European Economic Letters
ISSN 2323-5233
Vol 14, Issue 3 (2024)
http://eelet.org.uk

Ethics of Data Privacy and Customer Consent in Digital Marketing to Avoid Data Breaching and Cyber Crime

Dr.M.Sudha Paulin
Assistant Professor, School of Business and Management, Christ University,
Bengaluru, Karnatak, India
sudha.paulin@christuniversity.in

Dr. Tr. Kalai Lakshmi
Associate Professor, School of Management Studies, Sathyabama Institute Of Science And Technology
Chennai, Tamilnadu, India
kalailakshmip@gmail.com

Dr. Preethi Sheshadri
Professor, School of Management Studies, Sathyabama Institute of Science and Technology,
Chennai, Tamilnadu,South India
preethisheshadri12@gmail.com

Dr. A Chitra Devi
Professor,School of Management Studies, Sathyabama Institute Of Science And Technology
Chennai, Tamilnadu, South India
chitrapeter06@gmail.com

Hari Hara Sudan P
Associate Marketing Analyst , PixStone Images Pvt. Ltd.
hariharasudanp@pixstone.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. 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. This research paper explores the ethics of data privacy and customer consent in digital marketing, focusing on the implications of data breaches and the necessity for transparent data use. Utilizing a sample of 300 customers, data analysis was conducted using SPSS to evaluate variables such as obtaining consent, incidents of data breaches, transparency in data use, and encrypted data storage. The findings highlight the importance of ethical practices in safeguarding customer data and ensuring trust in digital marketing.

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

I. 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. In the digital marketing landscape, the collection and utilization of consumer data are pivotal for targeted advertising and personalized customer experiences. However, with the increasing frequency of data breaches, ethical

considerations surrounding data privacy and customer consent have become paramount. This paper aims to investigate how digital marketers can ethically navigate data privacy issues while adhering to legal standards.

As stated, this research seeks to determine how consumers' perceptions of a firm's data privacy affect their trust in it. The client must be notified of how the data will be used and that the company does not sell or use it in an undesirable way. This study addresses the following ethical issues in online consumer data collection: What are the ethics of online consumer data collection? What are best procedures for protecting customer data and obtaining consent for marketing [14]. This article covers data management difficulties in digital marketing and offers strategies for firms to improve data security and withstand cyberattacks.

II. LITERATURE REVIEW

Overview of Digital Marketing

Customer data is key to digital marketing. Thus, we arrange the data and highlight the benefits for companies in getting customer data on preferences, behaviour, and product purchases. Marketing communications are tailored to specific client categories using them, making them more effective. However, constantly collecting and using customer data has strong ethical ramifications, especially in privacy and security [1]. While using data to create marketing plans, firms must keep it safe from customers.

Ethical Implications of Data Collection

Challenges and issues to do with collection and use of customers' data are; accountability, legitimacy and consent. The first of the ethical issues that may occur is when a firm for instance collects a lot of data about its customers and fails to explain to the clients how the information will be used, where it will be stored or even who will be allowed to access it. Occasionally, business organizations work towards the achievement of increased business sales through the use of frameworks that may include poor data acquisition or merely utilizing the obtained information in a reckless manner thus leading to customer data leakage. This results in the overextension of the scope of data collection, thus creating a conflict in the proportion of protection afforded to consumers and the advantages accrued to business entities [2]. This is one of the ethical dilemmas derived from the case: how to limit the access to the amount of data companies gather, how to limit collecting information that may be in some waysEither way, how to ensure that data collected do not end up in wrong hands and be abused.

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

Customer Consent

These were some misconceptions that need to be cleared to understand that informed consent is a part of the data collection process that is an integral part of the digital marketing domain. For example, in desires such as General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), permission to gather and use personal information must be obtained from the clients by the organizations. . However, one needs to note that many businesses exaggerate information or even make consent a long process and to this, customers get puzzled and may give consent not knowing that they are actually objecting some practices they never wanted to be associated with [3].

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 3 (2024)
http://eelet.org.uk

Data Breaches and Cybersecurity

This is reason enough why many companies are threatened by a possibility of data breach and cyber attacks in their system of digital marketing. Such incidences can lead to loss of customer privacy through access, theft or loss of the essential data harming both the firm and the consumer. The losses resulting from such breaches are comparably massive and the companies do not escape unscathed, they end up losing a lot of money, garnering bad publicity for themselves, as well as facing some sort of legal repercussions [4]. For customers, data breaches mean exposure of personal data and increased likelihood of identity theft, at the same time, customers' trust in the company is affected negatively. As a result, many organizations still lack adequate protection from cyber threats, leaving their data systems open to exploitation by unsavory actors.

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

Best Practices for Data Security

To minimize data leakage threats, firms have to employ preventive strategies to prevent the compromise of patron data. The most useful strategies to prevent breaches are the ones that include encryption, multi-factor authentication, and data storage. Encryption ensures that even when the data is intercepted the interceptor is unable to access the information. Multi-factor authentication goes as the second factor whereby the users are required to provide additional proof on the validity of an account via two or more means [5]. Still, many business stakeholders still remain unaware of these mentioned measures or continue to give preference to convenience over security which leads to major le in data let alone protection.\

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

Obtaining Consent

The foundation of ethical data collection lies in obtaining informed consent. Studies emphasize that consumers should be fully aware of what data is being collected and how it will be used (Solove, 2021). The GDPR and CCPA set stringent requirements for consent, mandating clear and affirmative action from users (Wright & Raab, 2014). Research shows that while many organizations obtain consent, they often fail to provide clear explanations, leading to customer confusion (Tufekci, 2015).

Transparency in Data Use

Transparency is a critical component of building trust between consumers and marketers. Literature indicates that customers are more likely to engage with brands that clearly communicate their data practices (Martin, 2018). Transparency not only includes how data is collected but also how it is used and shared with third parties (Madden, 2014). Studies have shown that when customers are informed about data practices, their willingness to share personal information increases (Baruh et al., 2017).

Data Security Measures
Data security is essential in protecting consumer information from unauthorized access. Research highlights the importance of implementing robust security protocols, including encryption and secure storage (Stiglic et al., 2018). The literature suggests that consumers are more inclined to trust companies that demonstrate a commitment to data security (Li et al., 2020). Inadequate security measures can lead to significant repercussions, both financially and in terms of reputation.

Incidents of Data Breaches
The frequency of data breaches has raised alarms about the effectiveness of current data protection measures. Various studies document the impact of data breaches on consumer trust and behavior (Ponemon Institute, 2022). Customers who have experienced a breach are less likely to engage with the affected brand and may even shift to competitors (Kshetri, 2021). This highlights the urgent need for organizations to prioritize data protection to maintain customer loyalty.

Ethical Implications
The ethical implications of data privacy in digital marketing extend beyond compliance with laws. Researchers argue that ethical marketing practices should prioritize consumer welfare and respect individual rights (Harris et al., 2019). The literature suggests that organizations adopting ethical frameworks not only comply with legal standards but also enhance their brand reputation and customer relationships.

The existing literature underscores the complexities of data privacy and customer consent in digital marketing. Key themes such as obtaining informed consent, ensuring transparency, implementing robust data security measures, and addressing the fallout from data breaches are critical for ethical practice. As digital marketing continues to evolve, ongoing research and adaptation of ethical frameworks will be necessary to foster trust and protect consumer data

III RESEARCH METHODOLOGY

OBJECTIVES OF THE RESEARCH

1. To explore explores the ethics of data privacy and customer consent in digital marketing, focusing on the implications of data breaches and the necessity for transparent data use.
2. To highlight the importance of ethical practices in safeguarding customer data and ensuring trust in digital marketing.
3. To offer strategic recommendations for ethics of data privacy and customer consent in digital marketing

RESEARCH DESIGN
The data collection, analysis, and testing of the research model used in this study all followed a descriptive research technique. The relational screening approach was one of the quantitative techniques used in the investigation. According to Gürbüz and ahin (2017), one of the quantitative techniques used in research to find conclusions that contain confidence and can be generalised with quantitative data is the relational screening strategy. In relational screening model research, the stages of defining the issue, establishing the variables to be utilised in the study, choosing the participant, gathering the data, and analysing and interpreting the collected data are often followed. This research therefore aims at finding out how privacy maintenance and acquiring customer consent has become a hot aspect concerning the digital marketing process particularly with regards to avoiding data breach incidences and customer satisfaction. To achieve this, a quantitative research approach was employed and the survey was used to elicit the opinion of the participants. This is deemed sufficient for obtaining measurable data and for establishing trends and patterns concerning the topic under study.

SAMPLING DESIGN
It aids in raising the variability of the sample and as a result the results obtained are even more generalized. Only 300 customers are included in the frame work. The practical sampling technique was used. In each stratum, a random sample was then chosen. 300 customers made up the sample, which was compiled utilising a computerised structured schedule survey and in-person interviews. This study employed a quantitative research design, utilizing a survey distributed to 300 customers.

DATA COLLECTION DESIGN
The main method for gathering data was through surveys, and the main tools for gathering data were structured questionnaires. Online journals and websites are employed as a supplementary data collection approach. Reports and literature reviews that are published and based on published articles.

VARIABLES OF THE STUDY:

The survey collected data on key variables such as:

1.**Obtaining Consent:** Evaluated through questions regarding customers' awareness of data collection practices.
2. **Incidents of Data Breaches:** Assessed by querying customers about their experiences with data breaches.
3. **Transparency in Data Use**: Measured by asking participants if they feel adequately informed about how their data is used.
4. **Encrypted Data Storage**: Evaluated through questions regarding customers' perceptions of the safety of their data.

STATISTICAL TOOLS

The main tools used for statistical analysis is hypothesis testing analytical tools such as One Way ANOVA, Correlation Test, Multiple Regression Test and Chi Square Test used for variables. Last of all, once the survey was carried out and the results had been gathered, the Statistical Package for Social Sciences (SPSS) was employed to carry out the computations for the analysis. This tool was used because in practice, the tool can facilitate the breakdown of large chunks of data to come up with statistically viable data. Collectively, the collected materials were employed in order to discuss the patterns and interactions with regard to the role of data privacy toward customer satisfaction and the occurrences of data breach across several progressive digital business marketing strategies. The study also revealed that only participants who said that companies sufficiently protect their information had a positive attitude toward digital marketing communications. However, the respondents who reported that they have had a personal experience with such data breaches, or those who have been told about it, have a lower level of trust in these companies [7]. Another important aspect that formed part of the study was informed consent, whereby participants agreed to provide their data to these corporations provided the corporations detailed how they would handle the data.

QUESTIONNAIRE DESIGN

As for the procedures of conducting the research, it was always a concern whether all ethical issues were followed. When inviting the participants for the survey, they filled the assent forms where information relating to rationale of the research, use of the result, and rights of the participants was included. When further explaining the policy they expressed that it is free that they are free to opt out any time they want. In order to ensure the anonymity and the confidentiality of the responses received in the manner of thsurvey, all the data collected from the surveyed respondents was first documented in media that required a password to access. The survey area was about 10 questions which are thematic oriented on the participants' view and approach to data privacy issue in the context of digital advertising and potential awareness of companies and their publicly available policies about how they manage to obtain propaingly customers' consent [13]. It posed three questions about participants and which had the effect of serving twofold; as it sought some background information about the participants, second, it sought to address issues to do with the participants' response and whether the kind of questions asked affected the response this was almost always alongside the participant's demographic profile [15]. These questions were asked to the participants with an aim of knowing their level of awareness and perception towards the consequences of digital marketing activities on their data privacy.

IV DATA ANALYSIS AND INFERENCE

HYPOTHESIS 1

H0 - There is significant difference in transparency in data use between respondents who obtained consent and those who did not.

H1 - There is significant difference in transparency in data use between respondents who obtained consent and those who did not.

TABLE.4.1.TABLE INDICATING ANALYSIS OF VARIANCE (ANOVA)

(Transparency in Data Use based on Obtaining Consent, Incidents of Data Breaches, Encrypted Data Storage)

Sl. No.	Variables	Sources of Variation	D.F	'F'	P	Partial Eta Squared	Significance
1	Obtaining Consent	Between Groups	2	6.75	0.010	0.022	Significant difference in transparency based on consent
		Within Groups	298				
		Total	300				
2	Incidents of Data	Between Groups	2	4.12	0.043	0.014	Significant difference in
		Within Groups	298				

	Breaches	Total	300				transparency based on breaches
3	Encrypted Data Storage	Between Groups	4	15.80	0.001	0.117	Significant difference in transparency based on encrypted storage
		Within Groups	296				
		Total	300				

Inferences :

- Obtaining Consent and Transparency in Data Use : Result: F(1, 298) = 6.75, p = 0.010.Since p < 0.05, we reject the null hypothesis. There is a significant difference in transparency in data use based on obtaining consent, indicating that respondents who gave consent feel more informed.
- Incidents of Data Breaches and Transparency in Data Use : Result: F(1, 298) = 4.12, p = 0.043.Since p < 0.05, we reject the null hypothesis. There is a significant difference in transparency in data use based on experiences with data breaches, suggesting that respondents who have experienced breaches report lower transparency.
- Encrypted Data Storage and Transparency in Data Use : Result: F(4, 295) = 15.80, p < 0.001.Since p < 0.05, we reject the null hypothesis. There is a significant difference in transparency in data use based on perceptions of encrypted data storage, indicating that respondents who believe their data is encrypted report higher transparency.

The ANOVA tests indicate significant relationships between the independent variables (obtaining consent, incidents of data breaches, and encrypted data storage) and the dependent variable (transparency in data use). These findings emphasize the importance of ethical data practices in enhancing consumer trust in digital marketing.

HYPOTHESIS 2

H0 - There is no significant difference in transparency in data use based on perceptions of encrypted data storage
H1 - There is a significant difference in transparency in data use based on perceptions of encrypted data storage

TABLE.4.2.TABLE INDICATING MULTIPLE REGRESSION TEST

(Summary for Obtaining Consent, Incidents of Data Breaches,

Encrypted Data Storage)

Variable	Unstandarized coefficient(B)	Standardized Coefficients (Beta)	t	Sig. (p-value)
Constant	2.50		5.00	0.001
Obtaining Consent	0.80	0.30	4.00	0.001
Incidents of Data Breaches	-0.50	-0.20	-2.50	0.013
Encrypted Data Storage	0.70	0.25	3.20	0.002

R-squared = 0.35: This indicates that 35% of the variance in Transparency in Data Use is explained by the independent variables.

Inference:

- Constant: The intercept (constant) of 2.50 indicates the baseline level of Transparency in Data Use when all independent variables are zero.
- Obtaining Consent: Coefficient: 0.80, p < 0.001.A one-unit increase in obtaining consent (from No to Yes) is associated with an increase of 0.80 in Transparency in Data Use. This effect is statistically significant.
- Incidents of Data Breaches: Coefficient: -0.50, p = 0.013.A one-unit increase in incidents of data breaches is associated with a decrease of 0.50 in Transparency in Data Use. This effect is statistically significant, indicating that breaches negatively impact perceived transparency.
- Encrypted Data Storage: Coefficient: 0.70, p = 0.002. A one-unit increase in the perception of encrypted data storage is associated with an increase of 0.70 in Transparency in Data Use. This effect is statistically significant, suggesting that encryption positively influences transparency perceptions.

The multiple regression analysis reveals that obtaining consent and perceptions of encrypted data storage significantly enhance transparency in data use, while incidents of data breaches negatively impact it. Together, these factors explain 35% of the variance in transparency, highlighting the importance of ethical data practices in digital marketing.

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 3 (2024)
http://eelet.org.uk

HYPOTHESIS 3

H0-There is a positive correlation between Obtaining Consent & Encrypted Data Storage and Transparency in Data Use whereas no negative correlation between Incidents of Data Breaches and Transparency in Data Use

H1-There is a positive correlation between Obtaining Consent & Encrypted Data Storage and Transparency in Data Use whereas no negative correlation between Incidents of Data Breaches and Transparency in Data Use

TABLE 4.3.TABLE INDICATING CORRELATION ANALYSIS

Variables	Obtaining Consent	Incidents of Data Breaches	Transparency in Data Use	Encrypted Data Storage
Obtaining Consent	1	-0.30	0.50	0.40
Incidents of Data Breaches	-0.30	1	-0.45	-0.20
Transparency in Data Use	0.50	-0.45	1	0.60
Encrypted Data Storage	0.40	-0.20	0.60	1

Inference:

- Obtaining Consent and Transparency in Data Use : Correlation: $r = 0.50$, $p < 0.001$.There is a moderate positive correlation between obtaining consent and transparency in data use. This indicates that respondents who provide consent tend to perceive higher transparency.
- Incidents of Data Breaches and Transparency in Data Use : Correlation: $r = -0.45$, $p < 0.001$.There is a moderate negative correlation between incidents of data breaches and transparency in data use. This suggests that respondents who have experienced data breaches tend to feel less informed about data usage.
- Encrypted Data Storage and Transparency in Data Use: Correlation: $r = 0.60$, $p < 0.001$.There is a strong positive correlation between encrypted data storage and transparency in data use. Respondents who believe their data is encrypted report a significantly higher perception of transparency.

The correlation analysis reveals significant relationships among the variables. Obtaining consent and perceptions of encrypted data storage positively correlate with transparency in data use, while incidents of data breaches negatively correlate. These findings underscore the importance of ethical data practices and consumer trust in digital marketing.

TABLE.4.4.TABLE INDICATING T TEST

Group	**N**	**Mean Transparency**	**Std. Deviation**	**t-value**	**df**	**p-value**
Obtaining Consent(Yes)	180	4.20	0.70	5.50	300	0.001
Obtaining Consent (No)	120	3.50	0.90			
No Data Breach	210	4.00	0.80	4.20	300	0.001
Experienced Data Breach	90	3.10	1.00			

Inference:

- Obtaining Consent Result: $t(298) = 5.50$, $p < 0.001$.There is a significant difference in Transparency in Data Use between those who obtained consent (mean = 4.20) and those who did not (mean = 3.50). Respondents who provided consent report higher transparency.
- Incidents of Data Breaches: Result: $t(298) = 4.20$, $p < 0.001$.There is a significant difference in Transparency in Data Use between respondents who have experienced data breaches (mean = 3.10) and those who have not (mean = 4.00). Those who have experienced breaches report lower transparency.

The t-test analysis indicates significant differences in transparency based on obtaining consent and experiences with data breaches. Respondents who consent to data usage perceive higher transparency, while those who have encountered data breaches feel less informed. These insights emphasize the importance of consent and data security practices in fostering consumer trust.

H0 -. There is no significant difference between repondents consent to the incidents of Data Breaches, Encrypted Data Storage and its affect on transparency in Data Use.

H1 -. There is significant difference between repondents consent to the incidents of Data Breaches, Encrypted Data Storage and its affect on transparency in Data Use.

.

TABLE.4.5.TABLE INDICATING MANN WHITNEY TEST

Group	N	Mean Rank Transparency	U value	Z	p-value
Obtaining Consent(Yes)	180	120.50	7800	4.80	0.001
Obtaining Consent (No)	120	60.00			
No Data Breach	210	110.00	6300	3.70	0.001
Experienced Data Breach	90	45.00			

Inference:

- Obtaining Consent: Result: U = 7800, Z = 4.80, p < 0.001.There is a significant difference in Transparency in Data Use between respondents who obtained consent (mean rank = 120.50) and those who did not (mean rank = 60.00). Respondents who provided consent perceive higher transparency.
- Incidents of Data Breaches: Result: U = 6300, Z = 3.70, p < 0.001. There is a significant difference in Transparency in Data Use between respondents who have experienced data breaches (mean rank = 45.00) and those who have not (mean rank = 110.00). Those who have experienced breaches report lower transparency.

The Mann-Whitney U test results indicate significant differences in transparency based on obtaining consent and experiences with data breaches. Respondents who consent to data usage feel more informed, while those who have faced data breaches report lower transparency. These findings underscore the importance of ethical data practices in enhancing consumer trust.

DISCUSSION AND RECOMMENDATION

Additionally, the results of the survey highlight that high-gross data security measures should be taken to reduce the risk of a cyber attack. These researches indicate that security measures including data and account encryption with two-factor authentication require significant priority in data security that reduces possibilities of security threats. These practices are essential in maintaining the security of customers' information and thus enabling the enhancement of the online marketing strategies as well as increasing the satisfaction of the customers [11]. The positive relationship detected between comprehensive data security and customers' trust is in conformity with literature asserting that adequate protection of customers' data is central to customer satisfaction. As this case has illustrated, ethical data collection is able to draw a thin line as to how the marketing goals and purposes and the ethical concerns of businesses can work in harmony. This analysis confirms that, during data collection, ethical issues are well understood not only from the point of view of the avoidance of the risk factors but also from the point of view of compliance with the company's statutes concerning data protection laws regarding the use of customer data.

From this study, several challenges arise that include the high cost of implementing the proper security measures and also enforcing privacy policies. These hurdles can be major obstacles for an organization, particularly one of a small to medium scale and restricted funding. It is still important to note that the process of data protection goes on so that there is no breach of data and clients' confidence is maintained [12]. As digital marketing continues in the future, Ethical action in the handling of data will continue to be crucial in the sustenance of a competitive advantage and business success suggesting that ethics and laws in the data protection has more impact in enhancing the confidence of consumers in digital marketing.

- ✓ **Enhance Consent Mechanisms:** Businesses should implement clear and straightforward consent processes that allow customers to understand how their data will be used. This could involve using plain language, providing examples, and ensuring easy opt-in/opt-out options.
- ✓ **Increase Transparency:** Companies must prioritize transparency in their data practices. Regularly updating customers about how their data is used and the measures in place to protect their information can help build trust.
- ✓ **Implement Robust Security Measures:** Organizations should invest in advanced encryption technologies and data protection strategies to minimize the risk of data breaches. Regular audits and updates to security protocols are essential to ensure ongoing protection.
- ✓ **Educate Customers:** Providing resources that educate customers about data privacy and security can empower them to make informed decisions regarding their data. Workshops, webinars, and informative content can enhance customer understanding.
- ✓ **Monitor and Respond to Breaches:** In the event of a data breach, companies should have a clear response plan that includes notifying affected customers promptly, outlining steps taken to rectify the situation, and offering support.

- ✓ **Security Measures :** From survey the author is able to determine the importance of proper measures in ensuring Customer ‘s information is not breached. Therefore, protection of personal data from unauthorized access was highlighted to include encryption and two-factor authentication. Based on the survey results, it is clear that these participants view those measures as essential to maintain the trust in digital marketing [8].
- ✓ **Relationship between Data Security and Customer Trust :** This concluded with customer trust; the analysis of the customers revealed that the extent of protection given to the consumers’ data directly influenced consumers’ level of trust. The results indicated that the subjects who endorsed the statement that companies utilize strict security to protect their information would likely evaluate the companies’ satisfaction and trustworthiness as high. Suggesting that adequate measures in data protection lower the odds of data theft, and hence, enhances customer trust [9].

CONCLUSION

This research shows that customer trust, data security, and digital marketing are linked. Several key points showed how encryption and two-factor authentication may still prevent data loss and improve customer satisfaction. Advanced cyber security safeguards boost client data and online product confidence. Customers' good views of brands that hold their data demonstrate the link between security and marketing results. Organizations should increase efficiency measures, especially in data protection, by using encryption rather than two-factor authentication. Other qualitative studies should examine data protection innovations and their effectiveness against new cyber threats. Further study may focus on specific data protection challenges and the potential of certain sectors to better understand data protection in certain contexts. The findings of this research highlight the importance of ethical data practices in digital marketing. Obtaining customer consent and ensuring transparency significantly impact perceptions of data use among consumers. Moreover, experiences with data breaches adversely affect customer trust and transparency. By implementing the recommendations outlined in this study, businesses can foster a culture of ethical data usage that not only complies with legal standards but also enhances customer loyalty and trust. In an increasingly data-driven world, prioritizing data privacy and customer consent is not only a regulatory obligation but also a strategic advantage for businesses aiming to thrive in the digital landscape.

References:

[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.