International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 4 (April 2025), PP 202-216

A Study on the Violation of Data Privacy Due To Interest Based Advertisement in Online Shopping In Chennai

SIVAPRIYA.G.K
B.COM LLB (hons)
SAVEETHA SCHOOL OF LAW
SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCE (SIMATS)

ABSTRACT :
This study investigates the infringement of data privacy resulting from the proliferation of interest-based advertisements in the realm of online shopping. Through a thorough examination of existing literature, regulatory frameworks, and industry practices, the study sheds light on the challenges and risks associated with the indiscriminate collection and utilisation of personal data for targeted advertising purposes. It delves into the implications for user autonomy, regulatory compliance, corporate accountability, technological innovation, international cooperation, and ongoing vigilance. This study examines the violation of data privacy arising from interest-based advertisements in online shopping. Through a comprehensive analysis of demographic segments, including age, gender, education level, employment status, and occupation, the study investigates consumer perceptions, behaviours, and attitudes towards targeted advertising practices. By synthesising these findings, the study underscores the imperative for proactive measures to protect data privacy in the online shopping sphere, offering valuable insights for policymakers, businesses, and consumers seeking to navigate this increasingly complex landscape responsibly and ethically. The study highlights divergent opinions regarding the prioritisation of user privacy protection over the delivery of highly targeted interest-based ads, with implications for industry practices and regulatory policies. The findings underscore the importance of striking a balance between personalised advertising and user privacy protection to foster trust and transparency in the digital marketplace. Recommendations are provided for stakeholders to promote ethical advertising practices, enhance transparency, and advocate for robust data protection regulations in online shopping.
KEYWORDS: *Internet, Protection, Regulation, Prioritisation, Accountability.*

Date of Submission: 08-04-2025 Date of acceptance: 19-04-2025

I. INTRODUCTION:

Online shopping has become an integral part of daily life, offering convenience and access to a vast array of products and services. Interest-based advertising relies on sophisticated algorithms and tracking technologies to analyse user data and deliver relevant ads. However, the collection and utilisation of such data without adequate consent or transparency can infringe upon individuals' privacy rights. Concerns arise regarding the potential for data misuse, unauthorised access, and the creation of detailed profiles that may be vulnerable to exploitation or breaches. The methods and extent of data collection by online platforms and advertisers significantly impact privacy. Factors such as the types of data collected, the frequency of data updates, and the sources from which data is gathered can influence the level of intrusion into users' privacy. Rapid advancements in tracking technologies, such as cookies, device fingerprinting, and cross-device tracking, enable more sophisticated data collection and ad targeting. These technological innovations continuously reshape the online advertising ecosystem, raising new challenges for data privacy protection. The business models of online platforms and advertisers, which often rely on targeted advertising for revenue generation, shape their incentives regarding data collection and usage. Balancing commercial interests with user privacy rights poses ethical and economic considerations for companies operating in the digital advertising ecosystem. The Indian government introduced the Personal Data Protection Bill in 2019 to regulate the processing of personal data by individuals, companies, and the government. The bill aims to establish a comprehensive framework for data protection and privacy, including provisions related to consent, data localization, and the rights of data subjects. Telecom Regulatory Authority of India (TRAI) has issued regulations and recommendations related to data privacy and user consent in the telecom and digital communication sectors. While not directly targeting online shopping, these regulations can indirectly influence data privacy practices across various online platforms, including those involved in e-commerce and advertising. The Indian government has enacted consumer protection laws and regulations to

safeguard consumer rights in online transactions, including provisions related to data privacy and protection. These regulations aim to ensure transparency, fairness, and accountability in online business practices, which can impact how companies conduct interest-based advertising to online shoppers. This study aims to delve into the intricate relationship between online shopping, data privacy, and the pervasive use of interest-based ads.

II. OBJECTIVES:

- To find the frequency of encountering targeted advertisements based on browsing history on online shopping platforms.
- To identify users' attitudes towards internet advertisements related to conversations by smart speakers or voice assistants.
- To analyse the online platforms could be implemented to enhance the safeguarding of data privacy in interest-based ads.
- To find users' opinions on prioritising user privacy protection over the delivery of highly targeted interest-based advertisements on online shopping platforms.

III. REVIEW OF LITERATURE:

Kalinda Basho (2000), The increase in the private sector's collection and use of individuals' personal information raises a new threat to privacy in the electronic marketplace. Each day, businesses are collecting sensitive information about consumers' buying habits, occupations, income, families and product preferences. This information is used to create customised advertising campaigns, make decisions about which customers to market products to and predict consumers' future purchases. Current solutions to online privacy fail to give consumers control over how their information is used or compensation for the data they share. **A. Michael Froomkin (2000),** The rapid deployment of privacy-destroying technologies by governments and businesses threatens to make informational privacy obsolete. The first part of this article describes a range of current technologies to which the law has yet to respond effectively. These include: routine collection of transactional data, growing automated surveillance in public places, deployment of facial recognition technology and other biometrics, cell-phone tracking, vehicle tracking, satellite monitoring, workplace surveillance, Internet tracking from cookies to "click trails," hardware-based identifiers, intellectual property-protecting "snitch ware," and sense-enhanced searches that allow observers to see through everything from walls to clothes. **Steven A. Hetcher (2001),** This article explores an important development in the informal regulation of online privacy. Privacy norm proselytisers have been the leading contributors toward the recognition by Internet users of a moral entitlement to privacy in cyberspace. This article begins by examining the non-moral social meaning of the original personal data collection practices that emerged at the World Wide Web's inception in the early 1990s. **Paul M. Schwartz (2004),** Modern computing technologies and the Internet have generated the capacity to gather, manipulate, and share massive quantities of data; this capacity, in turn, has spawned a booming trade in personal information. Even as it promises new avenues for the creation of wealth, this controversial new market also raises significant concerns for individual privacy - consumers and citizens are often unaware of, or unable to evaluate, the increasingly sophisticated methods devised to collect information about them. **Norman E. Bowie (2006),** Consumer surveys indicate that concerns about privacy are a principal factor discouraging consumers from shopping online. The key public policy issue regarding privacy is whether the US should follow its current self-regulation course (where the FTC encourages websites to obtain private "privacy web-seals"), or whether a European style formal legal regulation approach should be adopted in the US. We conclude that the use of assurance seals has worked reasonably well and websites should be free to decide whether they have a privacy seal or not. **PATRICIA A. NORBERG et al… (2007),** Impelled by the development of technologies that facilitate collection, distribution, storage, and manipulation of personal consumer information, privacy has become a "hot" topic for policy makers. Commercial interests seek to maximise and then leverage the value of consumer information, while, at the same time, consumers voice concerns that their rights and ability to control their personal information in the marketplace are being violated. However, despite the complaints, it appears that consumers freely provide personal data. **Sara Dolnicar (2007),** Marketing communications media technologies have the potential to be intrusive and influence consumers' perceptions of marketing communication. Aggressive direct marketing (DM) is one communication tool that has the potential to lead to consumer concern about information privacy. Concerned consumers change their behaviour. They refuse to buy through risky channels or provide information, thus jeopardising the aim of DM. Responsible DM can prevent such reactions and build trust. Typical measures taken and recommended to protect consumers from privacy violations are of a regulative rather than a market-oriented nature, which is directly opposed to companies' profit-maximisation aims. **Kenneth A. Bamberger et al… (2011),** U.S. privacy law is under attack. Scholars and advocates criticise it as weak, incomplete, and confusing, and argue that it fails to empower individuals to control the use of their personal

information. These critiques present a largely accurate description of the law "on the books." But the debate has strangely ignored privacy "on the ground" —since 1994, no one has conducted a sustained inquiry into how corporations actually manage privacy, and what motivates them. This Article presents findings from the first study of corporate privacy management in fifteen years, involving qualitative interviews with chief privacy officers identified by their peers as industry leaders. **Katherina Glac et al… (2014),** Privacy issues surrounding the use of social media sites have been apparent over the past ten years. Use of such sites, particularly Facebook, has been increasing and recently business organisations have begun using Facebook as a means of connecting with potential customers or clients. This paper presents an empirical study of perceived privacy violations to examine factors that influence the expectations of privacy on Facebook. Results of the study suggest that the more important Facebook is to users, the more likely they are to perceive privacy violations and the more likely those violations are to be considered serious. Furthermore, how information is used is more important than the way this information is accessed. **Daniel J. Solove (2014),** One of the great ironies about information privacy law is that the primary regulation of privacy in the United States has barely been studied in a scholarly way. Since the late 1990s, the Federal Trade Commission (FTC) has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices. Despite over fifteen years of FTC enforcement, there is no meaningful body of judicial decisions to show for it. The cases have nearly all resulted in settlement agreements. **Micah Altman (2015),** Governments are under increasing pressure to publicly release collected data in order to promote transparency, accountability, and innovation. Because much of the data they release pertains to individuals, agencies rely on various standards and interventions to protect privacy interests while supporting a range of beneficial uses of the data. However, there are growing concerns among privacy scholars, policymakers, and the public that these approaches are incomplete, inconsistent, and difficult to navigate. To identify gaps in current practice, this Article reviews data released in response to freedom of information and Privacy Act requests, traditional public and vital records, official statistics, and e-government and open government initiatives. **Kelly D. Martin et al… (2017),** Although marketers increasingly rely on customer data, firms have little insight into the ramifications of such data use and do not know how to prevent negative effects. Data management efforts may heighten customers' vulnerability worries or create real vulnerability. Using a conceptual framework grounded in gossip theory, the authors link customer vulnerability to negative performance effects. Three studies show that transparency and control in firms' data management practices can suppress the negative effects of customer data vulnerability. **Ram D. Gopal et al… (2018),** Publishers websites are increasingly presenting content and services that are not created and managed by the website administrators themselves, but are provided by other third parties. While third party content and services provide value and utility to website users, this comes at the cost of user information being shared with the third party. Privacy concerns surrounding information leakage have been growing rapidly. With increasing concerns regarding online privacy and information disclosure, it is important to understand the factors that affect the level of sharing between publisher websites and third parties. **Komal S. Patel (2018),** This Note assesses First Amendment freedom of speech claims with regard to online civil rights testing. Transactions that have conventionally occurred in person are now more often completed online, and providers transacting online have been increasingly using algorithms that synthesise users' data. While these algorithms are helpful tools, they may also be yielding discriminatory results, whether intentionally or unintentionally. In order to test whether such algorithms are discriminating, civil rights testers and researchers have developed various online auditing methods. **DANIELLE KEATS CITRON (2019),** Those who wish to control, expose, and damage the identities of individuals routinely do so by invading their privacy. People are secretly recorded in bedrooms and public bathrooms and "up their skirts." Such images are used to coerce people into sharing nude photographs and filming sex acts under the threat of public disclosure. People's nude images are posted online without permission. Machine-learning technology is used to create digitally manipulated "deep fake" sex videos that swap people's faces into pornography. **Ido Kilovaty (2019),** Swaths of personal and nonpersonal information collected online about Internet users are increasingly being used in sophisticated ways for online political manipulation. This represents a new trend in the exploitation of data, where instead of pursuing direct financial gain based on the face value of the data, actors engage in data analytics using advanced artificial intelligence technologies that allow them to more easily access individuals' cognition and future behaviour. **Jacquellena Carrero (2020),** Data scraping the automated collection of data on the internet is used in a variety of contexts. On the commercial side, scraping might be used as a means of competition such as scraping by one company to retrieve information on prices for services provided by a competitor. On the noncommercial side, scraping could be used as a research tool such as scraping by a news outlet to investigate Amazon's pricing algorithm. Despite the varied applications of data scraping, courts' varying interpretations of the Computer Fraud and Abuse Act (CFAA) can impose both civil and criminal liability for scraping. **Dan Feldman et al … (2020),** Data-mining practices have greatly advanced in the interconnected era. What began with the internet now continues through the Internet of Things (IoT)—whereby users can constantly be connected to the internet through various means, like televisions, smartphones, wearables, and computerised personal assistants, among other "things." As many of these devices constantly receive and transmit data, the increased

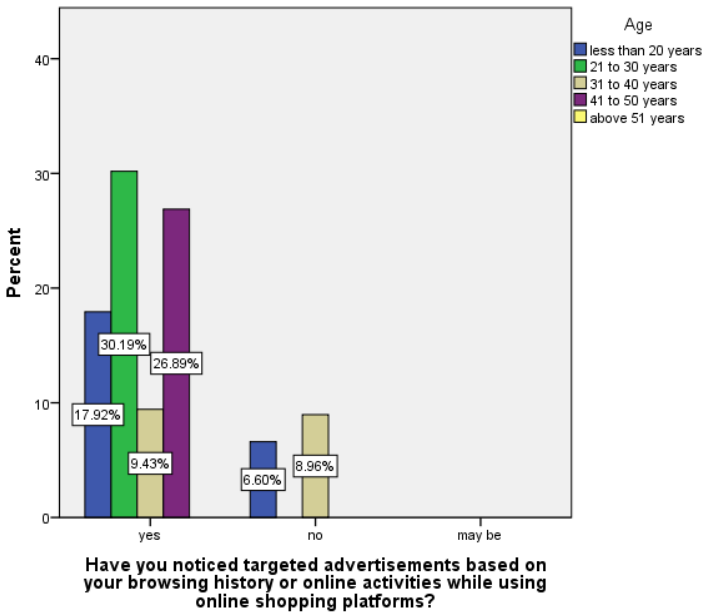
use of IoT devices might lead society into an "always-on" era, where individuals are "datafied"—constantly quantified and tracked. This situation leads to difficult policy choices. **David Alpert (2020)**, The California Consumer Privacy Act (CCPA) is the first-of-its-kind law in the United States providing Californians (and effectively citizens nationwide) with comprehensive protection of their online data. The CCPA provides consumers with four meaningful rights: a right to access the data companies collect from and about them; a right to have said data deleted; a right to know which categories of third parties these companies are sharing their data with or selling their data to; and, a right to opt out of such sales. This Note focuses specifically on the first right, the right of data access. **Mark MacCarthy (2023),** The rampant disinformation and hate speech on social media platforms cry out for the kind of regulation that seeks to control externalities in other areas of life such as environmental pollution. But government regulation of the content distributed by media firms has a bad reputation in the United States, and for good reason. Still, the dangers of private domination of the public's information space are real. Social media reformers need to pay attention to the dangers of government and private sector censorship in crafting measures that can respond to the rampant information disorder on social media platforms.

IV. METHODOLOGIES:

This research paper is done on the basis of non doctrinal research. The sample size is about 210 samples. The information taken for the research paper is from books, journals, articles, Internet etc.It includes relevant case laws for the research as evidence as well as references. The research paper has included the SPSS statistics which has a number of samples based on the gender variation and opinion variation it includes chi-squared table and interpretation for each table. The table is done on the basis of the questions asked to the public. The paper has been cited with citations with references.

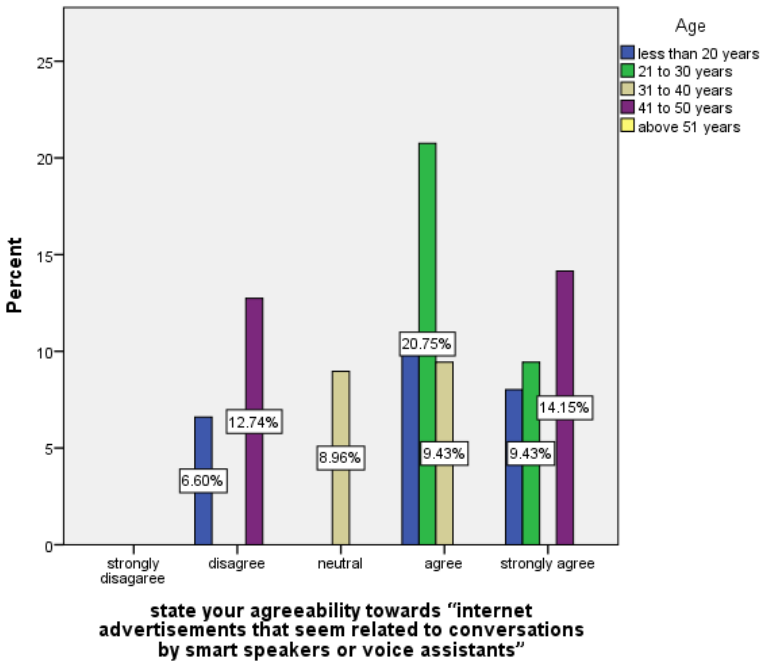
ANALYSIS OF DATA:

FIGURE 1:



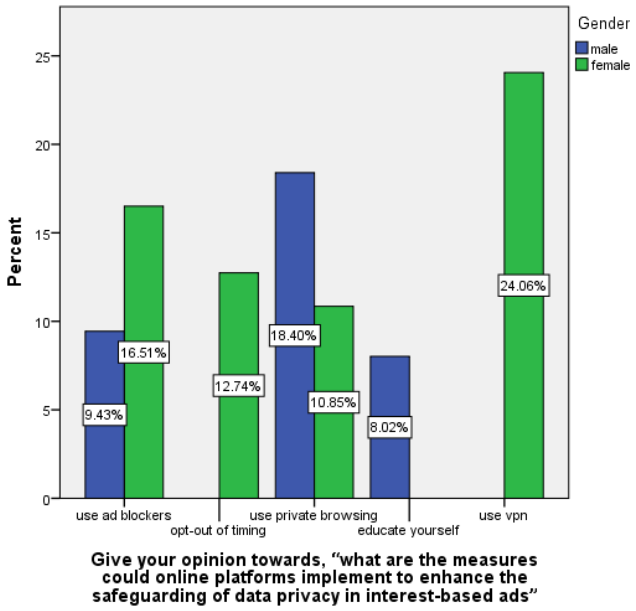
LEGEND: The graph represents the respondent of age wise distribution of the target advertisement based on your browsing history.

FIGURE 2:



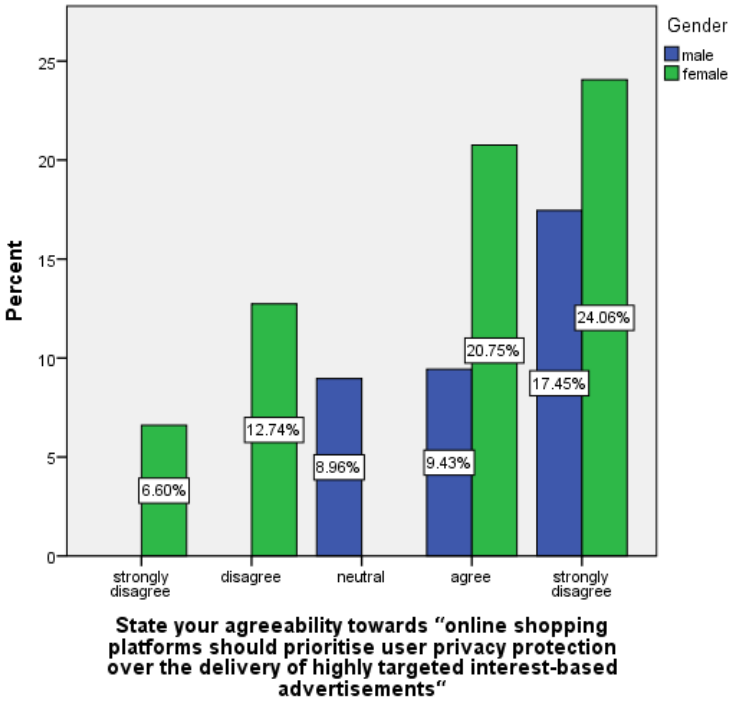
LEGEND: The graph represents the respondent of age wise distribution of agreeability on internet advertisement that seem relegated to conversations by smart speakers or voice assistants.

FIGURE 3:



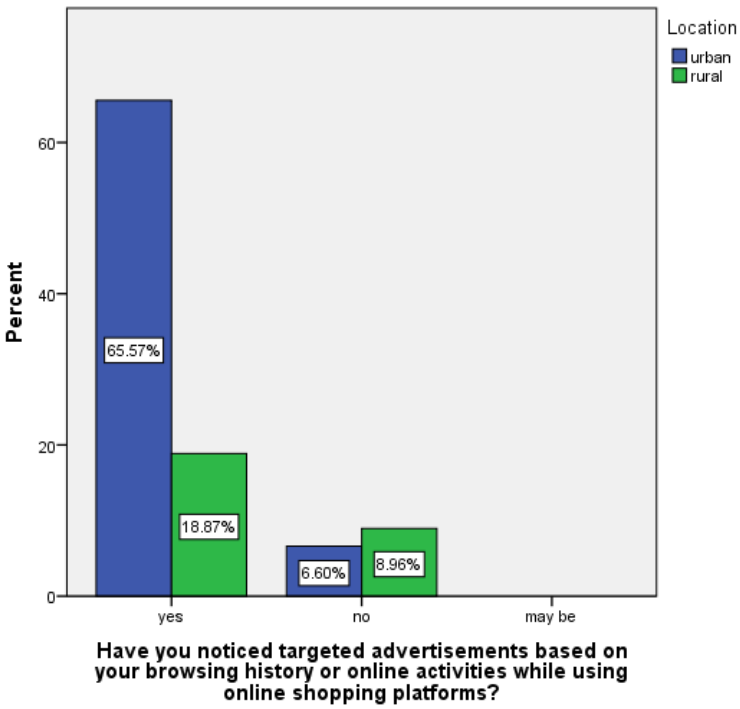
LEGEND: The graph represents the respondent of gender wise distribution of the measures could online platforms implement to enhance the safeguarding of data privacy in interest based ads.

FIGURE 4:



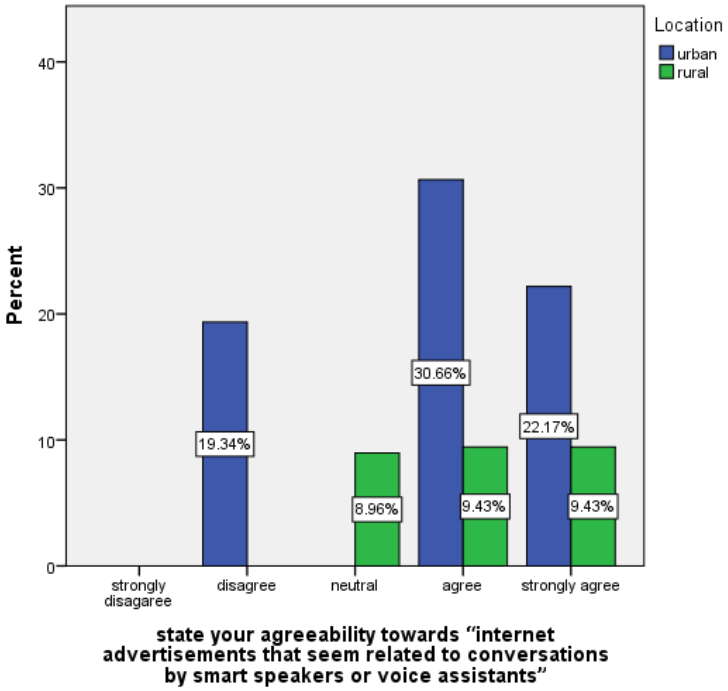
LEGEND: The graph represents the respondent of gender wise distribution of agreeability on the online shopping platforms should prioritise user privacy protection over the delivery of high targeted interest based ads.

FIGURE 5:



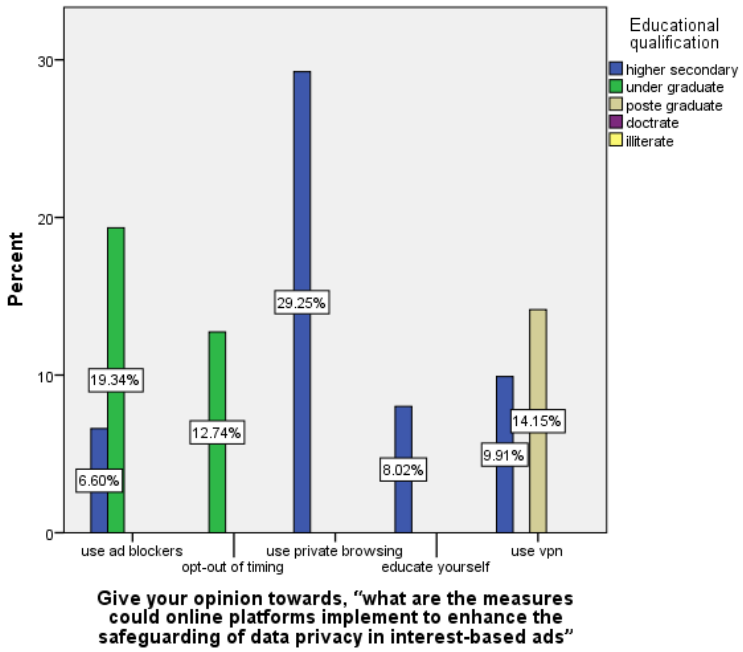
LEGEND: The graph represents the respondent of location of the target advertisement based on your browsing history.

FIGURE 6:



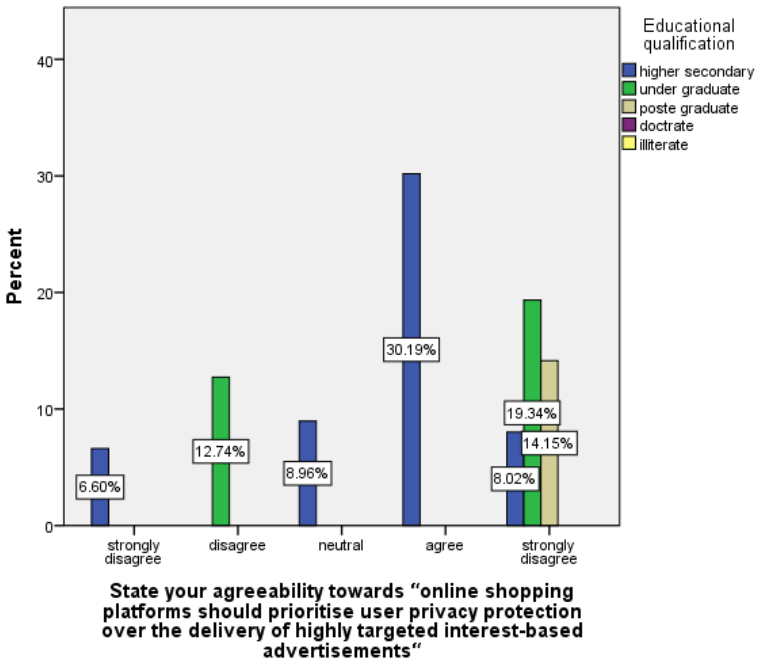
LEGEND: The graph represents the respondent of location of agreeability on internet advertisements that seem relegated to conversations by smart speakers or voice assistants.

FIGURE 7:



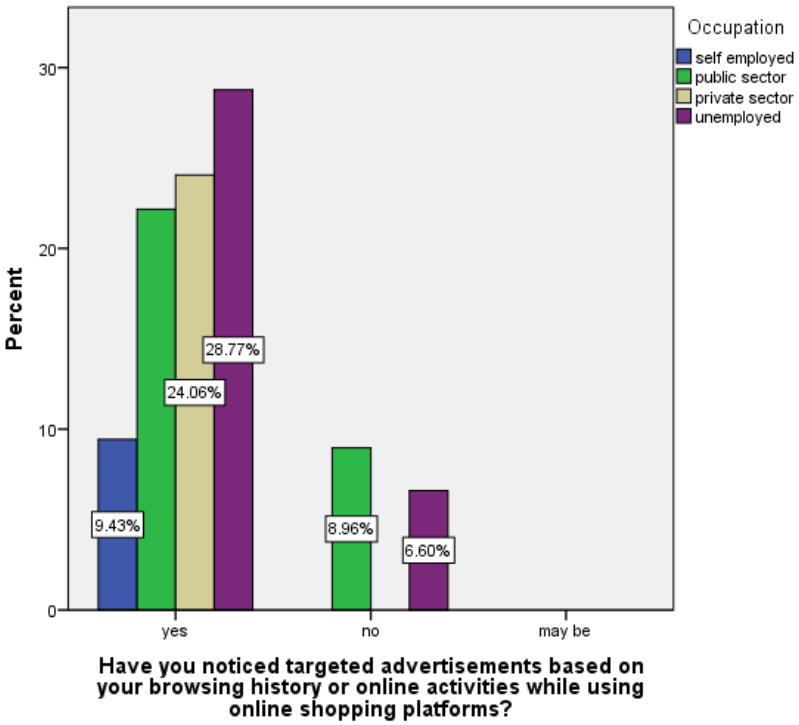
LEGEND: The graph represents the respondent of educational qualification of the measures online platforms could implement to enhance the safeguarding of data privacy in internet based ads.

FIGURE 8:



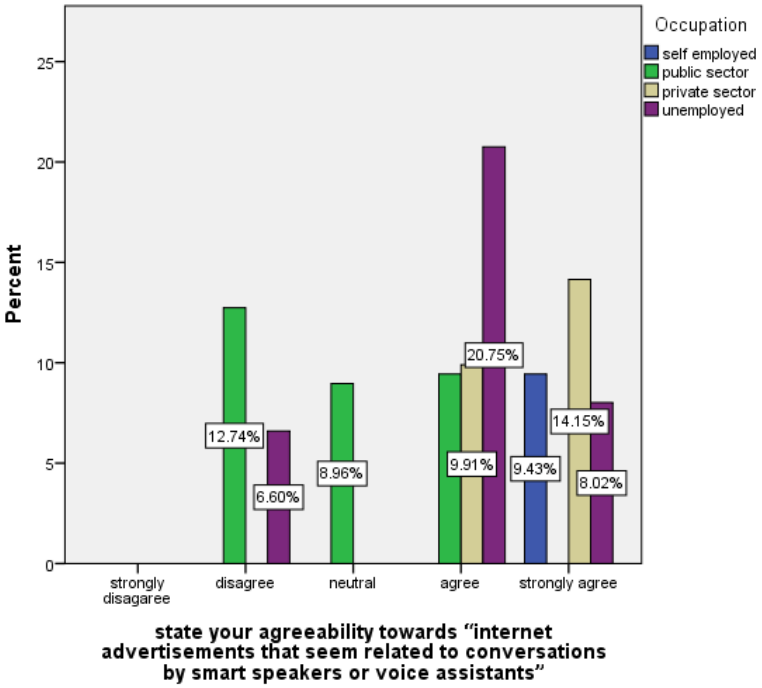
LEGEND: The graph represents the respondent of educational qualifications of agreeability on the online shopping platforms should prioritise user privacy protection over the delivery of high targeted interest based ads.

FIGURE 9:



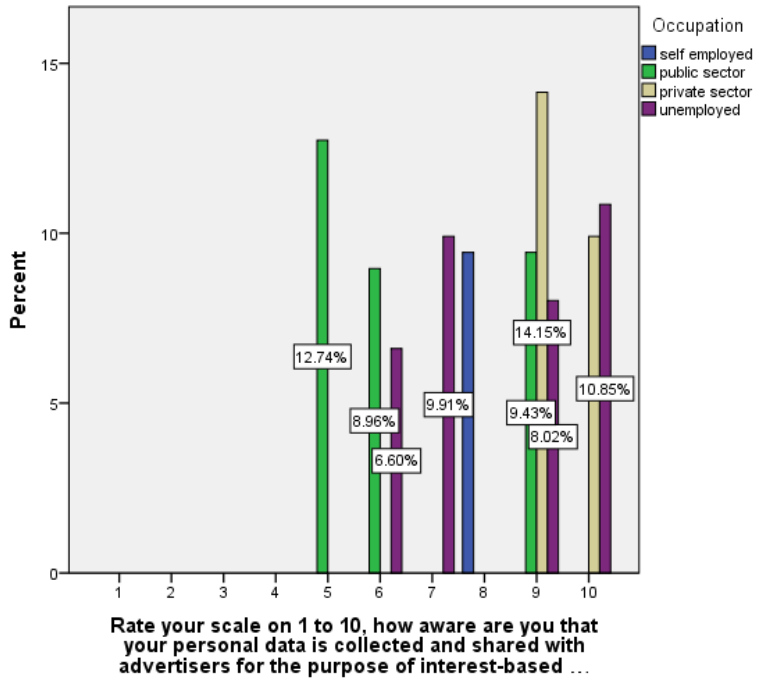
LEGEND: The graph represents the respondent of occupation of the target advertisement based on your browsing history.

FIGURE 10:



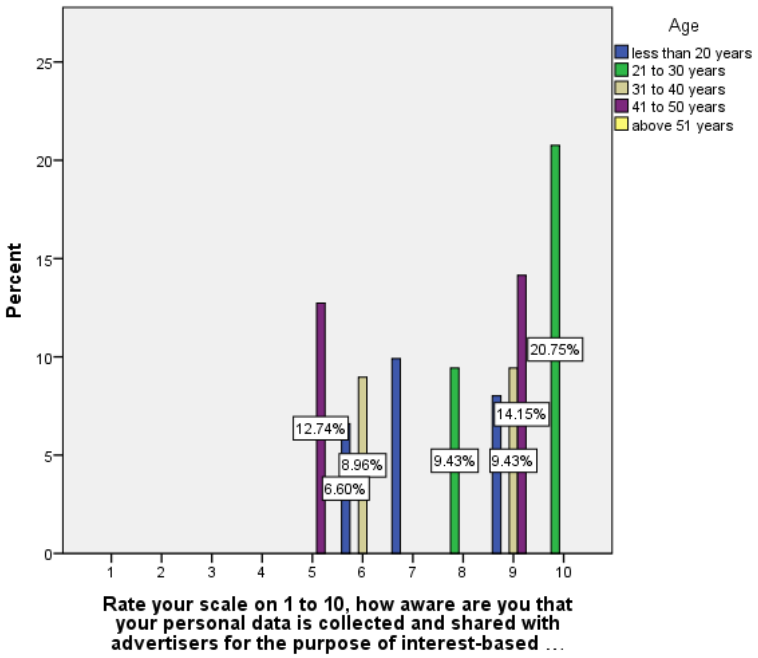
LEGEND: The graph represents the respondent of occupation of agreeability on internet advertisements that seem relegated to conversations by smart speakers or voice assistants.

FIGURE 11:



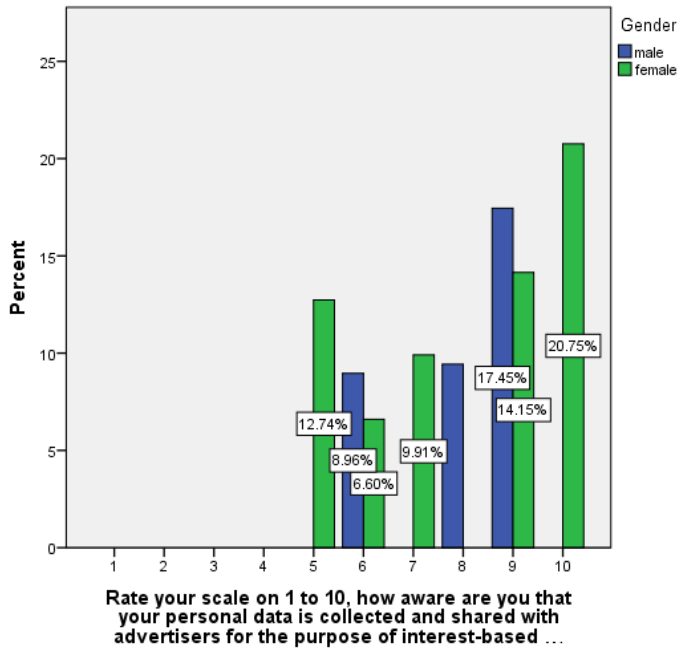
LEGEND: The graph represents the respondents of occupation of the scale on 1 tp 10 of the awareness about the personal data collected and shared with advertisement for the purposes of internet based ads.

FIGURE 12:



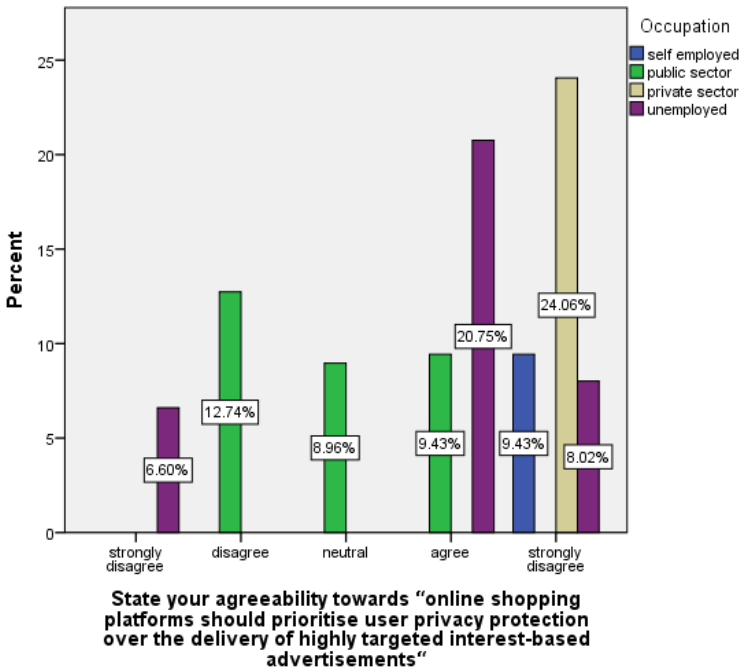
LEGEND: The graph represents the respondent of age wise distribution of the scale on 1 tp 10 of the awareness about the personal data collected and shared with advertisement for the purposes of internet based ads.

FIGURE 13:



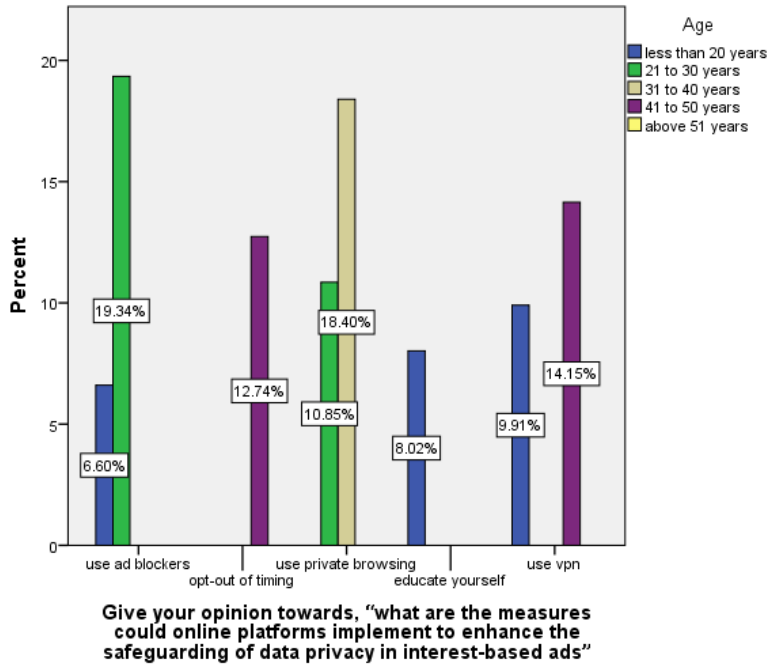
LEGEND: The graph represents the respondent of gender wise distribution of the scale on 1 tp 10 of the awareness about the personal data collected and shared with advertisement for the purposes of internet based ads.

FIGURE 14:



LEGEND: The graph represents the respondent of occupation of the online shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest based ads.

FIGURE 15:



LEGEND: The graph represents the respondent of age wise distribution of the measurescould online platforms implement to enhance the safeguarding of data privacy in internet based ads.

TABLE 1:

ANOVA

State your agreeability towards "online shopping platforms should prioritise user privacy pro

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	15.714	1	15.714	10.253	.002
Within Groups	321.847	210	1.533		
Total	337.561	211			

LEGEND: The graph represents the online shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest based advertising.

TABLE 2:

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Age * Have you noticed targeted advertisements based on your browsing history or online activities while using online shopping platforms?	212	100.0%	0	0.0%	212	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	60.023[a]	3	.000
Likelihood Ratio	68.720	3	.000
Linear-by-Linear Association	3.214	1	.073
N of Valid Cases	212		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.07.

LEGEND: The table represents the targeted advertisements based on your browsing history or online activities while using shopping platforms.

V. RESULTS:

FIGURE 1: The graph represents the respondents of 21 to 30 year old people who gave the highest (30.19%) opinion towards yes, they noticed target advertisements based on your browsing history or online activities while using online shopping platforms. **FIGURE 2:** The graph represents the respondent of 21 to 30 year old people who gave the highest (20.75%) agreeability towards them agreeing that internet advertisements that seem relegated to conversations by smart speakers or voice assistants. **FIGURE 3:** The graph represents the respondent of females giving the highest (24.06%) opinion towards use of vpn as the measure could online platforms implement to enhance the safeguarding of data privacy in internet based ads. **FIGURE 4:** The graph represents the respondent of females giving the highest agreeability (24.06%) towards them strongly disagreeing the online

shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest based ads. **FIGURE 5:** The graph represents the respondent of urban peoples who gave the highest opinion (65.57%) towards yes, they noticed target advertisements based on your browsing history or online activities while using online shopping platforms. **FIGURE 6:** The graph represents the respondent of urban people who gave the highest agreeability (30.66%) towards them agreeing that internet advertisement that seems relegated to conversations by smart speakers or voice assistants. **FIGURE 7:** The graph representing the respondent of higher secondary gave the highest opinion (29.25%) towards use of private browsing for the measures online platforms could implement to enhance the safeguarding of data privacy in internet based ads. **FIGURE 8:** The graph represents the respondent of higher secondary people who gave the highest agreeability (30.19%) towards the agreeing that online shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest based advertisements. **FIGURE 9:** The graph represents the respondent of unemployed people who gave the highest (28.77%) opinion towards yes, they noticed target advertisements based on your browsing history or online activities while using online shopping. **FIGURE 10:** The graph represents the respondent of unemployed people who gave the highest agreeability (20.75%) towards them agreeing that internet advertisements that seem relegated to conversations by smart speakers or voice assistants. **FIGURE 11:** The graph represents the respondent of private sector people who gave the highest (14.15%) scale on 9, they are aware that personal data is collected and shared with advertisers for the purpose of internet based ads. **FIGURE 12:** The graph represents the respondent of 21 to 30 years people who gave the highest (20.75%) scale on which they are aware that personal data is collected and shared with advertisers for the purpose of internet based ads. **FIGURE 13:** The graph represents the respondent of females given the highest (20.75%) scale on which they are aware that personal data is collected and shared with advertisers for the purpose of internet based ads. **FIGURE 14:** The graph represents the respondent of private sector people who gave the highest agreeability (24.06%) towards them strongly disagreeing that online shopping platforms should prioritise users' privacy protection over the delivery of highly targeted interest based ads. **FIGURE 15:** The graph represents the respondent of 21 to 30 years who gave the highest opinion (19.34%) towards using ad blockers for the measure online platforms could implement to enhance the safeguarding of data privacy in interest based ads. **TABLE 1:** It is found that the null hypothesis is accepted hence, there is no significant difference among the online shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest based advertisements. **TABLE 2:** It is found that (P= .073) alternative hypothesis is accepted hence, there is a significant relationship between the age and the notice targeted advertisements based on your browsing history or online activities while using online shopping platforms.

VI. DISCUSSION:

FIGURE 1: The majority of respondents aged 21 to 30 acknowledge noticing target advertisements based on their browsing history or online activities while using online shopping platforms. This indicates a high level of awareness among this age group regarding targeted advertising practices. **FIGURE 2:** Among respondents aged 21 to 30, there is a notable level of agreement with the notion of internet advertisements appearing in conversations initiated by smart speakers or voice assistants. This suggests that this demographic is receptive to this form of advertising. **FIGURE 3:** Female respondents express a significant preference for using VPN as a measure to enhance data privacy in internet-based ads. This indicates a concern among females for safeguarding their online privacy and suggests a potential solution they find effective. **FIGURE 4:** Female respondents strongly disagree with the idea of prioritising user privacy protection over the delivery of highly targeted interest-based ads by online shopping platforms. This indicates a preference among females for personalised advertising despite privacy concerns. **FIGURE 5:** Urban respondents overwhelmingly acknowledge noticing target advertisements based on their browsing history or online activities while using online shopping platforms. This suggests that urban dwellers are highly exposed to targeted advertising practices. **FIGURE 6:** Urban respondents show a high level of agreement with internet advertisements that appear in conversations by smart speakers or voice assistants. This indicates a willingness among urban residents to engage with this type of advertising. **FIGURE 7:** Respondents with a higher secondary education level express a strong preference for using private browsing as a measure to enhance data privacy in internet-based ads. This suggests a proactive approach towards safeguarding privacy among this demographic. **FIGURE 8:** Higher secondary respondents overwhelmingly agree that online shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest-based ads. This indicates a preference for privacy among this demographic. **FIGURE 9:** Unemployed respondents largely acknowledge noticing target advertisements based on their browsing history or online activities while using online shopping platforms. **FIGURE 10:** Unemployed respondents show agreement with internet advertisements appearing in conversations by smart speakers or voice assistants. This indicates a level of receptivity to this form of advertising among the unemployed demographic. **FIGURE 11:** Private sector respondents demonstrate a high level of awareness regarding the collection and sharing of personal data for internet-based ads. This indicates a heightened understanding of data privacy issues among individuals working

in the private sector. **FIGURE 12:** Respondents aged 21 to 30 exhibit a significant awareness of personal data collection and sharing for internet-based ads. This suggests that this age group is cognizant of privacy concerns associated with online advertising. **FIGURE 13:** Female respondents also show a notable awareness of personal data collection and sharing for internet-based ads. This highlights a general concern among females regarding privacy issues related to online advertising. **FIGURE 14:** Private sector respondents strongly disagree with prioritising user privacy protection over the delivery of highly targeted interest-based ads by online shopping platforms. This suggests a preference for personalised advertising despite privacy concerns among this demographic. **FIGURE 15:** Respondents aged 21 to 30 express a preference for using ad blockers as a measure to enhance data privacy in interest-based ads. This indicates a proactive approach towards safeguarding privacy among this age group. **TABLE 1:** It is found that the null hypothesis is accepted hence, there is no significant difference among the online shopping platforms should prioritise user privacy protection over the delivery of highly targeted interest based advertisements. **TABLE 2:** It is found that (P= .073) alternative hypothesis is accepted hence, there is a significant relationship between the age and the notice targeted advertisements based on your browsing history or online activities while using online shopping platforms.

VII. LIMITATION:

One of the major limitations of the study in the sample frame. There is a major constraint in the sample frame as it is limited to a small area. Thus, it proves to be difficult to extrapolate it to a large population. Another limitation is the sample size of 210 which cannot be used to assume the thinking of the entire population in a particular country, state or city. The physical factors have a larger impact, thus, limiting the study.

VIII. SUGGESTION:

Develop comprehensive recommendations based on the study findings to guide stakeholders, including online shopping platforms, advertisers, policymakers, and consumer advocacy groups, in addressing data privacy concerns. Offer actionable insights and practical strategies for implementing transparency, user control mechanisms, and ethical advertising practices to mitigate the risk of data privacy violations associated with interest-based ads.

IX. CONCLUSION:

As online shopping continues to surge, so do concerns regarding the unauthorised collection and use of personal data for targeted advertising. Government regulations, industry standards, and consumer awareness campaigns play crucial roles in safeguarding individuals' privacy rights. Effective implementation of privacy policies, transparency in data collection practices, and empowering users with control over their data are essential steps toward mitigating privacy violations in the online shopping landscape. Furthermore, ongoing research and collaboration between stakeholders are necessary to address emerging privacy challenges and ensure a trustworthy and ethical online environment for all users. Empowering users with knowledge about data privacy risks associated with interest-based ads is paramount. Education and awareness campaigns can help individuals make informed decisions about their online activities and the sharing of personal information. Strengthening regulatory frameworks to enforce data protection laws and hold companies accountable for privacy breaches is crucial. Governments should work towards comprehensive legislation that sets clear guidelines for data collection, storage, and usage, with stringent penalties for non-compliance. Online platforms and advertisers have a responsibility to prioritise user privacy and ethical data practices. Implementing privacy-by-design principles and conducting regular audits of data handling processes can help mitigate privacy risks and build trust with consumers. Investing in privacy-enhancing technologies such as encryption, anonymization, and differential privacy can help minimise the exposure of personal data while still allowing for effective advertising targeting. Given the global nature of online commerce, international cooperation and standardisation efforts are essential to address data privacy concerns comprehensively. Collaborative initiatives can facilitate information sharing, best practice exchange, and harmonisation of privacy regulations across borders. The landscape of online shopping and digital advertising is constantly evolving, making it imperative for stakeholders to continuously monitor emerging trends and adapt privacy policies and practices accordingly. Regular assessments and updates are necessary to stay ahead of privacy threats and ensure the protection of user data.

REFERENCE:

[1]. Kalinda Basho, The Licensing of Our Personal Information: Is It a Solution to Internet Privacy, California Law Review, Vol. 88, No. 5 (Oct., 2000), pp. 1507-1545

A. Michael Froomkin, The Death of Privacy, Stanford Law Review, Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May, 2000), pp. 1461-1543

[2]. Steven A. Hetcher, Norm Proselytizers Create A Privacy Entitlement in Cyberspace, Berkeley Technology Law Journal, Vol. 16, Supplement (Summer 2001), pp. 877-935

[3]. Paul M. Schwartz, Property, Privacy, and Personal Data, Harvard Law Review, Vol. 117, No. 7 (May, 2004), pp. 2056-2128

[4]. Norman E. Bowie and Karim Jamal, Privacy Rights on the Internet: Self-Regulation or Government Regulation, Business Ethics Quarterly, Vol. 16, No. 3 (Jul., 2006), pp. 323-342
[5]. PATRICIA A. NORBERG, DANIEL R. HORNE and DAVID A. HORNE, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours, The Journal of Consumer Affairs, Vol. 41, No. 1 (Summer 2007)
[6]. Sara Dolnicar and Yolanda Jordaan, A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing, Journal of Advertising, Vol. 36, No. 2, Special Issue on Responsibility in Advertising (Summer, 2007), pp. 123-149.
[7]. Kenneth A. Bamberger and Deirdre K. Mulligan, Privacy on the Books and on the Ground, Stanford Law Review, Vol. 63, No. 2 (JANUARY 2011), pp. 247-315
[8]. Katherina Glac, Dawn R. Elm and Kirsten Martin, Areas of Privacy in Facebook: Expectations and Value, Business & Professional Ethics Journal, Vol. 33, No. 2/3 (2014), pp. 147-176.
[9]. Daniel J. Solove and Woodrow Hartzog, THE FTC AND THE NEW COMMON LAW OF PRIVACY, Columbia Law Review, Vol. 114, No. 3 (APRIL 2014), pp. 583-676
[10]. Micah Altman, Alexandra Wood, David R. O'Brien, Salil Vadhan and Urs Gasser, Towards a Modern Approach to Privacy-Aware Government Data Releases, Berkeley Technology Law Journal, Vol. 30, No. 3 (2015), pp. 1967-2072
[11]. Kelly D. Martin, Abhishek Borah and Robert W. Palmatier, Data Privacy: Effects on Customer and Firm Performance, Journal of Marketing, Vol. 81, No. 1 (January 2017), pp. 36-58.
[12]. Ram D. Gopal, Hooman Hidaji, Raymond A. Patterson, Erik Rolland and Dmitry Zhdanov, How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas, MIS Quarterly, Vol. 42, No. 1 (March 2018), pp. 143-164, A1-A25
[13]. Komal S. Patel, TESTING THE LIMITS OF THE FIRST AMENDMENT, Columbia Law Review, Vol. 118, No. 5 (JUNE 2018), pp. 1473-1516
[14]. DANIELLE KEATS CITRON, Sexual Privacy, The Yale Law Journal, Vol. 128, No. 7 (MAY 2019), pp. 1870-1960
[15]. Ido Kilovaty, LEGALLY COGNIZABLE MANIPULATION, Berkeley Technology Law Journal, Vol. 34, No. 2 (2019), pp. 449-502
[16]. Jacquellena Carrero, ACCESS GRANTED, Columbia Law Review, Vol. 120, No. 1 (JANUARY 2020), pp. 131-172
[17]. Dan Feldman and Eldar Haber, Measuring and Protecting Privacy in the Always-On Era, Berkeley Technology Law Journal, Vol. 35, No. 1 (2020), pp. 197-250
[18]. David Alpert, BEYOND REQUEST-AND-RESPOND, Columbia Law Review, Vol. 120, No. 5 (JUNE 2020), pp. 1215-125