International Journal of Internet, Broadcasting and Communication Vol.15 No.2 227-239 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.2.227

IJIBC 23-2-26

The Ethics of AI in Online Marketing: Examining the Impacts on Consumer privacy and Decision-making

Preeti Bharti and Byungjoo Park*

Doctor's Course, Department of Multimedia Engineering, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
**Professor, Department of Multimedia Engineering, Hannam University*
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
*1112preeti@gmail.com, bjpark@hnu.kr**
**Correspondent Author: Byungjoo Park* (bjpark@hnu.kr)*

Abstract

Online marketing is a rapidly growing industry that heavily depends on digital technologies and data analysis to effectively reach and engage consumers. For that, artificial intelligence (AI) has emerged as a crucial tool for online marketers, enabling marketers to analyze extensive consumer data and automate decision-making processes. The purpose of this study was to investigate the ethical implications of using AI in online marketing, focusing on its impact on consumer privacy and decision-making. AI has created new possibilities for personalized marketing but raises concerns about the collection and use of consumer data, transparency and accountability of decision-making, and the impact on consumer autonomy and privacy. In this study, we reviewed the relevant literature and case studies to assess the potential risks and make recommendations for improving consumer protection. The findings provide insights into ethical considerations and offer a roadmap for balancing the advantages of AI in online marketing with the protection of consumer rights. Companies should consider these ethical issues when implementing AI in their marketing strategies. In this study, we explored the concerns and provided insights into the challenges posed by AI in online marketing, such as the collection and use of consumer data, transparency, and accountability of decision-making, and the impact on consumer autonomy and privacy.

Keywords: *Online Marketing, Artificial Intelligence, Ethics, Consumer Privacy, Decision-Making, AI Algorithms, AI-Powered Advertising, Digital Age Privacy.*

1. INTRODUCTION

The Online marketing sector has seen a rapid transformation because of AI, which has created new potential for customer engagement and customization. It is increasingly being used in online marketing to analyze consumer data, personalize marketing messages, and automate decision-making processes [1]. However, AI

Manuscript Received: April. 14, 2023 / Revised: April. 17, 2023 / Accepted: April. 20, 2023
Corresponding Author: bjpark@hnu.kr
Tel: +82-42-629-8489, Fax: +82-42-629-8489
Professor, Department of Multimedia Engineering, Hannam University, Korea

can improve online marketing efficiency and effectiveness, but it also raises ethical concerns, particularly regarding consumer privacy and decision-making.

Regarding consumer privacy, AI algorithms can collect and evaluate much information about consumers, which can be used to target them with personalized offers and advertisements. AI algorithms can affect consumers in terms of decision-making by providing customized recommendations and personalized advertisements [2]. This poses issues about the ethical consequences of collecting and using this data and the potential for abuse or misuse. Furthermore, AI algorithms get the opportunity to monitor and track consumer behavior, which can violate rights to privacy and a lack of control over how their data is used.

In this study, we aim to explore these concerns by examining the privacy issues raised by AI in online marketing and the implications for consumer data security. Additionally, we will examine the accountability and transparency of AI decision-making in online marketing and how it affects consumer autonomy and privacy rights. We will also investigate the effect of AI-driven marketing and advertising on consumer choice and privacy. By identifying the ethical issues related to AI use in online marketing and its effects on consumer privacy and decision-making, we hope to provide valuable insights into the challenges posed by this technology. Finally, we will make suggestions for enhancing consumer safety and privacy in the context of AI-driven online advertising.

This study offers a roadmap for ensuring that the advantages of AI in online marketing are balanced with the protection of consumer privacy and decision-making rights and contributes to the continuing discussion on the ethics of AI and its impact on society, and also provides recommendations for marketers, policymakers, and researchers to address these challenges and promote ethical AI in online marketing.

The methodology adopted in this study will ensure a comprehensive and multi-disciplinary approach to examining the ethics of AI in online marketing and its impact on consumer privacy and decision-making The combination of qualitative and quantitative research methods will provide a rich and diverse data set for analysis and increase the research findings' validity and reliability. The qualitative method includes a comprehensive review of the relevant literature on the ethics of AI in online marketing, consumer privacy, and decision-making and also analyzing relevant case studies to understand the practical implications of AI in online marketing on consumer privacy and decision-making, and the quantitative method includes an online survey of 300 AI (in online marketing) consumers from different countries across the continents.

2. METHODOLOGY

Literature Review: The first step in this research will be a comprehensive review of the relevant literature on the ethics of AI in online marketing, consumer privacy, and decision-making This review will be conducted using academic databases, such as JSTOR and Google Scholar, and scholarly journals in the field of marketing, ethics, and privacy.

Case Studies: The second step will be analyzing relevant case studies to understand the practical implications of AI in online marketing on consumer privacy and decision-making These case studies will be selected based on their relevance to the research objectives and will be analyzed using a qualitative research approach.

Surveys: A survey has been conducted to gather data from consumers on their perceptions of AI in online marketing, including their views on privacy and decision-making. The survey has been conducted online and is open to everyone who uses online marketing.

Data Analysis: The data collected through the literature review, case studies, and surveys will be analyzed

using both qualitative and quantitative research methods. The data will be analyzed to identify trends and patterns, draw conclusions, and make recommendations.

Statistical Analysis: The data from the survey has been coded and entered in SPSS (Statistical Product and Service Solutions from IBM) Version 29.0 software. Simple descriptive statistics analyses have been employed.

The methodology adopted in this research will ensure a comprehensive and multi-disciplinary approach to examining the ethics of AI in online marketing and its impact on consumer privacy and decision-making The combination of qualitative and quantitative research methods will provide a rich and diverse data set for analysis and increase the research findings' validity and reliability.

2.1. LITERATURE REVIEW

The rise of technology and the vast potential of AI in online marketing are limitless. The rapid advancement of AI has revolutionized the way businesses conduct online marketing; it is increasingly used in operational markets to identify risks, conduct consumer research, and coordinate business functions with target consumers [3]. AI has become an increasingly popular tool in the field of online marketing, offering numerous benefits; however, the use of AI also raises significant ethical concerns that may result in unintended consequences on individuals, society, and the environment [1].

The ethical considerations surrounding AI in online marketing are often discussed in the literature on AI ethics. The four key ethical concerns have been identified: transparency, privacy, fairness, and accountability [4]. These concerns are particularly relevant to online marketing, where AI is used to analyze customer data and make decisions based on such information.

2.1.1. Ethical Challenges of AI

AI technology presents a range of ethical challenges, including transparency, privacy, fairness, and accountability.

One of the most significant ethical concerns with AI is transparency. AI systems are often considered "black boxes" making it difficult for consumers to understand how they are being targeted or how decisions are being made [5, 6]. Transparency in AI decision-making is essential for understanding how and why certain decisions are being made on behalf of consumers. It also prompts questions about who should have access to this information and for what purposes. Lack of transparency makes it difficult to hold AI systems accountable, leading to concerns about the potential for abuse and misuse and also to mistrust and suspicion among customers [7]. Therefore, it is important for marketers to be transparent about the use of AI in marketing and provide clear explanations of how AI is being used to target customers.

Privacy is the second most important ethical concern related to AI [8]. In today's digital world, AI algorithms collect and analyze vast amounts of consumer data, that can include sensitive personal information such as demographic data, online behavior, and purchase history. While this data can be used to create personalized recommendations and enhance user experience, it can also pose a significant threat to consumer privacy [9]. One of the main concerns related to the use of AI in data collection is the potential for data breaches. If companies fail to secure this data properly, it could be accessed by unauthorized third parties, leading to identity theft, financial loss, and other privacy violations. This information could be used to manipulate consumers into making purchases or engaging in behaviors they may not otherwise do. Such manipulation can harm consumers and lead to ethical violations. Another significant concern is the potential for AI algorithms to make decisions based on biased data sets. This can lead to unequal treatment and a violation of the principle

of fairness.

Fairness is also widely recognized as a crucial concern of AI ethics. In particular, there is concern that AI systems may perpetuate existing biases and discrimination, leading to unequal outcomes for different groups, that can have a significant impact on public values such as dignity and justice [4]. This problem has been seen in various areas, including hiring algorithms that disadvantage women and algorithms used in the criminal justice system that perpetuate racial bias [10, 11]. Therefore, preventing unfair biases in AI systems is essential to promote social fairness. To achieve this, AI and autonomous systems should not impair individuals' autonomy, and the decision-making process should be made more transparent while identifying the entities accountable for the decisions made by the system.

The principle of accountability is frequently cited as the fourth most important principle in AI ethics. Its primary focus is on addressing issues related to liability [4]. The goal is to ensure that responsibility is assigned, and harm is prevented. AI systems are often proprietary, and their algorithms are not publicly available, making it difficult to determine who is responsible for decisions made by these systems. Companies using AI in online marketing should be accountable for the outcomes of their decisions and actions related to the AI system. They should be able to explain and justify the use of AI, and consumers should have a way to challenge those decisions. This helps to minimize issues related to culpability. It's important to ensure both technical and social accountability throughout the entire system, from development to implementation and operation. Accountability is closely tied to transparency, as it's necessary to understand the system in order to make informed decisions about liability.

2.2. CASE STUDY

As AI systems continue to revolutionize in every field, however, there have been instances of ethical failures within these systems. This case study examines six examples (as shown in Table 1) of how AI in online marketing has caused ethical concerns and impacted users' privacy and security.

Table 1. Case study

Case Study	Company	Issue
TikTok's Personal Data Collection (2021)	TikTok	Collection of vast amounts of personal data from users, including location data and browsing history
Amazon's Rekognition Technology (2021)	Amazon	Use of facial recognition technology (Rekognition)
Google's Location Tracking (2021)	Google	Location tracking, even when users have turned off location services
Facebook's Facial Recognition	Facebook	Use of facial recognition technology

Technology (2019)	for suggesting tags for friends
Amazon's Alexa Amazon Devices (2018)	Recording and storing of users' voice recordings without their knowledge or consent
Google Street View Program (2010)	Google Collection of personal data from unsecured Wi-Fi networks

2.2.1. Tiktok's Personal Data Collection (2021)

TikTok, owned by Chinese company Byte Dance, has rapidly grown in popularity among young people worldwide due to its short-video format and unique algorithm that shows personalized content based on user behavior. However, this has also raised concerns about the data that TikTok collects and how it is being used.

In 2021, TikTok faced backlash from lawmakers, regulators, and privacy advocates for collecting vast amounts of personal data from its users, including location data, device information, and browsing history [12]. Critics argued that this could be used to track users and build detailed profiles of their personal lives, potentially putting them at risk of identity theft and other forms of cybercrime.

TikTok also faced accusations of sharing user data with the Chinese government, which raised concerns about national security and foreign influence [13]. In response, TikTok denied the allegations, stating that user data is stored in the United States and Singapore, with strict access controls and data security measures in place.

Despite these assurances, TikTok's personal data collection practices remain controversial, and the app continues to face scrutiny from lawmakers and privacy advocates. In response, TikTok has announced new measures to improve transparency and user privacy, such as providing clearer explanations of how data is collected and used and allowing users to control their data preferences.

The TikTok case highlights the growing importance of data privacy and security in the age of social media and big data. As more people share their personal information online, companies must ensure that they are transparent and ethical in their data collection and use practices to protect users' privacy and build trust with their audience. Furthermore, government regulations and oversight may become necessary to ensure the protection of user data from misuse and unauthorized access.

2.2.2. Amazon's Rekognition Technology (2021)

In 2016, Amazon released its facial recognition technology, Rekognition; it is a facial recognition system that uses artificial intelligence to identify and track individuals in real time. The technology was marketed as a tool that could aid in identifying and tracking criminals and suspects quickly and efficiently, so it quickly gained popularity in law enforcement agencies across the United States.

However, it has raised serious concerns about privacy violations and the potential for bias and discrimination. Critics argue that the technology could be used to unfairly target, and track individuals based on their race, ethnicity, or other characteristics, leading to unfair treatment and discrimination. There have also been concerns about the accuracy of the technology, particularly in identifying individuals of different races

and genders.

In response to these concerns, Amazon has introduced new policies to address potential issues with Rekognition. For instance, the company has limited the use of its technology by law enforcement agencies and introduced new safeguards to prevent potential misuse. Amazon has also committed to working with government officials and civil rights groups to address concerns and develop policies that promote fairness and equity [14].

Despite these efforts, concerns about Rekognition and other facial recognition technologies continue to be raised. Many critics argue that the technology should be banned outright, while others call for more stringent regulations to ensure that its use is limited and regulated appropriately [15]. As the debate over facial recognition technology continues, it is likely that we will see continued scrutiny and debate over the role that these tools should play in our society.

2.2.3. Google's Location Tracking (2021)

In recent years, Google has been criticized for its location-tracking practices, which have been perceived as invasive and potentially compromising user privacy. One particular issue that drew criticism was Google's collection of users' location data even when they had turned off location services. This raised concerns about the security of personal data collected by Google and how it was being used. Many users felt that their privacy was being violated, and some even accused the company of using their data for profit without their consent. In response to these concerns, Google introduced new privacy settings that give users more control over their location data. These settings allow users to choose whether they want their location data to be collected and shared with Google and to specify which apps are allowed to access their location data.

Additionally, Google has made it easier for users to see and manage their location history, giving them more transparency about how their data is being used. The company has also taken steps to improve the security of user data by implementing encryption and other security measures.

Despite these efforts, some critics argue that Google's location-tracking practices still raise significant privacy concerns and that more needs to be done to protect users' personal data. Nonetheless, Google's response to the criticism demonstrates a willingness to address user concerns and improve privacy protections.

2.2.4. Facebook's Facial Recognition Technology (2019)

Facebook, one of the world's largest social media platforms, has come under scrutiny for its facial recognition technology. The feature scans users' photos to suggest tags for friends but has raised concerns about privacy violations. In particular, users need to be informed and allowed to opt out of this feature, but Facebook did not provide a clear way to disable it.

Privacy advocates have been vocal about their concerns, arguing that facial recognition technology raises serious privacy issues. In 2019, the American Civil Liberties Union (ACLU) filed a complaint with the Federal Trade Commission (FTC), stating that Facebook had violated users' privacy by collecting and storing their biometric data without their consent (E&T, 2019). The complaint argued that Facebook's facial recognition technology should be subject to the same regulations as other biometric data, such as fingerprints and DNA.

Facebook has responded to these concerns by making changes to its facial recognition technology. In 2019, the company announced that it would no longer offer the feature and paid a record-breaking $5 billion penalty [16]. Additionally, Facebook has introduced new privacy settings that allow users to control how their biometric data is used on the platform. However, critics argue that these changes do not go far enough and that

users should have the ability to opt-out of facial recognition technology entirely.

The issue of facial recognition technology and privacy is not unique to Facebook. Many other tech companies, including Google and Apple, use similar technology in their products. However, the controversy surrounding Facebook's facial recognition technology highlights the need for greater transparency and regulation in the use of biometric data [17].

2.2.5. Amazon's Alexa Devices (2018)

Amazon's Alexa is a virtual assistant that responds to voice commands and performs various tasks, such as playing music, setting alarms, and ordering products online. The device is always listening for its wake word, which is usually "Alexa." When it hears the wake word, it records the user's voice and sends the recording to Amazon's servers for processing. In April 2019, a report by Bloomberg revealed that Amazon's Alexa devices had been recording and storing users' voice recordings without their knowledge or consent. The report stated that Amazon had a team of contractors who listened to the recordings to improve the accuracy of the device's speech recognition [18].

The report sparked outrage among privacy advocates and customers, who felt that their personal data was being used without their consent. Amazon faced criticism for not being transparent about collecting voice data and for not giving users an easy way to delete their recordings.

In response to the scandal, Amazon took several steps to address the issue and regain the trust of its customers. First, the company introduced a new privacy setting that allowed users to delete their voice recordings. The setting was easy to use and could be accessed through the Alexa app or Amazon's website [19].

Second, Amazon reviewed its policies and practices related to the collection and storage of voice data. The company stated that it would no longer store recordings unless users specifically opted-in to the service. Additionally, Amazon stated that it would provide more transparency about using voice data and how it is stored and processed [20].

Third, Amazon announced that it would give users more control over their voice data. The company introduced a new feature that allowed users to opt out of having their voice recordings reviewed by contractors. Users could still use the Alexa device, but their recordings would not be used to improve the device's speech recognition [20].

The Alexa voice recording scandal was a wake-up call for Amazon and other companies that collect and store personal data. It highlighted the importance of transparency and user control when it comes to data privacy. Amazon took the scandal seriously and responded quickly with new privacy settings, policies, and features. These measures helped to address the concerns of its customers and regain their trust. However, the incident also showed that companies must be vigilant about data privacy and security and take proactive steps to protect their users' personal information.

2.2.6. Google Street View Program (2010)

Google Street View is a popular feature of Google Maps that allows users to see panoramic views of streets and locations around the world. The program uses special cameras mounted on vehicles to capture 360-degree images of streets and buildings. In May 2010, the German government requested that Google audit its data collection practices after discovering that the Street View program had collected personal data from unsecured Wi-Fi networks in Germany [21]. Google initially denied that it had collected any personal data but later

admitted that it had collected data "mistakenly."

The personal data collected by Google included emails, passwords, and other sensitive information. The company admitted that it had not properly notified individuals that their personal data was being collected, nor did it obtain proper consent. This event sparked investigations by governments around the world and raised concerns about privacy violations and the security of personal data collected by Google [22]. In response to the incident, Google apologized for the mistake and announced that it would improve its data collection practices. The company also agreed to delete the personal data that it had collected from unsecured Wi-Fi networks. Additionally, Google introduced new privacy features that allowed users to opt out of the Street View program and to have their homes and businesses blurred from the Street View images. The company also implemented new policies and procedures to ensure that personal data was collected and stored securely and that individuals were properly notified and given their consent.

The Google Street View privacy violation incident was also a wake-up call for the company and other organizations that collect and store personal data. It highlighted the importance of transparency and user consent when it comes to data privacy. Google took the incident seriously and responded with new privacy features, policies, and procedures to ensure that personal data was collected and stored securely and that individuals were properly notified and gave their consent. However, the incident also showed that companies must be vigilant about data privacy and security and take proactive steps to protect their users' personal information.

3. SURVEY DATA ANALYSIS

Despite AI technologies being widely recognized for their usefulness, they are also associated with ethical concerns. To ensure that AI technologies promote ethical well-being, various guidelines, principles, and regulatory frameworks have been established. However, the implications of these AI ethics principles and guidelines remain a subject of debate. To investigate the importance of AI ethics principles and the challenges they present, we conducted an empirical survey of 300 AI (in online marketing) consumers from different countries across all continents. Based on the survey data provided, out of 300 participants, 52% identified as female, 46.3% identified as male, and 1.7% preferred not to say. Our study confirms that transparency, privacy, and accountability are the most critical AI ethics principles, while a lack of ethical knowledge, legal frameworks, and monitoring bodies are the most common AI ethics challenges. An analysis of the challenges' impact on AI ethics principles reveals that conflict in practice is a highly severe challenge.

3.1 Transparency:

As shown in Table 2, it appears that a majority (59%) of respondents answered "Yes" when asked if they were more likely to trust a brand if it was transparent about its use of AI in marketing. Meanwhile, 28.7% of respondents answered "Maybe," and 12.3% answered "No."

Additionally, when asked how important it is for companies to be transparent about their use of AI in marketing activities, 45.7% of respondents answered "Extremely important," 40.3% answered, "Important," 11.3% answered, "Slightly important," and only 2.7% answered "Not important at all" (Table 2). These results show that transparency about the use of AI in marketing activities is important to a majority of respondents, with almost half considering it "extremely important." This suggests that companies that are transparent about their use of AI in marketing may be viewed more favorably by consumers, and those that are not transparent may be viewed less favorably.

Table 2. Frequency table

Are you more likely to trust a brand if they are transparent about its use of AI in marketing?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Maybe	86	28.7	28.7	28.7
	No	37	12.3	12.3	41.0
	Yes	177	59.0	59.0	100.0
	Total	300	100.0	100.0	

How important are companies to be transparent about using AI in their marketing activities?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Extremely important	137	45.7	45.7	45.7
	Important	121	40.3	40.3	86.0
	Not important at all	8	2.7	2.7	88.7
	Slightly important	34	11.3	11.3	100.0
	Total	300	100.0	100.0	

3.2 Privacy:

The SPSS descriptive data set shown in Table 3, provides information about the central tendency and variability of responses from 300 individuals for four questions related to personal data protection in online marketing and the use of AI in online marketing. The responses are measured on a scale of 1 to 5, where 1 indicates a low level of importance or comfort, and 5 indicates a high level.

For the first question about the importance of protecting personal data in online marketing, the mean score is 1.58, indicating that, on average, respondents consider protecting their personal data in online marketing to be 'somewhat important,' but the standard deviation of 0.941 suggests that there is considerable variability in the responses.

For the second related to the belief in AI invading privacy in online marketing, the mean score is 2.26, suggesting that respondents have 'some concerns' about AI invading their privacy in online marketing, whereas the standard deviation of 1.226 indicates that there is a considerable amount of variability in the responses.

For the next question related to the comfort with online marketing targeted based on personal data, the mean score is 2.81, indicating that, on average, respondents are 'somewhat comfortable' with online marketing being targeted to them based on personal data, whereas the standard deviation of 1.509 suggests that there is a considerable amount of variability in the responses.

Lastly, in the question about concerns regarding companies using personal data for AI-enabled marketing, the mean score is 2.30, suggesting that respondents have some concerns about companies collecting and using their data for AI-enabled marketing. The lower standard deviation of 0.604 suggests indicates that there is less variability in the responses compared to the other questions.

Overall, the data suggests that protecting personal data is important to the majority of respondents, and there is some level of concern about the use of AI in online marketing and the collection of personal data by companies.

Table 3. Descriptive statistics

		How important is protecting your personal data in online marketing to you?	Do you believe AI is invading your privacy in online marketing?	How comfortable are you with online marketing being targeted to you based on personal data collected from you?	How do you feel about companies collecting and using your data for AI-enabled marketing?
N	Valid	300	300	300	300
	Missing	0	0	0	0
Mean		1.58	2.26	2.81	2.30
Std. Error of Mean		.054	.071	.087	.035
Median		1.00	2.00	2.00	2.00
Mode		1	1	2	2
Std. Deviation		.941	1.226	1.509	.604
Minimum		1	1	1	1
Maximum		4	5	5	3

3.3 Accountability:

Based on the data below in Table 4, there is a strong agreement among the respondents that companies should take more measures to protect user data when using AI for online marketing (valid percent = 68.7%, with 40% strongly agreeing and 28.7% agreeing). Similarly, there is a considerable percentage of agreement that companies should be held responsible for any unintended consequences of using AI in online marketing, such as biased decision-making or discriminatory practices (valid percent = 52.6%, with 38.3% agreeing and 14.3% strongly agreeing). Regarding consumers' right to opt-out of being targeted by AI-driven marketing campaigns, there is a mixed response. While a significant percentage agrees that consumers should have this right (valid percent = 60%, with 35% agreeing and 24.7% strongly agreeing), there is also a considerable percentage of neutral responses (30.7%), suggesting that some respondents may not have a strong opinion on the matter.
Overall, the data indicates that there is a consensus that companies should take more measures to protect user data when using AI for online marketing and should be held accountable for any unintended consequences. However, opinions are more divided on whether consumers should have the right to opt out of AI-driven marketing campaigns, with a significant percentage of neutral responses.

Table 4. Frequency table

Should companies take more measures to protect user data when using AI for online marketing?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	86	28.7	28.7	28.7
	Disagree	14	4.7	4.7	33.3
	Neutral	57	19.0	19.0	52.3
	Strongly agree	120	40.0	40.0	92.3
	Strongly disagree	23	7.7	7.7	100.0
	Total	300	100.0	100.0	

Should companies be held responsible for any unintended consequences of using AI in online marketing, such as biased decision-making or discriminatory practices?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	115	38.3	38.3	38.3
	Disagree	27	9.0	9.0	47.3
	Neutral	102	34.0	34.0	81.3
	Strongly agree	43	14.3	14.3	95.7
	Strongly disagree	13	4.3	4.3	100.0
	Total	300	100.0	100.0	

Should consumers have the right to opt out of being targeted by AI-driven marketing campaigns?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	105	35.0	35.0	35.0
	Disagree	15	5.0	5.0	40.0
	Neutral	92	30.7	30.7	70.7
	Strongly agree	74	24.7	24.7	95.3
	Strongly disagree	14	4.7	4.7	100.0
	Total	300	100.0	100.0	

4. CONCLUSION

In conclusion, the use of AI in online marketing has the potential to improve customer engagement and personalization but also raises ethical concerns about consumer privacy and decision-making. In, this study, we explored these concerns and provided insights into the challenges posed by AI in online marketing, such as the collection and use of consumer data, transparency, and accountability of decision-making, and the impact on consumer autonomy and privacy. Through a review of relevant literature and case studies, as well

as a survey of 300 AI consumers from different countries across all continents, we found that transparency, privacy, and accountability are the most critical AI ethics principles, and a lack of ethical knowledge, legal frameworks, and monitoring bodies are the most common AI ethics challenges. This study recommends that companies should consider these ethical issues when implementing AI in their marketing strategies and provides a roadmap for balancing the advantages of AI in online marketing with the protection of consumer rights. By promoting ethical AI in online marketing, companies can enhance consumer safety and privacy while contributing to the ongoing discussion on the ethics of AI and its impact on society.

REFERENCES

[1] C. Pazzanese, "Ethical concerns mount as AI takes bigger decision-making role in more industries." The Harvard Gazette(blog). October 26, 2020.
DOI: https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role

[2] L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, E. Vayena, "AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines", Vol. 28, No. 4, pp. 689-707, Dec 2018.
DOI: https://doi.org/10.1007/s11023-018-9482-5

[3] C. Campbell, S. Sands, C. Ferraro, H. Y. J. Tsao, A. Mavrommatis, "From data to action: How marketers can leverage AI," Business Horizons, Vol. 63, No. 2, pp. 227-243, April 2020.
DOI: https://doi.org/10.1016/j.bushor.2019.12.002

[4] A. A. Khan, S. Badshah, P. Liang, B. Khan, M. Waseem, M. Niazi, M. A. Akbar, "Ethics of AI: A Systematic Literature Review of Principles and Challenges," In Proceedings of the International Conference on Evaluation and Assessment in Software Engineering, Gothenburg, Sweden, pp. 383–392, June 2022.
DOI: https://doi.org/10.1145/3530019.3531329

[5] I. Wigmore, "Black box AI. TECHTARGET NETWORK", August 2019.
DOI: https://www.techtarget.com/whatis/definition/black-box-AI

[6] G. B. Orgaz, J. J. Jung, D. Camacho, "Social big data: Recent achievements and new challenges. An international journal on information fusion," Vol. 28, pp. 45–59, March 2016.
DOI: https://doi.org/10.1016/j.inffus.2015.08.005

[7] S. Murugan, "How AI is Revolutionising Aircraft Maintenance in the Aviation Industry." Linkedin, March 2023.
DOI: https://www.linkedin.com/pulse/how-artificial-intelligence-ai-revolutionising-aircraft-murugan

[8] W. Wang, K. Siau, "Ethical and Moral Issues with AI-A Case Study on Healthcare Robots." In 24th Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018. Association for Information Systems. August 2018.
DOI: https://doi.org/Americas Conference on Information Systems (AMCIS 2018)

[9] Y. Zhang, M. Wu, G. Y. Tian, G. Zhang, J. Lu, "Ethics and privacy of artificial intelligence: Understandings from bibliometrics," Knowledge-Based Systems, Vol. 222, April 2021.
DOI: https://doi.org/10.1016/j.knosys.2021.106994

[10] N. Huet, "Gender bias in recruitment: How AI hiring tools are hindering women's careers." Euronews.Next. March 2022.
DOI: https://www.euronews.com/next/2022/03/08/gender-bias-in-recruitment-how-ai-hiring-tools-are-hindering-women-s-careers

[11] S. C. Davies, "Even Imperfect Algorithms Can Improve the Criminal Justice System." The New York Times, December 20, 2017.
DOI: https://www.nytimes.com/2017/12/20/upshot/algorithms-bail-criminal-justice-system.html

[12] T. Lorenz, "TikTok's Data Collection Has Prompted U.S. Security Concerns." The New York Times, February 25,

2021.
DOI: https://www.nytimes.com/2021/02/25/technology/tiktok-privacy-security.html
[13] BBC News, "TikTok faces privacy investigations by EU watchdog." BBC News, September 15, 2021.
DOI: https://www.bbc.com/news/technology-58573049
[14] T. Simonite, "Amazon Joins Microsoft's Call for Rules on Facial Recognition." WIRED, February 7, 2019.
DOI: https://www.wired.com/story/amazon-joins-microsofts-call-rules-facial-recognition/
[15] N. J. Reventlow, "How Amazon's Moratorium on Facial Recognition Tech Is Different From IBM's and Microsoft's." Cyber.Harvard.edu, 2020, June 11, 2020.
DOI:https://cyber.harvard.edu/story/2020-06/how-amazons-moratorium-facial-recognition-tech-different-ibms-and-microsofts
[16] Federal Trade Commission, "FTC Press Conference on Facebook Settlement [Video]." Federal Trade Commission (Protecting America's Consumers), July 24, 2019.
DOI: https://www.ftc.gov/media/71355
[17] Editorial Staff , "ACLU sues US government to expose use of facial-recognition technology." E&T, November 1, 2019.
DOI:https://eandt.theiet.org/content/articles/2019/11/aclu-sues-us-government-to-expose-use-of-facial-recognition-technology/
[18] M. Day, G. Turner, N. Drozdiak, "Amazon Workers Are Listening to What You Tell Alexa." Bloomberg, April 11, 2019.
DOI:https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio#xj4y7vzkg
[19] B. F. Rubin, "Amazon's new Alexa features put more emphasis on privacy." CNET, May 29, 2019.
DOI: https://www.cnet.com/home/smart-home/amazons-new-alexa-features-puts-added-emphasis-on-privacy/
[20] Amazon, "Amazon is earning and maintaining customer trust through privacy.: Amazon, January 28, 2022.
DOI:https://www.aboutamazon.com/news/how-amazon-works/amazon-is-earning-and-maintaining-customer-trust-through-privacy
[21] K. J. O. Brien, "Google Data Admission Angers European Officials." The New York Times, May 15, 2010.
DOI: https://www.nytimes.com/2010/05/16/technology/16google.htm
[22] D. Gross, "What Google's Street View breach means for your privacy." CNN, October 26, 2010.
DOI: https://edition.cnn.com/2010/TECH/web/10/26/google.street.view/index.html