Educational Administration: Theory and Practice
2023, 29 (3), 1474-1483
ISSN: 2148-2403
https://kuey.net/

Research Article

Exploring Teenagers' Privacy Concerns And Defensive Measures Adopted Online

Ms. Sangeeta Kumawat[1*], Dr. Vilas Chauhan[2]

[1*]Research Scholar Department of Commerce & Business Management, Faculty of Commerce,
[2]Assistant Professor Faculty of Commerce, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India

Citation: Ms. Sangeeta Kumawat[1], et.al (2023). Exploring Teenagers' Privacy Concerns And Defensive Measures Adopted Online, *Educational Administration: Theory and Practice*, 29 (3), 1474-1483
Doi: 10.53555/kuey.v29i3.9866

ARTICLE INFO

ABSTRACT

This study is an attempt to explore the Internet browsing behaviour of teenagers focusing on their' online privacy concerns and defensive measures adopted online. The study was undertaken specifically to get insights into teenagers' online browsing behaviour, their perceived degree of sensitivity towards privacy concern, the types of defensive measures adopted by them in relation to the perceived degree of privacy concerns, and to study the privacy related behaviour of teenagers. The primary objectives of the study focused on teenagers' concerns about online privacy, willingness to disclose / not to disclose personally identifiable information, and actual disclosure / non-disclosure of their real personal information online. A survey conducted in Jaipur city of Rajasthan, India with 184 teenagers aged 13-19 revealed that their perception, attitude, and concern towards personal data security in view of online privacy issues was quite commendable. They are extra cautious when it comes to sharing their personal information on the website in the process of registering for the same. But, at the same time they do not hesitate in submitting false / fabricated information when they don't have a choice. A surprising finding revealed by this research is that on the one hand they strongly show their concern for personal information / data security but at the same time they do give their permission for the same. Some of the findings surprisingly surface that their cognitive responses are not always seen in their actual behaviour. Finally, the privacy related behaviour reveals that they do take all precautionary measures and at the same time display a variety of defensive measures endorsing the fact that they are much smarter than previous generations!

Keywords: Spamming, Data Base Marketing, Permission Marketing, Information On–Demand, Privacy Paradox, Consumer Privacy, Privacy Concerns, Privacy Policy

1. INTRODUCTION:

Consumer Privacy is information privacy as it relates to the consumers of products and services. A variety of social, legal and political issues arise from the interaction of the public's potential expectation of privacy and the collection and dissemination of data by business or merchants. Consumer privacy generally originates with the interruption occurred due to unwanted mobile advertisements and marketing activities. The receiver gets disturbed while receiving these marketing messages or advertisements. Technology allows for this type of interruption marketing, is the main issue of concern. (Cleff, 2007)

1.1 Definition of the concept of "Privacy Concern"

With the emergence of the internet, people have changed the way they interact; the use of social networking sites has skyrocketed. Facebook, Twitter, and Instagram are growing at a surprising rate. Social Networking Sites users create their accounts to come across with people of the same interests or experiences. This process of registration is hazardous for the users as they must share their personal information with both friends and strangers as well. While an increasing number of users have joined various social networking sites, their privacy concerns persist. (Xu et al., 2011; Mahmoodi et al., 2018; Hong and Oh, 2020)
Marketing companies are usually inclined to gather more data that can be used for personalized marketing and

the main factor that affects consumers' privacy concern is completely based on trust. (Bleier et al., 2020). Marketing companies always have an inclination for the obstinate use of the collected data whereas the customers are inclined to have more control over their shared data and on the other hand, customers want to use digital technology services without compromising their privacy. (Anic et al., 2019; Hajli and Lin, 2016; Mazurek and Malagocka, 2019; Xu et al., 2012).

Privacy concern refers to an individual's worry or anxiety about the potential negative consequences of disclosing or sharing personal information, stemming from a perceived lack of control over how that information is safeguarded and used.

This summary effectively highlights the main aspects of privacy concerns. Here's a brief breakdown of each key point:

Perceived Risk: Individuals often feel that sharing personal information opens them up to various risks, such as it being misused, accessed without authorization, or used in ways they don't approve of.

Lack of Control: One of the strongest drivers of privacy concerns is the perception that individuals don't have control over their personal data once it's shared. This could mean uncertainty about how data is collected, who uses it, and for what purpose.

Emotional State: Privacy concerns are often associated with emotional reactions. People may feel anxiety, discomfort, or unease about their information being exposed, or about the loss of their right to privacy or freedom from surveillance.

Various Contexts: Privacy concerns are context dependent. They arise not only in online environments like social media or e-commerce but also in real-world interactions, especially when sensitive data is shared with businesses or even people in personal relationships.

Impact on Behavior: When privacy concerns are high, people often alter their behaviors. For example, they might limit the amount of personal data they share online, use privacy tools like stronger passwords, or actively choose to opt out of tracking systems.

Data Acquisition and Misuse: The easy access to personal data online, combined with the possibility that this data can be misused, contributes significantly to privacy concerns. This includes situations where personal or intimate data is unintentionally shared or maliciously exploited.

Advertisers and Loss of Privacy: Many individuals worry about their personal data being harvested by advertisers without their explicit consent. This can lead to a sense of privacy erosion, as they feel their information is constantly being tracked and used for targeted marketing, often without their knowledge or agreement.

1.2 Privacy Policies

The main issue within the domain-related policies is how to protect customers' privacy and how to put an end to unethical use of data provided by the customers. (Dogruel, 2019)

This is mandatory for marketing companies to disclose their privacy policy, why the data is being collected and for what use. How the data collected would be handled by the marketing companies. (Acquisti et al., 2016; Distler et al., 2020)

Consequently, allowing customers to permit or decline the policy of how companies will use their data, why it will be used, and for what it will be used for. (Afolabi et al., 2021; Anic et al., 2019; Mazurek and Malagocka, 2019)

1.3 Constitutional Provisions

The Constitution of 1950 does not expressly recognize the right to privacy. However, the Supreme Court first recognized in 1964 that there is a right of privacy as stated in the Constitution under Article 21.

Information Technology Act, 2000

In May 2000, the Indian Parliament passed the Information Technology Bill, now known as the Information Technology Act, 2000. The Act covers cyber and related information technology laws in India.

The Personal Data Protection Bill, 2006

Upon the footprints of the foreign laws, this bill has been introduced in Rajya Sabha in 2006. The purpose of this bill is to provide protection of personal data and information of an individual collected for a particular purpose by organizations for commercial or other purposes.

Telecom Unsolicited Commercial Communications Regulations, 2007

Telecom Regulatory Authority of India (TRAI) had issued Telecom Unsolicited Commercial Communications Regulations in 2007.The regulation was enacted in order to develop a mechanism for curbing the unsolicited telemarketing calls. The primary objective of the National Do Not Call Registry was to curb unsolicited commercial communication. Under this regulation, unsolicited commercial communication has been defined as any message, through telecommunications service, which is transmitted for the purpose of informing about, or soliciting or promoting any commercial transaction in relation to goods, which a subscriber opts not to receive.

Personal Data Protection Bill, 2019

The Bill aims to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the fundamental rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data.

The Digital Personal Data Protection (DPDP) Act, 2023

The 2019 bill exempted certain entities and businesses from notice and consent requirements under certain circumstances—for lawful state functions, medical and health services during emergencies or epidemics, breakdown of public order, employment-related data processing, the prevention and detection of unlawful activity, whistleblowing, and credit recovery, among others.

2. LITERATURE REVIEW:

The researchers have conducted an extensive literature review on privacy concern issues and objectives framed for the current research study. A brief review of the selected base articles is presented below:

- *Privacy And Security Information Awareness and Disclosure of Private Information By Users Of Online Social Media In The Ibadan Metropolis, Nigeria Omotayo, F. O. O., & Olayiwola, J. O. (2023).*

The study showed the behavioural attitudes of potential or past consumers regarding sharing their personal information and disclosing private data on online platforms. It also discovered the level of security awareness of the users of online social media (OSM). The factors that could affect the rate of disclosing private/personal information on social media platforms have also been identified.

- *Consumer Acceptance of The Use of Artificial Intelligence in Online Shopping: Evidence From Hungary Nagy, S., & Hajdú, N. (2021).*

The technology acceptance model (TAM) was used for investigating consumer acceptance of the use of Artificial Intelligence in online shopping. Trust was considered as a main factor that influences consumer's attitudes towards artificial Intelligence. Perceived usefulness of AI other than perceived case of use was considered the second most key factors that influence attitude and behavioural intentions of the consumers.

- *Privacy Concerns and Benefits Of Engagement With Social Media-Enabled Apps: A Privacy Calculus Perspective Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020).*

The users of social media apps merely tended to disclose their personal/private information. Social privacy concerns are highly affected by the risk factor.

- *Users' Information Privacy Concerns and Privacy Protection Behaviors In Social Networks Adhikari, K., & Panda, R. K. (2018).*

The main purpose of the study was to explore the impact of antecedents of users' information privacy concerns on privacy protection behaviour, perceived vulnerability, severity and self-efficacy have great impact on consumers' behaviour of data sharing. In such cases, rewards and other monetary benefits can't influence a customer for sharing or not sharing his personal data on any social networking site.

- *Privacy Concerns and Self-Disclosure in Private And Public Uses Of Social Media Anatoliy Gruzd and A´ngel Herna´ndez-Garcı´a, (2018).*

The study revealed that privacy paradox is found only if there is no significant relationship between the use's privacy concerns and the amount of disclosing personal information. The authors figured out the main five dimensions of self-discloser i.e. amount, depth, polarity, accuracy and interest. Two aspects of privacy concerns too have been figured out i.e. organizational concerns and social threats.

- *The Privacy Paradox–Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review Barth, S., & De Jong, M. D. (2017).*

Two main considerations: (i) Risk – benefit evaluation and (ii) Risk assessment is negligible as the willingness of sharing personal information is based on some factors that affect their decision-making power.

- *Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal Of Communication Baruh, L., Secinti, E., & Cemalcilar, Z. (2017).*

This paper investigated the relation between use of social networking sites and enclosed services, the level of sharing information and measures taken to protect user to privacy. The users who are concerned about their privacy are less likely to share their personal information and are more likely to use privacy protective measures.

- *Privacy Concerns and Online Purchasing Behaviour: Towards An Integrated Model Fortes, N., & Rita, P. (2016).*

Past or potential consumers using online platforms to buy things are more likely to make their decisions to purchase the product or use the service on behalf of measurements taken by the marketing companies to secure their personal data from being stolen or misused. The main factors like trust, risk, planned behaviour, to acceptance of technology affect the decision-making power of a consumer.

3. RESEARCH OBJECTIVES:

Research objectives have evolved from research problem statements, research gaps, and by in depth study of domain and review of literature. The objectives of the current study are as follows:

1. To get insights into teenagers' online browsing behaviour.
2. To explore the perceived degree of sensitivity of teenagers towards privacy concern.
3. To determine the types of defensive measures adopted by teenagers in relation to the perceived degree of privacy concerns.
4. To study the privacy related behaviour of teenagers.

4. RESEARCH METHODOLOGY:

Descriptive research design was used to fulfill the objectives designed for the study. Non-probability, and convenience method of sampling was used to collect primary data by surveying school and college/university students who were in close contact with the researchers. Primary data was collected from respondents. A structured non-disguised questionnaire was prepared and then administered through Google form.

The link of this Google form was shared among the students studying in schools and colleges/universities in Jaipur. The link of the Google form questionnaire was shared to 206 students at schools and colleges/universities. Of the 206 questionnaires, 196 students responded out of which 12 questionnaires were received with incomplete responses. Hence, after excluding those 12 questionnaires, the final data analysis of 184 respondents was undertaken and the findings of the same are presented in the study.

The questionnaire consisted of following sections: Demographic details; general questions on internet browsing behaviour of respondents, awareness about privacy concern concept, perceived degree of sensitivity for information privacy, and privacy related behaviour. Appropriate scales derived from past studies were used to measure the behavioural aspects of the respondents in all these areas. Five-point Likert scale anchored with (1) Strongly Disagree to (5) Strongly Agree was used to identify the 'Agreements' and 'Disagreements' to various items of these scales. Respondents were asked to indicate their level of awareness about the concept of 'Privacy Concern'. These statements focused on the level of awareness of a consumer about the concept of 'Privacy Concern' for some common products or services on some specific platforms. Since the research paper focused on the behavioural pattern of school and college students related to privacy, the analysis of the constructs was majorly done through frequency count. After gaining some basic insights, the researchers would then undertake a detailed study examining the degree of awareness privacy concerns of the respondents as a part of their future research.

Before administering the final questionnaire, a pilot study was conducted on 50 local respondents to check the accuracy of responses in line with the research objectives. Some required changes were made in the first draft of the questionnaire and then the final questionnaire was approved. The internal consistency of scales was verified with Cronbach's Alpha. The scales used for the study showed satisfactory scores ranging between 0.73 to 0.89.

IBM SPSS Statistics - Trial Subscription Package was used to analyze the primary data. Descriptive statistics, average mean, and standard deviation were calculated.

5. DATA ANALYSIS AND INTERPRETATION:

5.1 Demographic Profile of Respondents

Table 1: Profile of respondents

Demographic variables		**Frequency**	**Percent**
Gender	Female	77	41.85
	Male	107	58.15
Education	S.S.C.	68	37
	H.S.C.	79	43
	Under-Graduate Students	37	20

5.2 Internet Browsing Behaviour of Teenagers

Table 2: Internet Browsing Behaviour of Teenagers

Questions	Alternatives	Frequency	Percent
Period of Usage of Internet	1 to 3 Years	89	48.37
	Less than a Year	14	7.61
	More than 3 Years	81	44.02
Primary Usage (Purpose) of Internet	Entertainment, Education, Work related, Current events (News, Sports, Weather etc.), Online shopping, Gathering product information, Personal finance, Travel-related needs, Communication (Email, Chat), Social Networking, Gaming	5	2.72
	Entertainment, Education, Work related, Current events (News, Sports, Weather etc.), Online shopping, Personal finance, Communication (Email, Chat), Social Networking,	7	3.80
	Entertainment, Education, Work related, Current events (News, Sports, Weather etc.), Online shopping, Gathering product information, Personal finance, Travel-related needs, Communication (Email, Chat), Social Networking	7	3.80
	Entertainment, Education, Work related, Current events (News, Sports, Weather etc.), Online shopping, Personal finance, Travel- related needs, Communication (Email, Chat), Social Networking	8	4.35
	Other combinations of purposes given	157	85.33
Reading of Terms and Conditions on Websites	Never	4	2.17
	Rarely	48	26.09
	Sometimes	67	36.41
	Often	61	33.15
	Always	4	2.17
Rejected entering a website since you did not agree to their Terms and Conditions	Never	4	2.17
	Rarely	58	31.52
	Sometimes	86	46.74
	Often	36	19.57
	Always	00	00.00
Agree to Terms and Conditions, despite knowing that the personal data will be used for marketing purposes	Yes	147	79.89
	No	37	20.11
Knowledge about Consumer Disputes Redressal Commission	Yes	166	90.22
	No	18	9.78
Knowledge about Consumer Protection Act	Yes	171	92.93
	No	13	7.07
Submission of false personal information when asked to register on the website	Never falsified information	09	04.89
	Under 25% of the time	15	08.15
	26 – 50 % of the time	10	05.43
	51 – 75 % of the time	22	11.95
	Over 75% of the time	110	59.78
	Never registered with a site	18	09.78
Concerned about your security on the internet	Not at all concerned	11	5.97
	Slightly concerned	18	9.78
	Somewhat concerned	50	27.17
	Moderately concerned	96	52.17
	Extremely concerned	19	10.32

- From among the total respondents surveyed, 89 respondents (48.37%) have been using internet for 1 to 3 years and 81 respondents (44.02%) have been using internet for more than 3 years.
- Respondents when surveyed about the primary use of internet, 157 respondents (80%) use internet for Entertainment, Education, Work related, Current events (News, Sports, Weather etc.), Online shopping, Gathering product information, Personal finance, Travel-related needs, Communication (Email, Chat), Social Networking, Gaming etc.
- From among the total respondents, 61 respondents (33.15%) often read terms and conditions given on the websites. Only 4 respondents (2.17%) are such who always read the terms and conditions, whereas 67 respondents (36.41%) sometimes read the terms and conditions. Around 52 respondents (28.26%) of respondents never or rarely read the terms and conditions given on the websites.
- Surprisingly, none of the respondents surveyed rejected entering a website despite not agreeing to their terms and conditions. However, 36 respondents (19.57%) reject entering a website quite often because of their non-

agreement with the terms and conditions of the website.

- Further, despite knowing that the personal data will be used for marketing purposes, 147 respondents (79.89%) agree to Terms and Conditions of the websites and end up registering with the websites.
- 166 respondents (90.22%) are aware about 'Consumer Disputes Redressal Commission'.
- 171 respondents (92.93%) do have knowledge about the Consumer Protection Act.
- When asked to register with the website by providing personal information, 22 respondents (11.95%) of the total respondents enter falsified information for 51-75% of the time. 110 respondents (59.78%) register with the website by entering falsified information for over 75% of the time and 10 respondents (0.5.43%) register by giving false information for 26-50% of the time.
- Respondents, when asked to express their concern about their security on the internet, surprisingly only 19 respondents (10.32%) are extremely concerned. Whereas, around half of the total respondents i.e., 96 respondents (52.17%) are moderately concerned about their security. 50 respondents (27.17%) have expressed 'somewhat concern' about their security over internet.

5.3 Perceived Degree of Sensitivity towards Information Privacy

Table 3: Perceived Degree of Sensitivity towards Information Privacy

Questions	Alternatives	Frequency	Percent
In general, what is more important to you?	Convenience	14	7.6
	Privacy	170	92.4
If asked to provide personal information, how often did you refuse to give the requested personal information / leave the web site?	Always	3	1.63
	Often	76	41.30
	Rarely	20	10.87
	Sometimes	85	46.20
If you do provide personal information to web sites, how often did you provide false information?	Always	4	2.17
	Never	1	0.54
	Often	66	35.87
	Rarely	22	11.96
	Sometimes	91	49.46
How often do you feel that your privacy has been invaded by marketing activities done by companies or ad agencies?	Always	5	2.72
	Often	77	41.85
	Rarely	12	6.52
	Sometimes	90	48.91
How comfortable do you feel about companies gathering your data for marketing purposes?	Comfortable	27	14.67
	Uncomfortable	113	61.41
	Unsure	8	4.35
	Very Comfortable	1	0.54
	Very Uncomfortable	35	18.92
Do you think that companies should be allowed to share / sell information about your buying habits to third parties if that increases value for you as a customer?	No	139	75.54
	Yes	45	24.46

The perceived degree of sensitivity towards information privacy refers to how individuals subjectively assess the potential harm or risk associated with the disclosure of personal information, influencing their privacy concerns and willingness to share data. Analysis of the primary data reveals following:

Respondents, when asked about the importance given by them between the two: Convenience and Privacy, 170 respondents (92.4%) favored privacy as against 14 (7.6%) voting for convenience. Further, from among 184 respondents, most of the time, 76 respondents (41.30%) quite often, either refused to give personal information or preferred to leave the website. 3 respondents were such who always refused to give personal information and were also ready to leave the website also. 66 respondents (35.87%) of the total respondents often provided false information. Further, around 77 respondents (41.85%) of the total respondents surveyed quite often felt that their privacy has been invaded because of the marketing campaigns undertaken by the marketers or by the advertising agencies. Again, a very logical finding reveals that 113 respondents (61.41%) of the respondents feel uncomfortable and 35 respondents (18.92%) feel very uncomfortable, knowing that the personal data shared by them with the marketers will be used for marketing purposes. Finally, respondents when asked whether companies should be allowed to share / sell information about their buying habits to third parties if that increases value for him as a customer, majority of respondents i.e., 139 respondents (75.54%) strongly feel that companies should not be allowed to share the customers data with the third parties.

5.4 Defensive Measures Adopted Online:

The following are some major defensive measures adopted by respondents at individual level, when they perceive or feel a threat to the invasion of their privacy.

- **Fabricate:**

- 180 respondents (97.5%) consider making up fictitious responses to avoid giving the websites their real information.

- 178 respondents (97.0%) resort to another name or web/email address when registering with a website to gain full access and benefits as a registered user without divulging their real identity.
- 178 respondents (96.6%) smartly end up filling data partially.

- **Protect:**

- 179 respondents (97.2%) considered making use of software so that the recipient cannot track the origin of their e-mail account.
- 179 respondents (97.6%) are using software to eliminate cookies that are likely to track their browsing behaviour.
- 180 respondents (97.8%) tend to use software to disguise their identity.

- **Withhold:**

- 179 respondents (97.3%) are reluctant to register on the websites if they feel a threat to the invasion of their privacy.
- 178 respondents (96.9%) refuse personal information to the website which they feel are likely to threaten their privacy.
- 179 respondents (97.4%) will avoid visiting the same website again.

The above analysis reveals that fabricating, protecting and withholding the data/information, all three defensive measures are used by majority of the respondents to deal with privacy issues.

5.5 Privacy Related Behaviour

Table 4: Privacy related Behaviour (General Caution)

GENERAL CAUTION	Alternatives	Frequency	Percent
Do you only register for websites that have a privacy policy?	Always	14	7.61
	Never	1	0.54
	Often	152	82.61
	Rarely	3	1.63
	Sometimes	14	7.61
Do you read a website's privacy policy before you register your information?	Always	41	22.28
	Often	100	54.35
	Rarely	3	1.63
	Sometimes	40	21.74
Do you look for a privacy certification on a website before you register your information?	Always	30	16.30
	Often	112	60.87
	Rarely	2	1.09
	Sometimes	40	21.74
Do you read license agreements fully before you agree to them?	Always	42	22.83
	Never	1	0.54
	Often	98	53.26
	Rarely	5	2.72
	Sometimes	38	20.65

To explore the privacy related behaviour of college students, some basic questions related to 'general caution' and 'technical protection' were asked. Again, based on frequency analysis, the findings for both surfaced some important insights. Around 152 respondents (82.61%) of the respondents quite often registered only for those websites which followed a strict privacy policy. And that too after reading the website's privacy policy. Not only this, 142 respondents (77.17%) looked for a privacy certification on the website before registering on the website. Around 42 respondents (22.83%) always read license agreements before registering on the website. All these findings endorse that teenagers do adopt general caution since they are very clear and concerned about privacy policies and their rights regarding the same.

Table 5: Privacy related Behaviour (Technical Protection)

TECHNICAL PROTECTION	Alternatives	Frequency	Percent
Do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in or opt-out of certain offers)?	Always	11	5.98
	Often	129	70.11
	Rarely	6	3.26
	Sometimes	38	20.65
Do you remove cookies?	Always	41	22.28
	Often	110	59.78
	Rarely	5	2.72
	Sometimes	28	15.22
Do you use a pop up window blocker?	Always	26	14.13
	Never	2	1.09
	Often	124	67.39
	Rarely	2	1.09

	Sometimes	30	16.30
Do you check your computer for spyware?	Always	35	19.02
	Often	116	63.04
	Rarely	3	1.63
	Sometimes	30	16.30
Do you clear your browser history regularly?	Always	30	16.30
	Often	125	67.93
	Rarely	1	0.54
	Sometimes	28	15.22
Do you block messages/emails from someone you do not want to hear from?	Always	15	8.15
	Never	1	0.54
	Often	131	71.20
	Rarely	1	0.54
	Sometimes	36	19.57

Regarding technical protection, majority of the teenagers i.e., 129 respondents (around 70.11 %) quite often are looking for ways (such as check boxes that allow them to opt-in or opt-out of certain offers) to control what is sent to them. Further, 110 respondents (59.78%) quite often remove cookies. However, only 26 respondents (14.13%) use a pop-up window blocker. More than 63.04% of respondents (116) check spyware. 125 respondents (67.93%) regularly remove their browsing history. Overall, it can be concluded that teenagers are aware of and do apply proper preventive measures and / or get involved in protective behaviour.

6. KEY HIGHLIGHTS:

This study offers valuable insights into the online privacy behaviors of teenagers, particularly focusing on their browsing habits, concerns about privacy, and the defensive strategies they employ. Key findings from the study shed light on the complex and sometimes contradictory relationship teenagers have with their personal information and online privacy.

• Teenagers' Awareness and Concerns About Privacy:

Teenagers are quite aware of online privacy issues, including the importance of safeguarding personal information. They exhibit a strong understanding of their privacy rights and the associated risks.

The study finds that they are well-versed in consumer protection laws, such as the Consumer Dispute Redressal Commission and Consumer Protection Act, indicating a higher level of technical literacy regarding their digital rights.

• Privacy vs. Behavior Discrepancy:

Although teenagers express a strong concern for their online privacy, their actual behavior sometimes contradicts these concerns. For example, they often share false or fabricated information when they encounter registration forms on websites, especially if they feel that withholding information is not an option.

This presents an interesting dynamic where teenagers may be cautious about their privacy yet still engage in behaviors that could compromise it.

• Defensive Measures Adopted:

Teenagers actively adopt defensive measures to protect their personal data, such as using pseudonyms, avoiding certain websites, or using privacy-focused browser extensions. These precautions reflect their awareness of potential threats and their proactive attitude in managing personal data.

At the same time, their privacy behaviors suggest a balancing act between caution and convenience—choosing defensive measures when it suits them but also compromising their privacy when necessary (e.g., when required to register on websites).

• The Paradox of Concern vs. Permission:

An interesting paradox is that while teenagers express strong concerns about data security, they sometimes grant permission for data collection or share personal information without fully understanding the consequences. This could be attributed to their growing digital literacy but possibly limited experience in recognizing the full extent of privacy risks.

• Psychological and Cognitive Responses:

The study highlights that while teenagers may express strong cognitive concern about privacy, their actual online behaviors do not always align with those concerns. This suggests a gap between their theoretical understanding of privacy risks and their practical actions in navigating the digital space.

7. CONCLUSION:

This study emphasizes that while teenagers in Jaipur district, Rajasthan, demonstrate a commendable understanding of privacy concerns and protective measures, their behaviors reveal a complex interplay between concern, convenience, and digital literacy. The findings suggest that while they are technically savvy and aware of their rights, they are still navigating the balance between online privacy protection and the need to share personal data for various digital interactions. This research offers a deeper understanding of the contradictions inherent in the privacy behaviors of today's younger generation and suggests that privacy education may need to address both cognitive understanding and practical application to be truly effective.

References:

1. Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing*, *31*(2), 96-110.
2. Anatoliy Gruzd, and A´ ngel Herna´ndez-Garcı´a, (2018). Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media
3. Anic, I. D., Škare, V., & Milaković, I. K. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. Electronic Commerce Research and Applications, 36, 100868.
4. Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. IEEE Security & Privacy, 8(1), 21-27.
5. Bandara, R., Fernando, M., & Akter, S. (2020). Privacy concerns in E-commerce: A taxonomy and a future research agenda. Electronic Markets, 30(3), 629-647.
6. Barkhuus, L., & Dey, A. K. (2003, July). Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In Interact (Vol. 3, pp. 702-712).
7. Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics*, *34*(7), 1038-1058.
8. Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26-53.
9. Chung, W., & Paynter, J. (2002, January). Privacy issues on the Internet. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 9-pp). IEEE.
10. Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 50, 261-272.
11. Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7-29.
12. Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. American Economic Review, 102(3), 349-353.
13. Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Mis Quarterly*, 275-298.
14. Ischen, C., Araujo, T., Voorveld, H., van Noort, G., & Smit, E. (2020). Privacy concerns in chatbot interactions. In *Chatbot Research and Design: Third International Workshop, Conversations 2019, Amsterdam, The Netherlands, November 19–20, 2019, Revised Selected Papers 3* (pp. 34-48). Springer International Publishing.
15. Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, *24*(3), 579-595.
16. Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*, 106260.
17. Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*, 39-63.
18. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11).
19. Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for information systems*, *28*(1), 28.
20. Lina, L. F., & Setiyanto, A. (2021). Privacy concerns in personalized advertising effectiveness on social media. Sriwijaya International Journal Of Dynamic Economics And Business, 5(2), 147-156.
21. Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. Information, Communication & Society, 21(10), 1472-1492.
22. Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science, 35, 572-585.
23. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research, 15(4), 336-355.
24. Nowak, G. J., & Phelps, J. E. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. Journal of Direct Marketing, 6(4), 28-39.
25. Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of advertising*, *38*(4), 63-77.
26. Omotayo, F. O. O., & Olayiwola, J. O. (2023). Privacy and Security Information Awareness and Disclosure of Private Information by Users of Online Social Media in the Ibadan Metropolis, Nigeria. *The African Journal of Information Systems*, *15*(1), 3.

Webliography:

1) www.privacylaws.com
2) www.trai.gov.in/content/mpci.aspx
3) www.mit.gov.in/context/information-technology-act
4) www.privacylaws.com