IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

A Study on Privacy Risks and User Control in the Use of Cookies on the Internet

Sri Subashini. K[1] and Nishitha. V[2]
B.A., LL.B (Hons.)[1]
BBA LLB (Hons.)[2]
Saveetha School of Law, Saveetha Institute of Medical and Technical Science (SIMATS), Chennai

Abstract: *Cookies are small text files that are widely used on the internet to enhance the user experience by keeping track of preferences and providing personalized content and advertising. However, the use of cookies raises significant privacy concerns. Some of the problems with cookies in internet privacy include tracking, security, invasion of privacy, consent, and user control. Users often have limited control over cookies, and it can be challenging to delete them or prevent them from being used. So, it is essential for users to be aware of the risks and take steps to protect their privacy, such as using privacy-focused browsers and extensions, clearing cookies regularly, and being cautious about the information they share online. The major objective of the study is to explore the problems associated with the use of cookies in internet privacy and the extent to which users have control over their data. The research design followed here is empirical research. A total of 216 samples were collected through a convenient sampling method. The sample frame taken here is from cities like Trichy, Chennai, Madurai, Pondicherry, Dindigul, Coimbatore and Thanjavur through online surveys. Dependent variables here are gender, educational qualification, occupation and locality. Independent variables here are the most significant privacy risks associated with their use, current legal frameworks around the use of cookies, and how effective they are in protecting user privacy. The statistical tool used here is clustered bar graph and chi-square test. The findings of the study suggest that cookies pose significant privacy risks, and users have limited control over their data. To address these problems, it is important to increase awareness of the risks associated with cookies and to provide users with clear and accessible options for controlling their use.*

Keywords: Cookies, privacy, internet, data storage and tracking

I. INTRODUCTION

The history of cookies dates back to the early days of the internet in the 1990s. Cookies are small text files that are placed on a user's device by a website. They are designed to store user data, such as login credentials, website preferences, and shopping cart items, and to help websites remember users from visit to visit. The first web browser to support cookies was Netscape Navigator, which introduced them in 1994. The original purpose of cookies was to enable online shopping carts to function properly, as they allowed websites to keep track of what items users had added to their carts. Over time, cookies became more sophisticated and began to be used for a wider range of purposes. Advertisers began using cookies to track users' browsing history and display targeted ads. Website owners used cookies to gather data about their visitors, such as which pages they viewed and how long they spent on the site. As the use of cookies became more widespread, concerns began to arise about their impact on user privacy. In response, governments and industry groups around the world began to develop regulations and guidelines for the use of cookies. Today, cookies continue to play a central role in the functioning of the internet. While their use remains controversial, they are an essential part of many websites' functionality and are likely to remain so for the foreseeable future.

In India, there is currently no specific law or regulation that directly addresses the use of cookies for internet privacy. However, there have been some steps taken by the government to address broader privacy concerns related to the collection and use of personal data. Personal Data Protection Bill, 2019: The Personal Data Protection Bill 2019,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 9, June 2025 Impact Factor: 7.67

Guidelines on Privacy and Confidentiality of Information in Telecom Networks, 2017, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are some of the legislations that provide some protections for users.

In recent years, there has been a growing trend towards stricter regulations and increased user control over cookies and internet privacy. Here are a few notable developments: Increased browser control, Regulations on cookie consent, Focus on data privacy and Impact on digital advertising.

II. REVIEW OF LITERATURE

Acquisti (2007), This paper discusses how individuals make decisions about privacy in online contexts, and the role that rationality plays in these decisions. The authors explore the ways in which individuals make trade-offs between privacy and convenience, and suggest that understanding the factors that influence these trade-offs can help to improve privacy decision-making.

Balebako (2012), This paper discusses the design and implementation of user controls for privacy management on social media platforms. The authors analyze the privacy settings of several popular social media sites and propose a set of design principles for effective privacy controls. They also describe the results of a study in which users were asked to evaluate different privacy control designs.

Castelluccia (2014), This paper highlights the privacy risks associated with data management systems and proposes the development of privacy-aware data management systems as a solution. The authors discuss the challenges involved in developing such systems, including the need to balance privacy with data utility, and suggest several research directions for future work in this area.

Cranor (2012), This paper discusses the limitations of current privacy notice and choice mechanisms, and proposes the development of standardized mechanisms to improve their effectiveness. The author argues that the current system of privacy notices and controls is often too complex for users to understand, and suggests that a more standardized approach could help to simplify the process and make it more effective.

Debatin (2009), This paper examines the attitudes and behaviors of Facebook users with regard to privacy, and the unintended consequences of Facebook's privacy policies. The authors describe the results of a survey of Facebook users, and discuss the implications of these results for privacy management on social media sites.

Eckersley (2010), This paper examines the extent to which web browsers can be used to uniquely identify individual users, even in the absence of cookies. The author describes several browser fingerprinting techniques and analyzes the extent to which they can be used to identify users. The paper also discusses the privacy implications of browser fingerprinting and suggests several possible solutions.

Grannis (2011), This paper presents an empirical analysis of the effectiveness of industry self-regulation in the United States in protecting user privacy online. The authors examine the use of cookies, a widely used technology that allows websites to track users, and analyze the effectiveness of the self-regulatory efforts in the online advertising industry. The study finds that while self-regulation has led to improvements in cookie control mechanisms, it has not been sufficient to adequately protect user privacy. The authors conclude that a more comprehensive approach to privacy regulation is needed.

Hengartner (2012), This paper investigates the privacy risks associated with the storage of web browsing history by web browsers. The authors analyze the browsing history collected by popular web browsers and demonstrate that it can reveal sensitive information about users, including their political views, health status, and financial transactions. The study also evaluates the effectiveness of various privacy protection techniques, including clearing browsing history and using private browsing modes. The authors conclude that these techniques are insufficient to protect user privacy and call for the development of new privacy-preserving browsing technologies.

Hoofnagle (2010), This paper examines the differences in attitudes and behaviors related to information privacy between young and older adults. The authors conduct a survey of adults in the United States and find that younger adults are more likely to share personal information online and less likely to take steps to protect their privacy. The study also shows that older adults have a greater understanding of privacy risks and are more likely to take steps to

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

protect their privacy. The authors conclude that age is an important factor to consider when designing privacy policies and technologies.

Jansen (2014), This study examines the privacy paradox, where individuals express concerns about privacy on social network sites (SNSs) but still engage in behaviors that compromise their privacy. The authors investigate the role of individual characteristics (such as privacy concerns, self-disclosure, and risk-taking propensity) and group norms (such as attitudes towards privacy) in explaining this phenomenon. Results suggest that individual characteristics and group norms both play a significant role in shaping privacy attitudes and behaviors on SNSs.

OBJECTIVES

- To calculate the awareness about the issues that could be raised due to cookie provision on the Internet.
- To evaluate the most significant privacy risks associated with the use of cookies
- To find out the Effectiveness of the current legal framework of India to control cookies.

III. METHODOLOGY

The research conducted is Non-doctrinal research and the research design followed is empirical method. A total of 216 samples were collected through a convenient sampling method. The sample frame taken here is from cities like Trichy, Chennai, Madurai, Pondicherry, Dindigul, Coimbatore and Thanjavur through online surveys. The dependent variables here are gender, educational qualification, occupation and locality. Independent variables are the most significant privacy risks associated with their use, current legal frameworks around the use of cookies, need of International laws and how effective will be the 2019 bill in protecting user privacy. The statistical tool used here is clustered bar graph and chi-square test.

HYPOTHESIS

Null Hypothesis:-

There is no significant relationship between occupation of the respondents and the privacy risk associated with the use of cookies.

There is no significant relationship between the educational qualification and the implementation of Personal Data Protection Bill 2019 for protecting the privacy of users.

Alternative Hypothesis:-

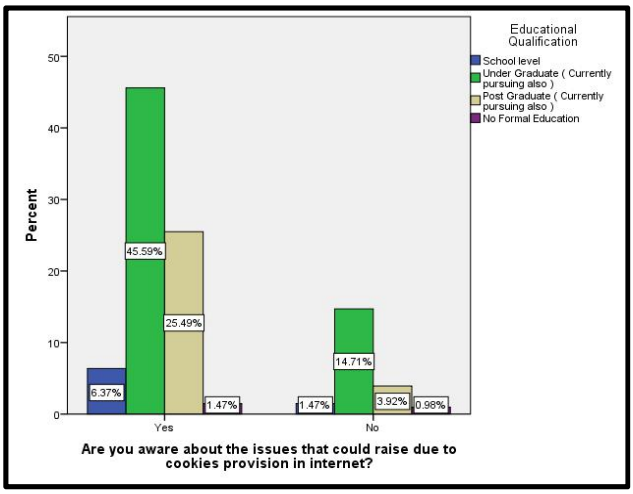
There is a significant relationship between occupation of the respondents and the privacy risk associated with the use of cookies.

There is a significant relationship between the educational qualification and the implementation of Personal Data Protection Bill 2019 for protecting the privacy of users.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

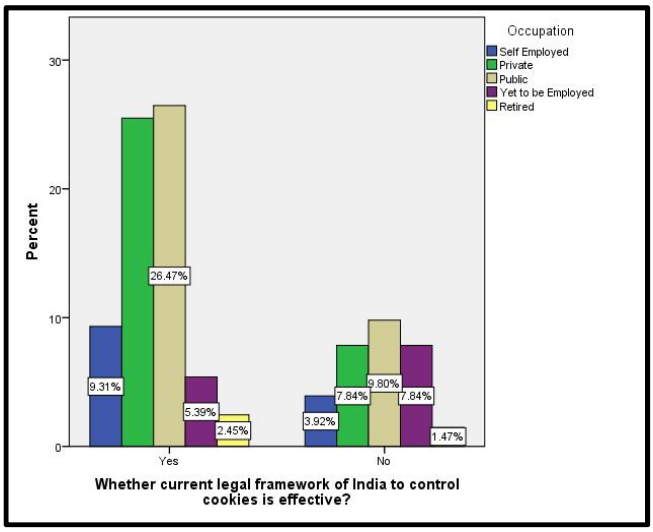
IV. ANALYSIS

Figure 1



Legend:- Fig. 1 represents the Educational distribution of sample population and Awareness about the issues that could be raised due to cookies provision in the Internet.

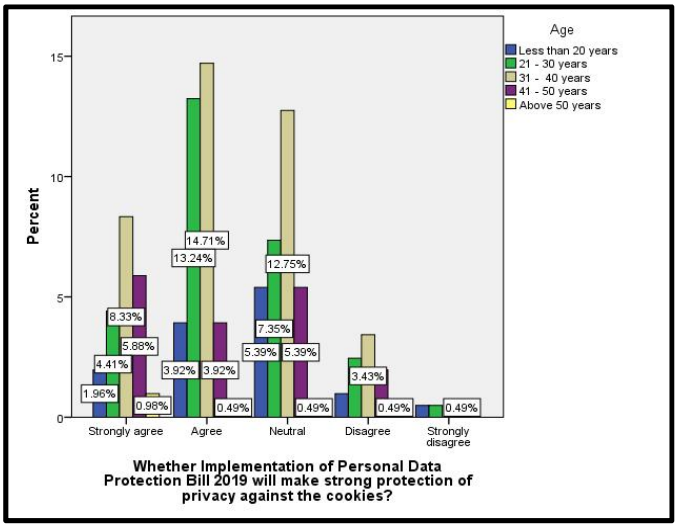
Figure 2



Legend:- Fig. 2 represents the Occupational distribution of sample population and Effectiveness of current legal framework of India to control cookies.

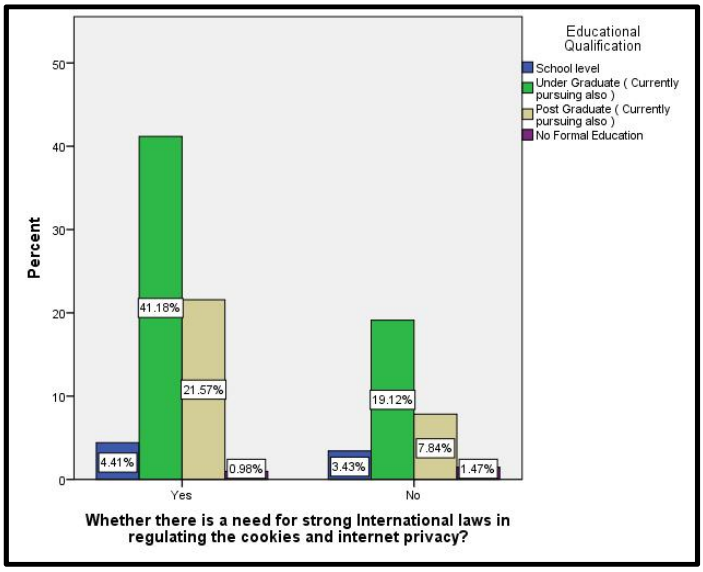
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure 3



Legend:- Fig. 3 represents the Age distribution of sample population and Agreeability about the Implementation of Personal Data Protection Bill 2019 will make a strong protection of privacy against the cookies.

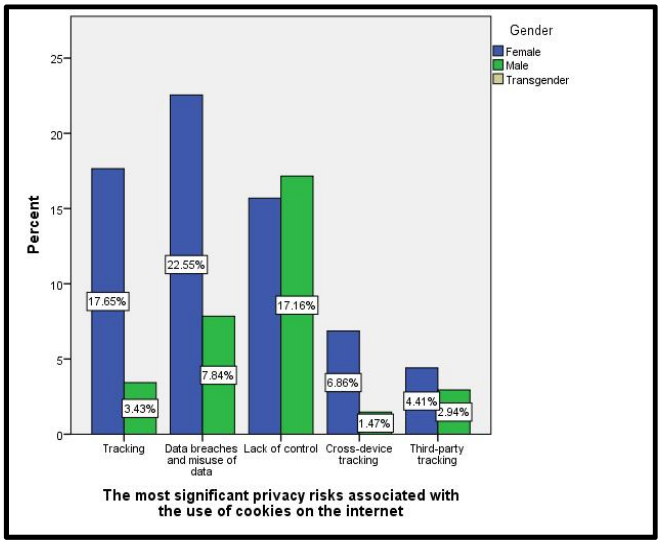
Figure 4



Legend:- Fig. 4 represents the Educational distribution of sample population and need for a strong international laws in regulating the cookies and internet privacy

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Figure 5



Legend:- Fig. 5 represents the Gender distribution of sample population and most significant privacy risks associated with the use of cookies on the internet.

Chi-square test:

Table 1

Occupation * The most significant privacy risks associated with the use of cookies on the internet Crosstabulation

Count

		The most significant privacy risks associated with the use of cookies on the internet					
		Tracking	Data breaches and misuse of data	Lack of control	Cross-device tracking	Third-party tracking	Total
Occupation	Self Employed	7	7	9	2	2	27
	Private	14	18	23	7	6	68
	Public	9	29	28	4	4	74
	Yet to be Employed	10	5	5	4	3	27
	Retired	3	3	2	0	0	8
Total		43	62	67	17	15	204

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	18.416[a]	16	.300
Likelihood Ratio	19.509	16	.243
Linear-by-Linear Association	.869	1	.351
N of Valid Cases	204		

a. 9 cells (36.0%) have expected count less than 5. The minimum expected count is .59.

INTERPRETATION:-The calculated p value is 0.300. Since p value is >0.05, null hypothesis is accepted. So there is no significant relationship between occupation of the respondents and the privacy risk associated with the use of cookies.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Table 2

Educational Qualification * Whether Implementation of Personal Data Protection Bill 2019 will make strong protection of privacy against the cookies? Crosstabulation

Count

		Whether Implementation of Personal Data Protection Bill 2019 will make strong protection of privacy against the cookies?					
		Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total
Educational Qualification	School level	6	4	5	1	0	16
	Under Graduate (Currently pursuing also)	16	51	42	13	1	123
	Post Graduate (Currently pursuing also)	20	18	16	4	2	60
	No Formal Education	2	1	1	1	0	5
Total		44	74	64	19	3	204

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	17.641[a]	12	.127
Likelihood Ratio	17.378	12	.136
Linear-by-Linear Association	.596	1	.440
N of Valid Cases	204		

a. 10 cells (50.0%) have expected count less than 5. The minimum expected count is .07.

INTERPRETATION:-The calculated p value is 0.127. Since p value is >0.05, null hypothesis is accepted. So there is no significant relationship between the educational qualification and the implementation of Personal Data Protection Bill 2019 for protecting the privacy of users.

V. RESULTS

Fig.1: It is evident that the majority of the respondents were undergraduates and they have answered that they were aware about the issues that could be raised due to cookie provision on the Internet. (45.59%), Fig. 2: majority of the respondents were working in public sectors and they have stated that they were aware about current legal framework of India to control cookies are effective (26.47%), Fig. 3: majority of the respondents were belonged to Age category of 31-40 years and they were aware about Implementation of Personal Data Protection Bill 2019 will make a strong protection of privacy against the cookies(14.71%),Fig. 4: it is clear that majority of the respondents were and they have answered that there is a need for a strong international laws in regulating the cookies and internet privacy (14.18%), Fig. 5: majority of them were females and they have answered that Data breaches and misuse of data are the most significant privacy risks associated with the use of cookies on the internet (22.55%).

VI. DISCUSSIONS

Cookies were introduced to make the internet user-friendly. It was supposed to ease the users to store the shopping carts, history of search etc. But eventually it became a trap for users as it started to interrupt the privacy of the individual. The daily routines and locational moves are even tracked through the cookies. As per the survey conducted people are aware about the presence of cookies option in their internet but not in-depth. Females face the most common issues such tracking, misuse of data and breach of data. But Males found that lack of control over the internet as a major issue. In spite of these they also believe that the present legislations in India are sufficient to combat the issues that could arise out of cookies. Because they are not aware of what could be done in regard. Furthermore, the Internet is a global service which has to be under the control of the International Laws but has to be governed and regulated by the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

domestic laws. So there is an immense need for strong International Laws that has to be ratified by every state. From the survey it can be concluded that the people are not ready to take steps individually to protect themselves from the internet privacy issues. They are always prepared to blame the government and laws for the problems that occurred and damage suffered. They wanted many domestic and International laws and authorities to prevent and ensure protection to internet users from the violation of privacy rights by the third parties or the online platform providers such as Google, Amazon, WhatsApp, etc.,

VII. LIMITATION

One of the major limitations of the study is the study frame as it was restricted only within Tamil Nadu and Pondicherry. In addition the datas are collected through a convenient sampling method where a large population is not covered.

VIII. SUGGESTION

Here are some suggestions for individuals to protect themselves against cookies:

- **Use browser privacy settings:** Most web browsers allow users to control cookies through their privacy settings. Users can choose to block or restrict cookies from specific websites, or to delete cookies automatically when they close their browser.
- **Install ad-blockers:** Ad-blockers are browser extensions that can block ads and prevent websites from tracking your online behavior using cookies.
- **Use cookie management tools:** There are several tools available that allow users to manage their cookies more easily. These tools can help users delete cookies, view their cookie history, and control which cookies are allowed on their device.
- **Use private browsing mode:** Private browsing mode, also known as incognito mode, can prevent cookies from being stored on your device. However, it's important to note that private browsing does not provide complete privacy and may not protect you from all forms of tracking.
- **Be cautious with personal information:** Be careful about sharing personal information online, particularly on websites that you don't trust. Avoid entering personal information such as your name, address, and email address on websites that you are not familiar with.
- **Keep software up to date:** Keep your web browser and operating system up to date with the latest security patches and updates. This can help prevent security vulnerabilities that could be exploited by malicious cookies or other forms of malware.

Remember that while these suggestions can help protect your privacy online, they may not provide complete protection against all forms of tracking and data collection. It's important to stay informed about new threats and vulnerabilities and to take steps to protect yourself accordingly.

IX. CONCLUSION

Cookies can have significant effects on users' internet privacy. While cookies can provide useful features for website personalization and advertising, they can also be used to track users' online behavior and collect personal information without their consent. This can lead to privacy violations, identity theft, and other forms of online harm. Effective legal frameworks and regulations are needed to protect users' privacy online, particularly in the absence of clear standards for cookie usage. Governments around the world have taken steps to address these issues, including implementing regulations like the GDPR and CCPA. However, there is still much work to be done to ensure that users are fully informed about how their data is being collected and used, and that they have control over their online privacy. Individuals can also take steps to protect themselves against cookies, including using privacy settings, ad-blockers, and cookie management tools. However, these measures may not provide complete protection, and it is important for users to remain vigilant and informed about online privacy threats. Overall, further research and action are needed to address

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

the complex issues surrounding cookies and internet privacy. By working together, we can help ensure that users' privacy is protected and that the internet remains a safe and secure place for all.

REFERENCES

[1]. Acquisti, A., & Grossklags, J. (2007). Privacy and rationality in individual decision making. IEEE Security & Privacy, 5(3), 24-30.

[2]. Balebako, R., Jung, J., & Cranor, L. F. (2012). Policing privacy: User controls for privacy management on social media. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 94-105).

[3]. Castelluccia, C., & Narayanan, A. (2014). Privacy risks and the need for privacy-aware data management systems. In Proceedings of the 2014 ACM SIGMOD international conference on Management of data (pp. 1143-1144).

[4]. Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. IEEE Security & Privacy, 10(2), 68-71.

[5]. Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83-108.

[6]. Eckersley, P. (2010). How unique is your web browser? In Proceedings of the 2010 conference on Privacy Enhancing Technologies (pp. 1-18).

[7]. Grannis, A., & Cox, L. (2011). Cookie control mechanisms in US privacy regulation: An empirical analysis of the effects of industry self-regulation. International Journal of Communication, 5, 710-732.

[8]. Hengartner, U., Steiner, M., & Tsudik, G. (2012). On the privacy of web browsing history. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 171-182).

[9]. Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? Berkeley Center for Law & Technology Research Paper, (2010-16).

[10]. Jansen, B. J., & Molina, J. (2014). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. International Journal of Human-Computer Studies, 72(10), 717-727