PRIVACY CONCERNS IN THE AGE OF BIG DATA

* K.Anil
** M.Anuradha Reddy
*** Ravi Akula

*Research Scholar, Department of Commerce, Palamuru University, Mahabubnagar, Telangana.

**Assistant Professor, Department of Commerce, Palamuru University, Mahabubnagar, Telangana.
*** Professor & Head, Department of Commerce, Mahatma Gandhi University, Nalgonda, (T.G.)

Abstract

In today's digital world, online marketing is everywhere. Incidents such as data breach and theft will seriously damage consumer trust. This loss of trust makes people hesitant to shop online or share their data, which poses a problem for marketers who need consumer information to tailor their products and stay competitive. Many consumers express worries about privacy but do not initiate steps to protect their data or change privacy settings. This gap between knowing about privacy issues and acting on them highlights the need for marketers to address these concerns seriously. Consumers need more information about how to protect their data and the risks of data breach. There is also a need for clearer laws focused specifically on data protection and consumer privacy. As technology evolves, data privacy has become a crucial issue, affecting digital communication and consumer safety. Privacy has become a major concern in online marketing. This study looks at different privacy issues, what motivates consumers, and how these concerns impact online shopping. The present study aims to understand the privacy concerns that online shoppers have and how these concerns affect their behaviour and trust. By learning about these privacy issues, businesses can address customer concerns, build trust, and develop strategies to engage customers more effectively. This understanding will also help the companies provide more value to their customers, improve relationships, and guide the policy makers in creation of better privacy laws. The study focuses on five districts in Telangana —Mahabubnagar, Nagarkurnool, Gadwal, Wanaparthy and Narayanapet. A questionnaire was sent to over social media groups, and 216 responses were collected. After removing invalid responses, 210 were used for analysis. The sampling combined purposive and convenience sampling methods. Statistical tools such as chi square and correlation tests are employed. The study found positive correlation between awareness of data collection and privacy concerns significantly impact their trust and purchasing decisions.

Key words: Online shopping, Data breaches, Consumer trust, Privacy concerns, Online buying behaviour.

INTRODUCTION

We are living in the age of the Internet of Things (IoT), where the internet, despite its widespread use, is becoming increasingly unsafe. As more people use the internet globally, incidents like identity theft, cybercrimes, and data breaches are rising. Examples include: **Facebook:** 540 million records exposed; **Yahoo (2013-2017):** Data of 87

billion people breached; **eBay (2014):** 145 million accounts compromised and **Uber (2016):** 57 million records hacked.

Historically, the term "caveat emptor" or "let the buyer beware" suggests that sellers should inform buyers about their products in detail. In today's context, this idea should extend to how consumers' data is handled, recognizing that buyers often know less about how their information is used. Today, companies collect and store vast amounts of customer data, using it to understand online behavior and enhance their services. However, this raises concerns about security of data and misuse of personal information. Despite the rise in cyberthreats and breaches, many consumers continue to share their data online, often without fully understanding the risks or the measures they can take to protect their information. With the surge of the Digital interconnectedness, online safety has become a major concern. Increased internet usage has led to more identity theft, cybercrimes, and data breaches, with incidents affecting millions of users. These breaches have made online transactions riskier and have raised consumer worries about how their personal data is handled. Despite the increase in online crimes and data breaches, many consumers are still wary of online transactions due to a lack of strong regulations and trust in how their data is protected. This wariness affects online businesses by limiting consumer engagement and hindering companies' ability to offer personalized services.

In response, modern marketing has expanded beyond the classic 4 Ps—Product, Price, Place, and Promotion—to include Privacy, Personal Interests, Personal Networks, and Public Commentary. This shift acknowledges the importance of data privacy in digital marketing. Consumer privacy laws have evolved, but there is still a gap in awareness and protection. As digital marketing grows, businesses must ensure they handle customer data responsibly and transparently. This includes informing consumers about how their data is used and protecting it from unauthorized access. Organizations need to address these privacy concerns to maintain trust and build long-term relationships with their customers. This helps companies provide a safer online environment, drive customer loyalty, and gain a competitive edge.

Typically, e commerce sites will collect the following four types of customer data:

1. **Basic Data:** Includes personal details like name, contact information, age, job title, gender, and income.
2. **Interaction Data:** Covers customer touch points such as page views, downloads, subscriptions, social shares, demo requests, and email inquiries.
3. **Behavioral Data:** Tracks customer interactions with the product, including free trial sign-ups, logins, feature usage, deactivations, and license changes.
4. **Attitudinal Data:** Reflects customer opinions and feedback through online reviews, comments, ratings, and satisfaction surveys.

Review of Literature

Dev et al. (2019) explored privacy practices of WhatsApp users from Arab and Indian backgrounds, revealing significant regional differences in feature use and security management. Indians were less concerned about contact from strangers but more cautious with professional contacts, often hiding profile and location details from them. The study recommended privacy enhancements for WhatsApp users, including improved blocking and location-sharing features. Privacy issues with location-based services (LBS) that use GPS to track users' locations. highlighted concerns about revealing users' exact locations and discuss security methods like k-anonymity to protect privacy. The study also explores how queuing systems and location obfuscation can enhance privacy in LBS (Biswas and Sairam, 2018). Kumar, Kumar, and Bhasker (2018) explore how trust and security concerns impact user behavior on social networks. Their study finds that users' willingness to share personal information is significantly influenced by their trust in the platform and their interaction intentions. Senthil Kumar, Saravanakumar, and Deepa (2016) highlight that while social networks facilitate personal sharing, they also pose privacy risks due to users exchanging information for rewards. The study recommends safety measures like strong, regularly updated passwords and antivirus software to mitigate these risks. Many Facebook users become concerned about privacy only after sharing sensitive information and are often unaware of how to use privacy settings effectively. This gap between perceived and actual security settings results in more people viewing their posts and photos than users realize (Venkat et al. (2014).

Objectives of the Study

This research aims to understand the different data collection practices by e-commerce platforms in India and their privacy concerns about it. The study also focuses on awareness and privacy concerns relate to buying behavior among individuals. Accordingly, the objectives of the study are:

1. To examine consumer awareness of data collection practices of e-commerce platforms.
2. To identify specific privacy concerns of consumers.
3. To study the influence of privacy concerns on consumer purchasing behavior

Hypotheses

Ho1: There is no significant relationship between Demographical factors and awareness level on data collection by E- Commerce platforms.

Ha1: There is significant relationship between Demographical factors and awareness level on data collection by E- Commerce platforms.

Ho2: There is no significant relationship between awareness levels / concern about data breaches on e-commerce platforms and the likelihood of purchasing from platforms.

Ha2: There is significant relationship between awareness levels / concern about data breaches on e-commerce platforms and the likelihood of purchasing from platforms.

Research Methodology

Present study involves an analysis of consumer awareness and privacy concerns on e-commerce platforms. It aims to explore the relationship between awareness and buying behavior of consumers from e-commerce platforms in the Mahabubnagar, Gadwal, Nagarkurnool, Wanaparthy and Narayanapet districts. The research primarily uses data collected through a questionnaire, focusing on two key areas such as finding consumer awareness on data collection and data privacy concerns and to know the relationship between awareness/privacy concerns and buying behavior of consumers across e-commerce platforms. The questionnaire includes demographic questions and queries about awareness of data collection and privacy concerns with responses measured on a Likert scale from "Strongly Agree" to "Strongly Disagree". Google Form questionnaire is distributed through various channels, including social media platforms, Participants are provided with the link to the questionnaire and requested to complete it at their convenience. Anonymity and confidentiality of responses are ensured throughout the data collection process. Convenient sampling Method and the sample size – 210, Sample unit – All E- Commerce application users and the area of study consists of Mahabubnagar, Nagarkurnool, Gadwal, Wanaparthy and Narayanapet districts. Appropriate statistical tolls such as Chi square Test has been employed to assess whether there exists a significant relationship in Demographical factors and awareness levels and privacy concerns. Further, the Spearman correlation test, was employed to ascertain whether there is significant relationship between awareness on data collection /privacy concern about data breaches on e-commerce platforms and the likelihood of purchasing from platforms.

Data analysis and interpretation
1. Demographic profile of the respondents

Table - 1: Profile of the Respondents

Demographics		Frequency	Percentage
Age	Below 20	55	26.19%
	20 - 30	61	29.05%
	30 - 40	38	18.10%
	40 - 50	38	18.10%
	Above 50	18	8.57%
	Total	**210**	**100%**
Gender	Male	115	54.76%
	Female	95	45.24%

	Total	**210**	**100%**
Location	Semi Urban	88	41.90%
	Urban	65	30.95%
	Rural	57	27.14%
	Total	**210**	**100%**
How often do you shop online?	Monthly	69	32.86%
	Occasionally	53	25.24%
	Weekly	50	23.81%
	Daily	26	12.38%
	Never	12	5.71%
	Total	**210**	**100%**

Source: *Primary Data*

The data in Table 1 represents a demographic profile of 210 respondents based on their age, gender, location, and frequency of online shopping. The majority of the respondents fall within the age group of 20-30 years, followed closely by those under 20. The smallest group is those above 50 years. There is a slight majority of male respondents compared to female respondents. Most respondents are from semi-urban areas, followed by urban and rural locations. The data indicates that a majority of respondents shop online on a monthly basis, with a smaller group shopping weekly or daily. A small portion of respondents never shop online. Overall, the demographic profile indicates a diverse group of respondents, with a higher representation of younger individuals, males, semi-urban residents, and those who shop online regularly

2. Relationship between age and awareness levels

H_0: There is no significant relationship between age and awareness. In other words, the distribution of awareness is independent of age.

H_1: There is a significant relationship between age and awareness. In other words, the distribution of awareness depends on age.

Table 2 : Age and Awareness

Age	Awareness					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Below 20	24	19	11	1	0	55
20 - 30	16	25	17	3	0	61
30 - 40	15	15	6	2	0	38
40 - 50	6	18	10	3	1	38
Above 50	3	9	4	2	0	18
Total						210

Source: Primary data

The data indicates that awareness levels are generally higher among younger individuals. The age group below 20 shows the strongest positive responses, with most strongly agreeing or agreeing with the awareness

statements. The above 50 age group shows the lowest levels of strong agreement and agreement, with more neutral and negative responses.

Table – 2.1: Relationship between age and awareness levels

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	17.974	12	.116
Likelihood Ratio	17.304	12	.139
Linear-by-Linear Association	8.741	1	.003
N of Valid Cases	210		

Source: *Primary Data*

The p-value which is 0.116 is higher than 0.05. Hence, the null hypothesis is accepted which means that there is no significant relationship between age and awareness. In other words, the distribution of awareness is independent of age.

3. Relationship between Gender and Awareness levels

H0: There is no significant relationship between gender and awareness.

H1: There is a significant relationship between gender and awareness.

Table 3 : Gender and Awareness

Gender	Awareness					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Male	40	46	22	7	0	115
Female	24	40	26	4	1	95
	Total					210

Source: Primary data

Males generally show higher positive awareness, with more strong agreements and agreements compared to females. Females have a higher number of neutral responses, indicating less certainty.

Table – 3.1: Relationship between gender and awareness levels

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.979	3	.264
Likelihood Ratio	4.380	3	.223
Linear-by-Linear Association	1.940	1	.164
N of Valid Cases	210		

Source: *Primary Data*

The p-value is 0.264, which is higher than 0.05. Hence, the null hypothesis is accepted and alternative hypothesis is rejected which means that there is no significant relationship between gender and awareness.

4. Relationship between Location and Awareness levels

H0: There is no significant relationship between location and awareness.

H1: There is a significant relationship between location and awareness.

Table 4 : Location and Awareness

Location	Awareness					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Urban	29	21	12	3	0	65
Semi urban	21	38	24	4	1	88
Rural	14	27	12	4	0	57
Total						210

Source: Primary data

In urban areas, people generally show strong positive awareness with fewer neutral or negative responses. Semi-urban areas also have positive awareness but with more neutral responses and a few disagreements. Rural areas exhibit positive awareness as well, though with the fewest strong agreements.

Table – 4.1 : Relationship between location and awareness levels

	Value	d.f.	Asymptotic Significance (2-sided)
Pearson Chi-Square	10.572	6	.103
Likelihood Ratio	10.615	6	.101
Linear-by-Linear Association	5.850	1	.016
N of Valid Cases	210		

Source: *Primary Data*

The p-value of 0.103 is greater than the common significance level threshold of 0.05. Hence, the result is not statistically significant. This means there is no strong evidence to suggest that location and awareness are related.

5. Relationship between Frequency of buying and Awareness levels

H0: There is no significant relationship between the frequency of online buying and awareness. **H1:** There is a significant relationship between the frequency of online buying and awareness.

Table 5 : Frequency of buying and Awareness

Frequency of buying	Awareness					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Daily	10	9	5	1	1	26
Weekly	19	20	8	3	0	50
Monthly	19	33	14	3	0	69
Occasionally	16	20	15	2	0	53
Never	0	4	6	2	0	12
Total						210

Source: Primary data

Frequent buyers, such as those purchasing monthly or weekly, generally show strong positive awareness, with many agreeing or strongly agreeing with the statements. Daily buyers also have positive awareness but with fewer strong agreements. Occasionally buyers have moderate positive awareness with a mix of strong agreements and neutral responses. Those who never buy have the lowest positive awareness and a higher proportion of neutral responses.

Table – 5.1 : Relationship between frequency of buying and awareness levels

	Value	d.f.	Asymptotic Significance (2-sided)
Pearson Chi-Square	17.710	12	.125
Likelihood Ratio	17.272	12	.140
Linear-by-Linear Association	3.425	1	.064
N of Valid Cases	210		

Source: *Primary Data*

The p-value of 0.125 is more than 0.05. Hence, the result is not statistically significant. This indicates that there is no evidence to suggest that the frequency of online buying is related to awareness.

6. Relationship between age and data privacy concern

H0: There is no significant relationship between age and privacy concerns.

H1: There is a significant relationship between age and privacy concerns.

Table 6: Age and data privacy concerns

Age	Privacy concern					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Below 20	23	25	5	1	1	55
20 - 30	21	28	10	0	2	61
30 - 40	14	18	4	2	0	38
40 - 50	10	18	5	3	2	38
Above 50	4	11	3	0	0	18
Total						210

Source: Primary data

Younger age groups (Below 20 and 20-30) express higher privacy concerns, with many strongly agreeing or agreeing. Privacy concerns decrease with age, as shown by fewer strong agreements and more neutral responses in older groups. The 30-40 and 40-50 age groups have moderate privacy concerns, while those above 50 show the lowest level of concern.

Table 6.1: Relationship between age and privacy concerns

	Value	d.f.	Asymptotic Significance (2-sided)
Pearson Chi-Square	13.286	12	.349
Likelihood Ratio	15.335	12	.224
Linear-by-Linear Association	3.293	1	.070
N of Valid Cases	210		

Source: *Primary Data*

Since the p-value of 0.349 is higher than 0.05, the result is not statistically significant. This suggests that there is no strong evidence to indicate that age and privacy concerns are related.

7. Relationship between Gender and Data privacy concern

H0: There is no significant relationship between gender and privacy concerns.

H1: There is a significant relationship between gender and privacy concerns.

Table - 7: Gender and data privacy Concerns

Gender	Privacy concern					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Male	38	61	11	3	2	115
Female	34	39	16	3	3	95
Total						210

Source: Primary data

Males show a higher level of privacy concern compared to females, with more strongly agreeing and agreeing responses. Females have a higher proportion of neutral responses and slightly more disagreement. Both genders have low levels of strong disagreement.

Table – 7.1 : Relationship between gender and privacy concerns

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.800	3	.849
Likelihood Ratio	.798	3	.850
Linear-by-Linear Association	.020	1	.886
N of Valid Cases	210		

Source: *Primary Data*

The p-value of 0.849 is much higher than the 0.05. This suggests that there is no strong evidence to support a relationship between gender and privacy concerns.

8. Relationship between Location and Data privacy concern

H0: There is no significant relationship between location and privacy concerns.

H1: There is a significant relationship between location and privacy concerns.

Table - 8: Location and data privacy concerns

Location	Privacy concern					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Urban	26	30	7	2	0	65
Semi urban	31	39	11	3	4	88
Rural	15	31	9	1	1	57
	Total					210

Source: Primary data

Privacy concerns are highest in semi-urban areas, where people show more strong agreements and agreements. Urban residents also express notable privacy concerns but with fewer strong agreements. Rural areas have the lowest privacy concerns, with a higher proportion of neutral responses and fewer strong agreements.

Table – 8.1: Relationship between location and privacy concerns

	Value	d.f.	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.636	6	.356
Likelihood Ratio	7.882	6	.247
Linear-by-Linear Association	2.391	1	.122
N of Valid Cases	210		

Source: *Primary Data*

The p-value 0.356 is greater than 0.05 and it suggests that there is no strong evidence to indicate that privacy concerns vary significantly across different locations.

9. Relationship between Frequency of buying and Data privacy concern

H0: There is no significant relationship between the frequency of online buying and privacy concerns.

H1: There is a significant relationship between the frequency of online buying and privacy concerns.

Table - 9: Frequency of buying and data privacy concerns

Frequency of buying	Privacy concern					Total
	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	
Daily	13	11	2	0	0	26
Weekly	17	24	4	3	2	50
Monthly	27	29	10	1	2	69
Occasionally	15	29	7	2	0	53
Never	0	7	4	0	1	12
Total						210

Source: Primary data

People who buy monthly or weekly tend to have the highest privacy concerns, with many strongly agreeing or agreeing. Daily buyers also express privacy concerns but at lower levels. Occasionally buyers have moderate concerns, while those who never buy show the lowest concern, with more neutral responses.

Table – 9.1: online purchase frequency and privacy concerns

	Value	d.f.	Asymptotic Significance (2-sided)
Pearson Chi-Square	17.990	12	.116
Likelihood Ratio	23.469	12	.024
Linear-by-Linear Association	5.556	1	.018
N of Valid Cases	210		

Source: *Primary Data*

The p-value of 0.116 is higher than the conventional level of significance 0.05. Since the p-value of 0.116 is greater than 0.05, the result is not statistically significant.

10. Relationship between Awareness levels and Buying behaviour

H0: There is no significant relationship between awareness of data collection practices (browsing behavior) and the likelihood of purchasing from e-commerce platforms.

H1: There is a significant relationship between awareness of data collection practices (browsing behavior) and the likelihood of purchasing from e-commerce platforms.

Table - 10: Correlation between awareness and intention of online purchase

			I am aware that e-commerce platforms collect personal data	I am more likely to purchase from an e-commerce platform
Spearman's rho	I am aware that e-commerce platforms collect personal data	Correlation Coefficient	1.000	.220[**]
		Sig. (2-tailed)	.	.001
		N	210	210
	I am more likely to purchase from an e-commerce platform	Correlation Coefficient	.220[**]	1.000
		Sig. (2-tailed)	.001	.
		N	210	210

Source: *Primary Data*   **. Correlation is significant at the 0.05 level (2-tailed).

Spearman's rho Correlation Coefficient (0.220): This coefficient measures the strength and direction of the monotonic relationship between awareness of data collection and the likelihood of purchasing from e-commerce platforms with transparent privacy policies. A positive value of 0.220 suggests a weak to moderate positive correlation. This means that higher awareness of data collection practices is associated with a slightly higher likelihood of preferring platforms with strong privacy policies.

Since the p-value is 0.001, which is less than 0.05, results in the rejection of null hypothesis**.** This means that there is a statistically significant positive relationship between the awareness of data collection practices and the likelihood of purchasing from e-commerce platforms with strong privacy policies.

11. Relation between Data privacy concerns and Buying behavior

H0: There is no significant relationship between concern about data breaches on e-commerce platforms and the likelihood of purchasing from platforms.

H1: There is a significant relationship between concern about data breaches on e-commerce platforms and the likelihood of purchasing from platforms.

Table - 11: Correlation between data breach concerns and likelihood of online purchase

			I am concerned about Data breaches on e-commerce platforms	I am more likely to purchase from an e-commerce platform
Spearman's rho	I am concerned about Data breaches on e-commerce platforms	Correlation Coefficient	1.000	.122**
		Sig. (2-tailed)	.	.077
		N	210	210
	I am more likely to purchase from an e-commerce platform	Correlation Coefficient	.122	1.000
		Sig. (2-tailed)	.077	.
		N	210	210

Source: *Primary Data*   **. Correlation is significant at the 0.05 level (2-tailed).

Spearman's rho Correlation Coefficient (0.122): This coefficient measures the strength and direction of the monotonic relationship between concern about data breaches and the likelihood of purchasing from e-commerce platforms with transparent and robust privacy policies. A value of 0.122 suggests a very weak positive correlation. This means there is a slight tendency for individuals who are concerned about data breaches to prefer platforms with strong privacy policies, but the relationship is weak.

Since the p-value is 0.077, which is slightly greater than 0.05, the null hypothesis is accepted. This means that, based on this test, there is no strong statistical evidence to suggest a significant relationship between concern about data breaches and the likelihood of purchasing from e-commerce platforms with robust privacy policies.

Findings

- Age groups range primarily from 20 to 40 years, with respondents from both urban and rural locations. Both genders are represented, with responses from individuals who shop online occasionally to monthly.
- Most respondents agree or strongly agree that they are aware e-commerce platforms collect personal data, including contact details, payment information, purchase history, browsing behaviour, and location data. A significant number of respondents expressed neutrality or agreement towards understanding e-commerce privacy policies, indicating a moderate level of awareness.
- Privacy concerns heavily influence whether respondents trust and choose to make purchases on specific e-commerce platforms, indicating that privacy is a critical factor in consumer decision-making. Concerns are high regarding data breaches, unauthorized data sharing, misuse of personal data, and the security of payment information. Many respondents indicated they are more likely to purchase from platforms with transparent and robust privacy policies. Trust in e-commerce platforms is notably affected by privacy concerns, with many consumers reading privacy policies and preferring platforms with third-party security certifications.

- There is a significant positive correlation between awareness of data collection practices and the likelihood of preferring platforms with robust privacy policies.

- There is a weak positive correlation between concern about data breaches and the likelihood of purchasing from e-commerce platforms with robust privacy policies. Although the correlation is weak, it is not statistically significant at the 0.05 level, suggesting that concern about data breaches does not have a strong influence on purchasing behavior.

- Offer consumers privacy settings with customization, allowing them to choose the level of data sharing they are comfortable with, thereby improving their shopping experience while addressing privacy concerns, showing a clear preference for platforms that prioritize their privacy.

Suggestions

- Given that no significant relationships were found between gender or age and privacy concerns or awareness, it suggests that privacy-related factors might be universally relevant across different demographics. E-commerce platforms should consider addressing privacy concerns broadly rather than tailoring privacy policies based on demographic factors.

- Since there is a significant positive correlation between awareness of data collection practices and the likelihood of preferring platforms with robust privacy policies, e-commerce platforms could benefit from enhancing transparency about data practices. Educating customers on how their data is used and the measures taken to protect it might increase customer loyalty and preference.

- Although concern about data breaches showed a weak correlation with purchasing behavior, emphasizing strong and transparent privacy policies remains important. Ensuring that privacy policies are easily accessible and clearly communicated can build trust and potentially influence purchasing decisions.

- E-commerce platforms should create concise and easy-to-understand privacy policies to encourage more consumers to read them.

- Introduce simple, user-friendly privacy settings that allow consumers to control what data they share, helping them feel more secure. Consider offering incentives, such as discounts or personalized recommendations, to consumers who opt to share more data, balancing privacy concerns with added value.

References

- Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems, 41*(4), 62–96. https://doi.org/10.17705/1cais.04104

- Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041.

- Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

- Gerke, S., & Rezaeikhonakdar, D. (2022). Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps. *Intelligence-Based Medicine, 6*(April), Article 100061. https://doi.org/10.1016/j.ibmed.2022.100061

- Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers and Security, 66*, 129–141. https://doi.org/10.1016/j.cose.2017.01.010

- Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management, 34*(6), 761–769. https://doi.org/10.1016/j.ijinfomgt.2014.07.006

- Nijssen, E. J., van der Borgh, M., & Totzek, D. (2022). Dealing with privacy concerns in product-service system selling: Value-based selling as fair treatment practice. *Industrial Marketing Management, 105*(June), 60–71. https://doi.org/10.1016/j.indmarman.2022.05.017

- Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization, and societal level: A literature review. *Vilakshan - XIMB Journal of Management, 18*(2), 171–186. https://doi.org/10.1108/xjm-08-2020-0096

- Senarathna, I., Yeoh, W., Warren, M., & Salzman, S. (2016). Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs. *Australasian Journal of Information Systems, 20*, 1–20. https://doi.org/10.3127/ajis.v20i0.1193

- Sheth, S., Kaiser, G., & Maalej, W. (2014). Us and them: A study of privacy requirements across North America, Asia, and Europe. In *Proceedings - International Conference on Software Engineering* (Vol. 1, pp. 859–870). https://doi.org/10.1145/2568225.2568244

- Wang, X., Zhang, J., Ma, D., & Sun, H. (2023). Green agricultural products supply chain subsidy scheme with green traceability and data-driven marketing of the platform. *International Journal of Environmental Research and Public Health, 20*(4), Article 3056. https://doi.org/10.3390/ijerph20043056

Online resources

- https://www.thecommerceshop.com/blog/customer-data-and-ecommerce-how-important-is-it/ retrieved on 10-8-2024

- https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/ retrieved on 05-07-2024

- https://www.ibm.com/reports/data-breach retrieved on 10-08-2024

- https://www.fortinet.com/resources/cyberglossary/data-security retrieved on 17-08-2024

- https://www.crowdstrike.com/cybersecurity-101/data-protection/data-privacy/ retrieved on 10-06-2024
- https://www.signalhire.com/blog/what-is-buyer-behavior-types-influencing-factors-effects/ retrieved on 06-08-2024