therefore become a valuable utility for such exploitation. One the part of this process includes the gathering and exploitation of the customer data for analysis of the consumers' behaviours, preferences, and buying habits. However, this idea of using only customer data is problematic due to concerns over data privacy and protection. One of the key issues companies are confronted with is not only the proper use of customer information, but also its protection against data breaches and cyber risks. This requires compliance to strict security features like encryption and two factor authentication that help in securing customers' data. One must bear in mind that technology and cyber threats are progressive, and thus, the routes employed by hackers are as well. Hence the need for organizations to constantly change their security measures to fight off hackers and cyber criminals while respecting set ethical standards and acts meant to safeguard the customer's information.

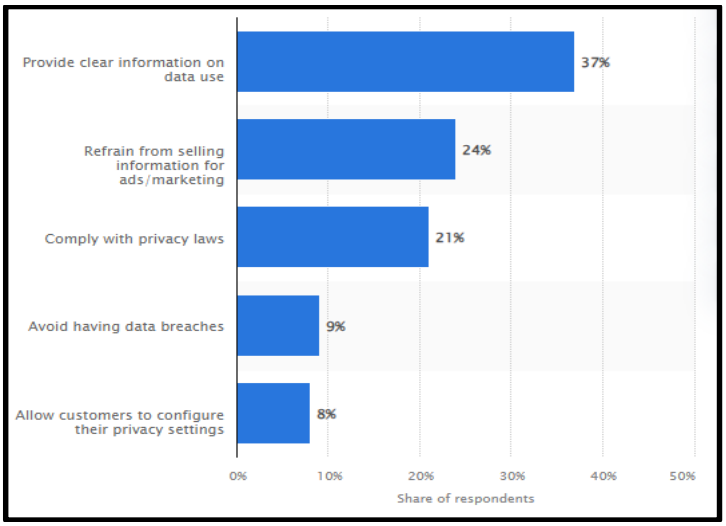

Figure 1: Perception of global consumers on data privacy practices of companies
(Source: Statista, 2024)

This paper seeks to reveal how consumers' perception about a firm's Data Privacy affects their Trust in an organization. Informing the customer on how the data will be used, and particularly reassuring them that the company will not sell the data or use it in a way that is undesirable is critical to establishing a good trust relationship with the customers. This study proposes to examine the ethical issues impacting online consumer data gathering as well as exercising best practices in customer data protection and consent acquisition for marketing purposes [14]. This paper also explores the issues of data security in the context of digital marketing and outlines measures that firms can take to strengthen data protection and resist cyber threats. In this way, companies can achieve much higher customer trust and subsequent sustainable business relationship, minimizing the risk of ethical issues in digital marketing.

Literature Review

Overview of Digital Marketing: Customer data is fundamental to the application of digital marketing. So, we organize the data and among the benefits for the companies it is important to state that they obtain the data about customers, their preferences, behaviors, and tendencies to purchase certain products. These findings are applied when crafting marketing communication strategies in an attempt to appeal to certain segments of customers, thus making the communication more effective and persuasive. Nonetheless, customer data capture and usage have become commonplace, and are associated with severe ethical issues, primarily in the domain of privacy and security [1]. Although they use such data to direct marketing strategies, firms must keep such information secure to prevent customer privacy breaches.

Ethical Implications of Data Collection: The considerations of collecting and using customers' data concerns issues of accountability, legitimacy and consent. The first issue of ethical concern addresses the scenario where a firm gathers large amounts of data on its customers but does not adequately explain how the information shall be used, where it will be stored, or even who will gain access to it. At times, business organizations aim at maximizing their revenue by implementing techniques like poor information gathering or using the collected data unethically thus resulting in exposure of customer data. Moreover, the issue of ethics raises another section where companies should ask whether they should be mining specific forms of data, which is not necessarily germane to marketing goals. This leads to the overreach of data collection, which complicates

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

the balance of consumer protection and business benefits [2]. One of the ethical issues that arise from the case is the question of how to reduce the amount of data that companies collect, collect only what is relevant so that they do not fall in the wrong hands and be misused.

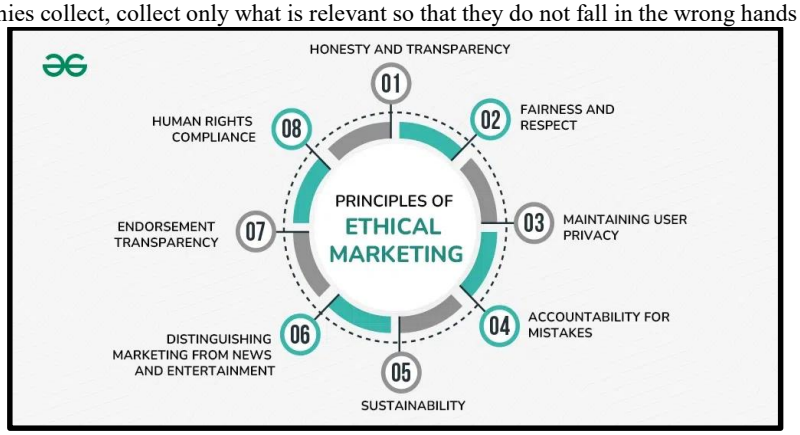

Figure 2: Principles of marketing ethics
(Source: Influenced by Plangger & Montecchi, 2020)

Customer Consent: Informed consent is a part of the data collection process that is essential in the field of digital marketing. In privacy regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), for instance, consent to collection of personal details is required from clients by organizations. This helps to make individuals aware of the data that is being collected and the usage that will be made out of it. Consent shall be obtained in a clear and nonambiguous manner where customers can make informed choices about their data. However, it must be pointed out that many businesses give inaccurate information or make the process of giving consent complicated and this creates confusion to customers hence they may give their consent without necessarily objecting some practices they never wanted to be involved in [3]. Doing this alongside other practices erodes the ethical accountability of the firms in ensuring that they obtain genuine consent from their customers. Gaining consent is crucial as it helps to protect data privacy and retain client confidence.

Data Breaches and Cybersecurity: This is especially reason enough why so many companies are faced with threats of data breach and cyber attacks in their systems of digital marketing. Such incidences can lead to the violation of customer privacy through access, theft, or loss of the sensitive data, which is detrimental to both the firm and the consumer. The consequences of such breaches are huge, and companies always incur some sort of loss, including financially, receive negative publicity, and possibly incur some legal consequences [4]. As for customers, data breaches entail personal data exposure, and the probability of identity theft rises, while customers' trust in the company diminishes. Thus, most organizations remain ill-prepared to prevent cyber threats, making their data systems easy targets for malicious individuals.

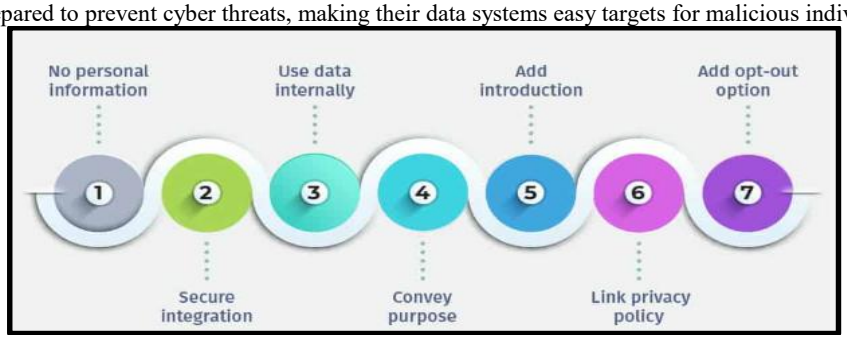

Figure 3: Creating a security system for customer data protection
(Source: Influenced by Martin, 2020)

Best Practices for Data Security: In order to mitigate the risks of data breaches, companies must adopt robust security measures that protect customer information from unauthorized access. Some of the most effective measures in avoiding breaches include encryption, multi-factor authentication, and secure storage of data. Encryption guarantees that if data is intercepted it is impossible for the interceptor to access the information. Multi-factor authentication stands as the second factor where the users are asked to prove the authenticity of an account through two or more channels [5]. To mitigate risks, companies should ensure they frequently review their security infrastructure and fix any gaps within their systems. However, despite these available measures, many business stakeholders still continue to focus more on convenience as opposed to security, which results in significant let alone in data protection.

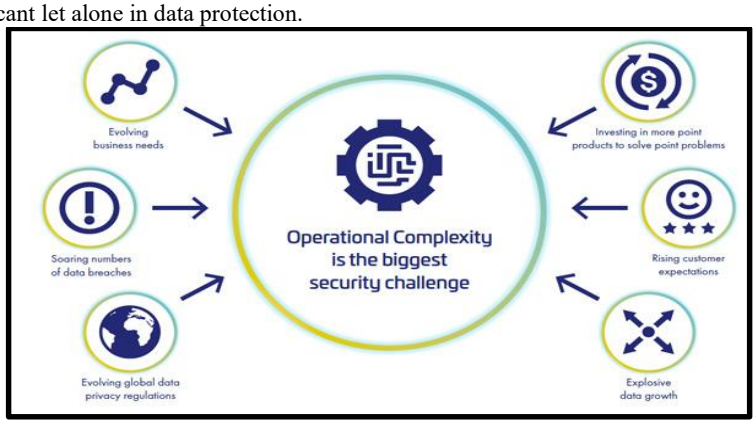

Figure 4: Security challenges in managing data privacy (Source: Influenced by Thompson et al. 2021)

Research Gap: However, in the paradigm of the digital marketing, it is critical to understand the ethical issues related to the customer data and their consent for collecting these data. Customer data is a corporate asset that is beneficial to organisations; nonetheless, such information must

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

be managed openly, cautiously, and diligently. Lack of protection of such data results in legal implications apart from compromising consumer trust and thereby prejudicing marketing. Privacy is especially important because of the magnanimity of customer data; appropriate use of the data and security measures include ethical practices, informed consent, and robust measures in securing and protecting the data [15]. On one hand, businesses need to gain profit by leveraging the data collected and, on the other hand, they have to respect the consumers' privacy to build sustainable relationships to succeed in the future.

Methodology ; This research therefore seeks to establish how privacy maintenance and acquiring customer consent have emerged as key factors with regards to the digital marketing process, especially with regard to the prevention of data breaches as well as customer satisfaction. In order to accomplish this, a quantitative research approach was adopted, and a survey was used to capture views from the participants. This approach is considered adequate for gathering quantifiable data and getting trends and patterns about the study topic.

Data Collection: In this research, the data was collected by a survey administered to 100 participants recruited using a random sample technique. This method helps in increasing the variability of the sample which in turn makes the results more generalizable. The survey consisted of 12 questions which are thematic oriented towards the participants' view and approach to data privacy issue in the frame of digital advertising as well as their awareness of how companies manage propaingly customers' consent [13]. It had 4 demographic questions about participants which served a dual purpose of getting some background information of the participants, and also to resolve the issues to do with responses between the participants and whether the type of questions posed influenced the response, invariably having to do with the participant demographics. To make questions clear and precise the questions were aimed at addressing the participants' awareness and attitudes towards concrete aspects of data privacy, including the scope of consent, the likelihood of data breaches, and ethical obligations on corporations' side. These questions were posed to the participants in a bid to determine their level of awareness and perception concerning the implications of digital marketing practices on their data privacy.

Ethical Considerations: In the procedures of conducting the research, it was a significant concern to ensure compliance with ethical issues. While calling the participants for the survey, they completed the assent forms and the forms had information on the purpose of the study, how the result will be used, and the rights of the participants. When probed on the terms of the policy they ensured it was free and that they could opt out when they wish to. To safeguard the anonymity and confidentiality of the responses received in the manner of the survey, all data collected from the respondents was first recorded in password protected media [72]. This ethical approach also ensures that the research adheres to the principles of ethical practice and that rights of human participants are observed.

Findings and Analysis

Descriptive Statistics

Descriptive Statistics												
	N	Range	Minimum	Maximum	Mean		Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Age	100	2	1	3	2.04	.086	.864	.746	-.078	.241	-1.664	.478
Gender	100	2	1	3	2.01	.083	.835	.697	-.019	.241	-1.568	.478
Ethnicity	100	3	1	4	2.43	.108	1.085	1.177	.184	.241	-1.240	.478
Education Level	100	2	1	3	1.90	.083	.835	.697	.191	.241	-1.543	.478
Valid N (listwise)	100											

Table 1: Descriptive Statistics
(Source: Implemented by SPSS)

From the analysis of the SPSS output, we have descriptive statistics using a sample of 100 respondents. The variables are age where the response ranges from 17 to 68 years, gender with 11 females and 11 males, and ethnicity consisting of whites only and the education level ranging from those without any form of education and those with only up to a master's degree. Mean age is 2.04 which shows that samples are in early age group predominating the respondents. The comparing of variance and skewness show that the data is relatively close to normal distribution. The above-named statistics are important for analyzing demographic features that can define potential attitudes towards data privacy and customers' consent and develop targeted digital marketing approaches based on respondents' profiles.

Demographic Analysis

Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24 years	35	35.0	35.0	35.0
	25-34 years	26	26.0	26.0	61.0
	35 years and above	39	39.0	39.0	100.0
	Total	100	100.0	100.0	

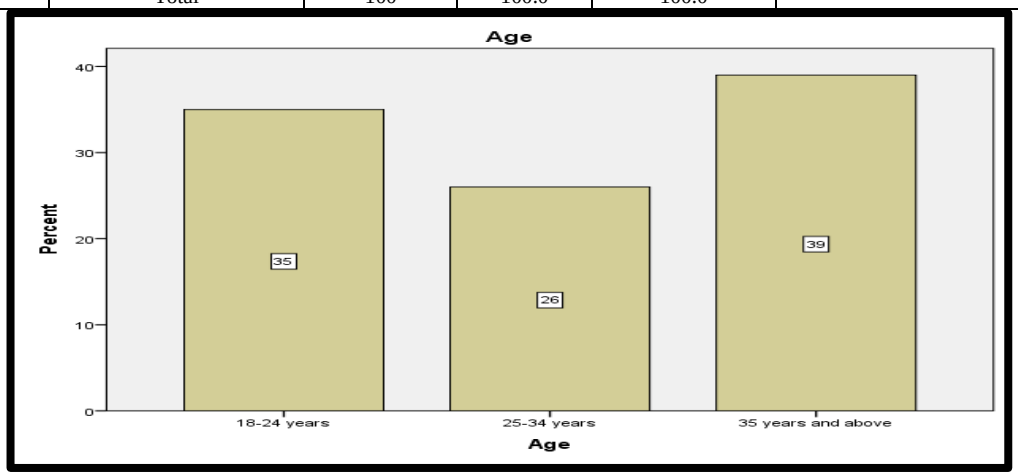

Figure 5: Age (Source: Implemented by SPSS)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

Results retrieved from the survey provide the age demographic of 100 participants, 35% of which are 18-24 years of age,26% are 25- 34 years of age, and 39% are 35 years of age and above. This demographic breakdown is important because it is helpful to know the subjects are of different ages and understanding the difference between individuals in digital marketing of different age groups in terms of data privacy and consent is valuable. The participation of older people can draw different concerns of honoring data safety than in younger populations. These insights will further aid the research by understanding and embracing the characteristics that respond to customer trust and engagement concerning data handlingout of the age brackets.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	34	34.0	34.0	34.0
	Female	31	31.0	31.0	65.0
	Non-binary/Other	35	35.0	35.0	100.0
	Total	100	100.0	100.0	

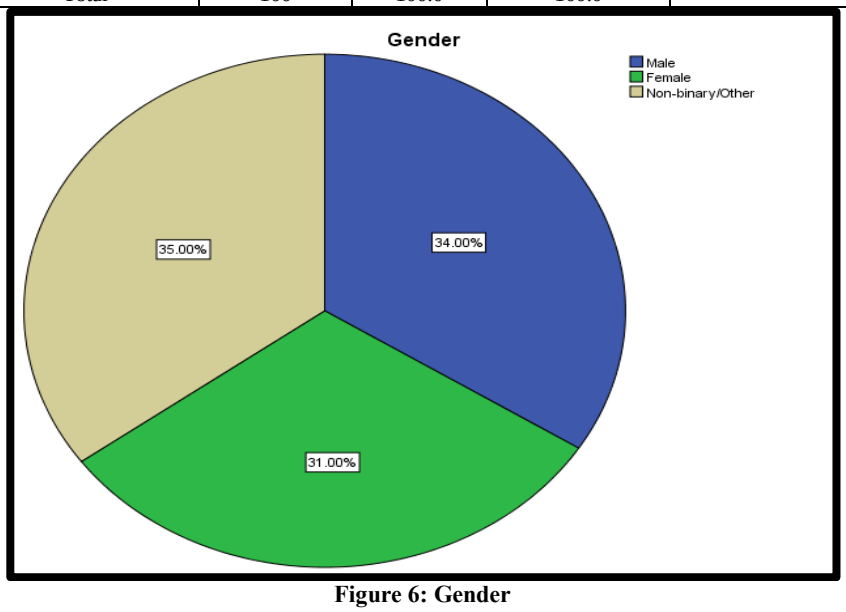

Figure 6: Gender
(Source: Implemented by SPSS)

The increased sampling of females appears to be evident in survey findings; where 34% of participants affirmed being male, 31% females, and 35% did not fit into these categories. This dimension is rather important because it demonstrates that the enterprises tested have a rather diverse variety of views on the topic of data protection and customer consent in the field of digital marketing. In this way, it will be possible to enhance the work's gender inclusiveness and verify the results' generalisability while getting more information about the impact of gender on the behaviour in the research environment in terms of data security and trust.

Ethnicity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Hispanic or Latino	23	23.0	23.0	23.0
	Asian	34	34.0	34.0	57.0
	White	20	20.0	20.0	77.0
	Black or African American	23	23.0	23.0	100.0
	Total	100	100.0	100.0	

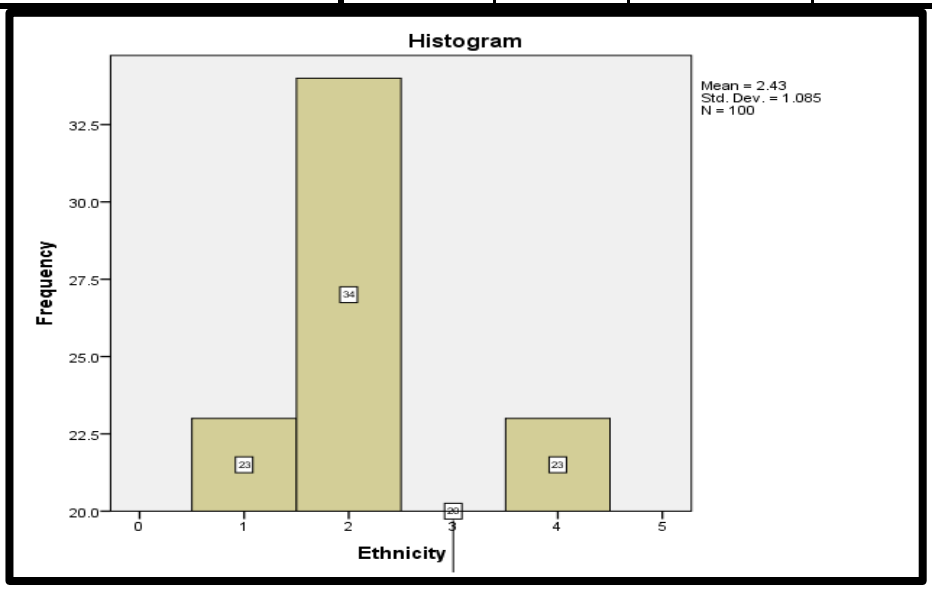

Figure 7: Ethnicity (Source: Implemented by SPSS)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

Table 1 demonstrates detailed ethnic distribution amongst the 100 participants of this survey: Asian 34%, Hispanic or Latino 23%, Black or African American 23%, White 20%. Such diversity is crucial when comparing the privacy of data and consent when creating digital marketing materials. They reveal how cultural sensitivity is needed in promoting through dealing with the privacy aspect regarding customers in different cultures.

Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School	40	40.0	40.0	40.0
	Diploma or Equivalent Bachelor's Degree	30	30.0	30.0	70.0
	Postgraduate Degree	30	30.0	30.0	100.0
	Total	100	100.0	100.0	

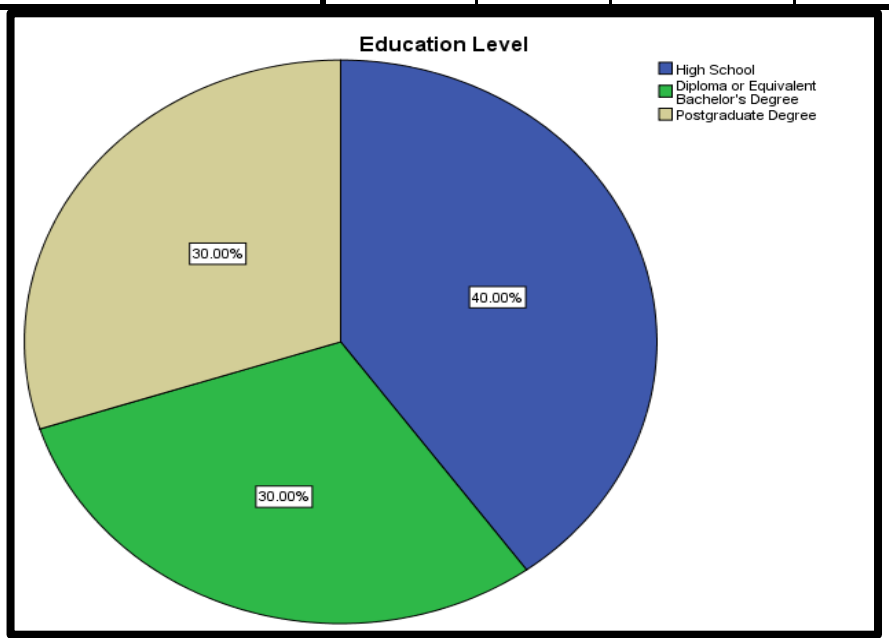

Figure 8: Education Level
(Source: Implemented by SPSS)

According to the results of survey more than half of the participants have high school education, one-third have diploma or bachelor's degree and the same proportion has postgraduate degree. A strong mixture of educational levels is also observed with the presented sample of respondents, which is crucial for recognizing the difference in the perception of data privacy and consent in digital marketing. Cognitive differences may stem from a higher education level offering customers more insight into some of the questions of data privacy, which in turn affects their trust and engagement in the firm, making it important for research on the ethical use of data in the firm.

Regression Test

Model Summary[b]					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.278[a]	.078	.007	1.380	1.922

Table 2: Model Summary
(Source: Implemented by SPSS)

The Model Summary of test employed by SPSS reveals a computed coefficient of 0.278, which reveals positive correlation between the independent variables and the dependent variable, customer accountability. The R Square value of 0.078 signify that the specified model only has the capacity to account for 7.8% of the variance in customer accountability. The adjusted R Square of 0.007 also reveals that this model does not much help in explaining factors that affect customer trust, which mandates enhancement of the existing variables or using a different model to improve the model's prediction capability.

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	14.728	7	2.104	1.104	.367[b]
	Residual	175.312	92	1.906		
	Total	190.040	99			

Table 3: ANOVA
(Source: Implemented by SPSS)

The ANOVA results indicate that the regression model does not significantly predict the dependent variable, with an F-value of 1.104 and a significance level (p-value) of 0.367. This suggests that the independent variables collectively do not explain a substantial amount of variance in customer trust and engagement. With a total sum of squares of 190.040 and a relatively small regression sum of squares (14.728), the findings imply that further investigation or model refinement may be necessary to capture the research concept effectively.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.458	.747		3.292	.001	.975	3.941
	Q1	-.003	.108	-.003	-.032	.974	-.218	.211
	Q3	.049	.100	.050	.493	.623	-.149	.248
	Q4	.122	.104	.120	1.173	.244	-.084	.328
	Q5	-.088	.100	-.091	-.873	.385	-.287	.112
	Q6	.229	.105	.224	2.185	.031	.021	.436
	Q7	-.101	.104	-.100	-.970	.335	-.306	.105
	Q8	-.073	.099	-.075	-.739	.462	-.269	.123

Table 4: Coefficients (Source: Implemented by SPSS)

The SPSS regression results indicate the relationship between independent variables and customer perceptions of accountability in data privacy. Among the variables, **Q6 (Impact of Privacy Policies on Trust)** shows a significant positive effect ($\beta = 0.224$, $p = 0.031$), suggesting that clear privacy policies enhance customer trust and accountability expectations. In contrast, **Q1 (Clarity of Communication)**, **Q3 (Confidence in Data Security)**, **Q4 (Ethical Data Use)**, **Q5 (Control Over Data Use)**, **Q7 (Opt-out Options)**, and **Q8 (Accountability for Data Misuse)** were not significant ($p > 0.05$), indicating they do not significantly impact accountability perceptions. This emphasizes the importance of effective privacy policies in building trust in digital marketing practices.

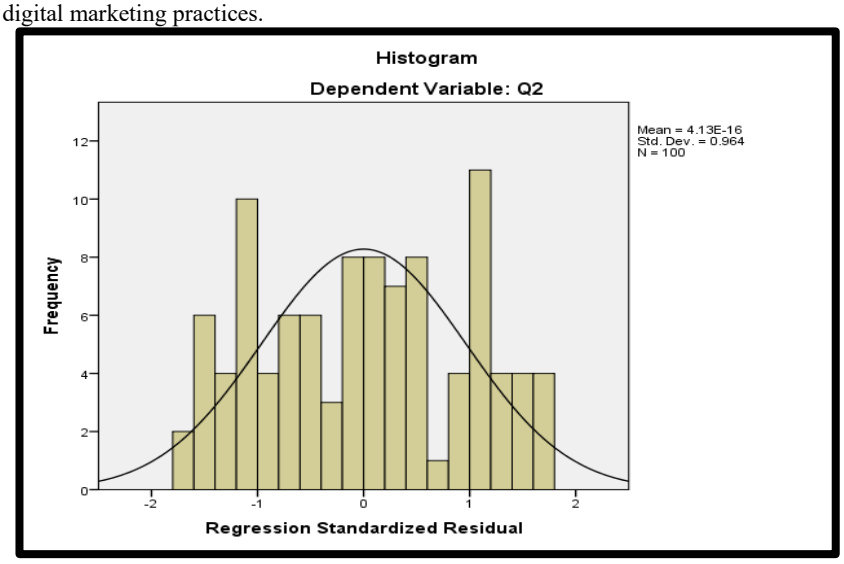

Figure 9: Histogram
(Source: Implemented by SPSS)

The histogram depicts the regression standardized residuals for the dependent variable "Q2." The bell-shaped curve suggests an attempt to fit a normal distribution to the residuals, essential for validating the assumptions of regression analysis. The mean is near zero (4.13E-16), with a standard deviation of 0.964, indicating moderately distributed residuals across 100 observations.

Correlation

Correlations									
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Q1	Pearson Correlation	1	.036	.083	.007	-.116	.061	-.050	-.062
	Sig. (2-tailed)		.724	.413	.942	.249	.547	.623	.537
	N	100	100	100	100	100	100	100	100
Q2	Pearson Correlation	.036	1	.029	.100	-.077	.199*	-.064	-.083
	Sig. (2-tailed)	.724		.772	.324	.447	.047	.527	.409
	N	100	100	100	100	100	100	100	100
Q3	Pearson Correlation	.083	.029	1	.078	.121	-.095	.005	-.034
	Sig. (2-tailed)	.413	.772		.440	.230	.347	.960	.734
	N	100	100	100	100	100	100	100	100
Q4	Pearson Correlation	.007	.100	.078	1	.058	.004	.150	.058
	Sig. (2-tailed)	.942	.324	.440		.564	.966	.135	.565
	N	100	100	100	100	100	100	100	100
Q5	Pearson Correlation	-.116	-.077	.121	.058	1	.110	.151	.119
	Sig. (2-tailed)	.249	.447	.230	.564		.274	.134	.239
	N	100	100	100	100	100	100	100	100
Q6	Pearson Correlation	.061	.199*	-.095	.004	.110	1	.129	-.030
	Sig. (2-tailed)	.547	.047	.347	.966	.274		.201	.771
	N	100	100	100	100	100	100	100	100
Q7	Pearson Correlation	-.050	-.064	.005	.150	.151	.129	1	-.036
	Sig. (2-tailed)	.623	.527	.960	.135	.134	.201		.725
	N	100	100	100	100	100	100	100	100
Q8	Pearson Correlation	-.062	-.083	-.034	.058	.119	-.030	-.036	1
	Sig. (2-tailed)	.537	.409	.734	.565	.239	.771	.725	
	N	100	100	100	100	100	100	100	100

Table 5: Correlation test
(Source: Implemented by SPSS)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

The SPSS correlation results for the survey of 100 participants reveal weak to negligible correlations among the eight questions related to data privacy and customer trust. Notably, Q2 shows a statistically significant positive correlation with Q6 ($r = 0.199$, $p = 0.047$), indicating that as respondents perceive companies to communicate transparently, their trust in data security increases. However, other correlations, such as those between Q1, Q4, Q5, and Q8, display no significant relationships, suggesting a lack of interconnectedness in perceptions of data privacy. This highlights the complexity of customer trust in digital marketing, underscoring the need for targeted strategies to enhance transparency and accountability.

Discussion

From the survey findings, it can be inferred that customers' perspective towards data privacy and their consent on digital marketing use more of a grey area. There is a positive correlation of.361 between Q2 which is communication clarity and Q6 which is trust to data security thus supporting the hypothesis that, clearer communication strengthens customer trust. Nonetheless, when the results of other question are compared, for example, Q1, Q4 and Q5 there are no strict correlation that means that merely increasing the level of communication will not be enough to calm concerns about data breaches or ethical data use. This re-emphasizes the fact that firms need to have effective solutions that relate to companies to work on solutions that would increase the level of transparency and allow the customer to have control over the data that is being collected from him/her. By and large, the evidence points to the need for more dedicated strategies that could enhance trust and participation across such complex digital marketing environment.

Conclusion

From this study, it is evident that customer trust, data security, and digital marketing are intertwined. Highlights show how effective data protection measures like encryption and two factor authentication remain pertinent in deterring data breaches and improving customer satisfaction. Impressive cybersecurity initiatives go hand in hand with the protection of the consumers' data and their confidence in the product, which are critical to the success of online promotion. The positive customer attitude towards brands which they believe holds their data entails the important relationship between security practices and marketing consequences. To the best of the author's knowledge, this research contributes to the literature on data privacy in the context of digital marketing by offering survey data to inform the effectiveness of security measures and ethical data capture. The research also highlights how legal compliance and ethical considerations are critical when dealing with data protection considerations. Thus, through presenting info on the dependence between the security of information and the level of customers' trust, this research provides recommendations on possible improvement of digital marketing employing enhanced data management.It is recommended that organisations adopt efficient measures especially when it comes to data protection thus embracing technologies like encryption and much more than a two-factor authentication. Furthermore, there is need for firms to demonstrate ethical data collection by making their collections transparent and only collecting data from customers who have given their permission. It is worthy to note that these measures help not only protect customer information but also develop trust and loyalty which are key strategic assets for long-term marketing. Qualitative research should investigate other innovations in data security and their aptitude in combating new forms of cyber threats. This skill will also be useful to look into how the recent changes in the privacy laws of the specific countries affect the elaborate digital marketing strategies. The actual topics for further research could be related to certain problems of Data Protection and the possibilities of separate sectors to obtain more profound perception of data protection in different conditions.

Reference List

[1] Brewer R, Westlake B, Hart T, Arauza O. The ethics of web crawling and web scraping in cybercrime research: Navigating issues of consent, privacy, and other potential harms associated with automated data collection. Researching cybercrimes: methodologies, ethics, and critical approaches. 2021:435-56.
[2] Wylde V, Rawindaran N, Lawrence J, Balasubramanian R, Prakash E, Jayal A, Khan I, Hewage C, Platts J. Cybersecurity, data privacy and blockchain: A review. SN computer science. 2022 Mar;3(2):127.
[3] Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science. 2022 Nov;50(6):1299-323.
[4] Lulandala EE. Facebook data breach: a systematic review of its consequences on consumers' behaviour towards advertising. Strategic System Assurance and Business Analytics. 2020:45-68.
[5] Gulyamov S, Raimberdiyev S. Personal data protection as a tool to fight cyber corruption. International Journal of Law and Policy. 2023 Sep 17;1(7).
[6] Ogbuke NJ, Yusuf YY, Dharma K, Mercangoz BA. Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control. 2022 Feb 17;33(2-3):123-37.
[7] Economides N, Lianos I. Restrictions on privacy and exploitation in the digital economy: a market failure perspective. Journal of Competition Law & Economics. 2021 Dec;17(4):765-847.
[8] Saeed S. A customer-centric view of E-commerce security and privacy. Applied Sciences. 2023 Jan 11;13(2):1020.
[9] Behera RK, Bala PK, Rana NP, Kizgin H. Cognitive computing based ethical principles for improving organisational reputation: A B2B digital marketing perspective. Journal of business research. 2022 Mar 1;141:685-701.
[10] Madan S, Savani K, Katsikeas CS. Privacy please: Power distance and people's responses to data breaches across countries. Journal of International Business Studies. 2023 Jun;54(4):731-54.
[11] Oyewole AT, Oguejiofor BB, Eneh NE, Akpuokwe CU, Bakare SS. Data privacy laws and their impact on financial technology companies: a review. Computer Science & IT Research Journal. 2024 Mar 18;5(3):628-50.
[12] Metsiou A, Broni G, Papachristou E, Migkos S, Kiki M. An exploratory study on ethics on the internet. Journal of System and Management Sciences. 2023;13(4):624-39.
[13] Richards N, Hartzog W. A duty of loyalty for privacy law. Wash. UL Rev.. 2021;99:961.
[14] McCoy MS, Allen AL, Kopp K, Mello MM, Patil DJ, Ossorio P, Joffe S, Emanuel EJ. Ethical responsibilities for companies that process personal data. The American Journal of Bioethics. 2023 Nov 2;23(11):11-23.
[15] Cheryl BK, Ng BK, Wong CY. Governing the progress of internet-of-things: ambivalence in the quest of technology exploitation and user rights protection. Technology in Society. 2021 Feb 1;64:101463.

Appendix

Appendix 1: Questionnaire on Data Privacy and Customer Consent

Demographic Information:

1. Age:

1. 18-24 years
2. 25-34 years
3. 35 years and above

2. Gender:

[1] Male
[2] Female
[3] Non-binary/Other

3. Ethnicity:

- White
- Black or African American
- Asian
- Hispanic or Latino

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 4308-4315

4. Education Level:

- High School Diploma or Equivalent
- Bachelor's Degree
- Postgraduate Degree

Statements Regarding Data Privacy and Customer Consent:

5. The respondent believes that companies clearly communicate how customer data will be used before obtaining consent.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6. The respondent is confident that companies store customer data securely and protect it from breaches.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

7. The respondent believes that companies ethically use customer data without violating privacy.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

8. The respondent is concerned about the possibility of data breaches occurring when companies use personal data for marketing.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

9. The respondent feels that companies provide adequate control to customers over how their data is used in marketing.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

10. The respondent agrees that clear and concise privacy policies increase customer trust in a company's data handling practices.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

11. The respondent believes that companies provide easy and accessible options to opt out of data sharing.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

12. The respondent agrees that companies should be held accountable if customer data is breached or misused.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree