International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

Consumer Perceptions of Cookies and Personalised Advertising: An Analysis of Awareness, Acceptance, and Behavioural Responses

Nikhil Ganesh

Neev Academy

DOI: 10.46609/IJSSER.2025.v10i10.066 URL: https://doi.org/10.46609/IJSSER.2025.v10i10.066

Received: 7 October 2025 / Accepted: 22 October 2025 / Published: 3 November 2025

ABSTRACT

Consumer perceptions of cookies and targeted advertising have posed some serious concerns about awareness, which in turn have economic implications. The dominant research conducted prior explores the safety and privacy concerns cookies can pose, therefore having significant impacts on users on websites. Further research also explores the economic implications of poor cybersecurity systems and privacy frameworks. This research explores cookies through the viewpoint of consumer perceptions and how they have an impact on our daily lives at a more micro level. Through the analysis which used a survey distributed to a community of respondents of various age groups aged 18 and above and graphical representations created from the data collected, the study found that a majority accept cookies while knowing the implications. Results exhibit that while 53.8% of participants accept cookies, 97.4% have experienced targeted advertisements, regardless of whether they consented to cookies. Moreover, 66.7% of respondents refuse to accept cookies even when the purpose is disclosed, highlighting a growing skepticism and awareness of privacy concerns. Hence, a relation was found between acceptance of cookies and targeted advertising. This can be attributed to cognitive biases such as the status quo bias. It was concluded that accepting cookies can result in increased privacy concerns and possibilities of data being leaked which in turn can have a grave economical impact.

Keywords: Cookies, Targeted Advertisements, Users, Consumers, Data Privacy, Security, Behaviour

1. Introduction

1.1. General Background

In the 21st century, websites, apps, and digital services have become increasingly ingrained in the daily lives of individuals. The online ecosystem is growing at a increasingly rapid rate in the

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

digital era. With the plethora of digital tools and technologies available to improve business performance and user experience, such as pop-ups and cookies, it has become imperitive to understand consumer and user attitudes [1]. Cookies are small files saved on users' devices that help track and retain user behavior, including preferences, search history, and login credentials [2, 3]. Similarly, pop-ups are visual pages that generally ask for permissions, like enabling notifications, accepting cookies, or signing up for newsletters.

Cookies have a plethora of purposes. They are used to personalise content, enable targeted advertising and marketing by looking at the interests of consumers who access those websites. This allows websites to collect data points to make their websites perform better [2]. Targeted advertising is a data-driven marketing technique in which ads are directed towards specific groups of people who share common traits, behaviors, or interests. Research defines targeted advertising as the practice of delivering customised promotional messages to audience segments identified by demographic, psychographic, or behavioural data [4]. Generally, these functions claim to support a user's experience on the internet; however, such tools can pose serious concerns regarding digital privacy and digital security. Consequently, they can have economic implications as well.

The growing dependence on cookies and other technologies has created a debate on data security and its economic implications. High-profile data breaches have an immense economic impact while also making users more conscious of how their data is being used [5]. In response to these issues, Governments across the world are introducing policies to enforce data security. For example, the European Union's "General Data Protection Regulation" (GDPR) and "India's Digital Personal Data Protection" (DPDP) Bill, which prioritise data security and give control to the user over their data instead of the corporation, yet even with laws like these pushing for transparency [5]. Businesses continue to use targeted advertising for marketing, which is based on user data and profiles.

Even though such policies exist, there is a major awareness gap between consumers and firms over cookies and their implications. Most users accept all cookies without understanding their implications, a phenomenon coined as "consent fatigue". The repetitive nature of these requests and the complex language and designs used make users prioritise convenience over privacy [6]; this can also be inferred as the Status quo bias in behavioural economics.

1.2. Literature review

The association between cookies, targeted advertisements, and data security has been widely explored in the literature. In Pierson and Heyman (2011) [7], the research delves into how cookies and other tools are part of a new wave of tools in the new media landscape (social

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

media). Social media has enabled a new type of communication called mass self-communication, which is characterised by communication that can reach a global audience while the content is self-generated. However, while tools like cookies are meant to support this mass self-communication, they create a paradox through privacy issues. The research paper mentions how in online environments and ecosystems, consumers are not completely aware of how their data is being collected and used. In Almotri (2022) [8], the risks associated with cookies are explored through an experiment. A total of 471 participants were asked to answer 34 questions, including one that made users access an experimental website for the study. Through the above data, the research concluded that while 77% of participants were aware of the dangers associated with cookies, a majority frequently accepted cookies. Hence, this showed that even after knowing the limitations of cookies, users are accepting them on a regular basis.

According to Anderson and Moore (2006) [9], information security is not a technical problem based on computers and data, but rather an economic one. Data breaches and failures in information security, for example the 2013 Cambridge Analytica incident, where Facebook users' personal information was leaked, highlight this issue. However, this paper will not focus on the security aspect of data protection but instead explore how data holds immense value in the modern era, particularly through social media and everyday tools like Google. This paper is not directed towards the security aspect of data security; rather, it will look at data as a tool for advertising and predictive tools. In Anderson and Moore(2006) [9], the idea of misaligned incentives is built upon substantially. Security failures don't occur because of technical issues; rather, the incentives are not aligned to ensure the data is safe. An example given is when those responsible for the security of your data are not the ones suffering when the data is leaked. This concept helps us understand why social media companies value our data but are not impacted greatly if that data is leaked. In the case of Cambridge Analytica, while Facebook was expected to be fined 5 billion dollars, they only paid 500,000 dollars, yet millions of users' personal information was leaked.

In Goldfarb and Que (2022) [10], the idea of misaligned incentives is further explored, however, from a different perspective, looking at the cost-benefit trade-offs that a company has to make for consumer privacy or better market analytics and predictive data. These tradeoffs are for data flows, wherein the paper argues that using data from consumers can help consumers receive better products, data-driven innovation, and products at a much lower cost, therefore improving consumer welfare. For a firm, the use of data flows leads to more profits, better targeted advertising, and the potential to explore new markets; however, the costs are also considered. One of the costs is the intrinsic value of data and privacy. There is no set value assigned to privacy and data, and each consumer may view it differently. Authors also explore externalities related to data flows, calling the release of data a negative externality as one person's data could

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

lead to another person's data being revealed, directly or indirectly, through correlation of behaviour and habits or directly via contact lists. The externality is cited as the excessive collection of personal information by firms.

In Sonkar (2025) [11], the exploration of the economic impact is further delved into via the perspective of small and medium sized enterprises (SME's), The research argues that SME's with better cybersecurity policies and technology are significantly more resilient to cyber threats, therefore eliminating the risk involved with cyber threats and hence reducing the economic impact associated with that. Further, this was proven using a quantitative analysis. The study used regression analysis and hypothesis testing, which returned a R^2 value of 0.729, indicating a strong correlation between cybersecurity measures and economic resilience to such attacks. In Wirth (2017) [12], the research delves into another aspect of economics and security, which was not explored in the previous papers. He coined the term malware production, cyber fraud, as part of an underground economy. This economy consists of many cybercrime organisations operating as businesses, offering services related to cybercrime. The study comments that this economy is growing as the world has experienced a growing production of malware. In 2008, 1 million viruses were produced annually, whereas in 2016, that number had increased to 1 million a day. In a report by the World Bank [13], another research explores cybersecurity as a systemic issue and something that needs to be addressed urgently, especially for developing countries. The report states that countries that invest in strong cybersecurity infrastructure can experience a 1.5% growth in GDP. It comments that cyberbreach is a systemic problem that has ramifications across all levels of the economy.

Therefore, it can be argued that from the literature that the mere use and acceptance of cookies can lead to multiple risks. It can result in unintended targeted advertisements and other consequences, including cyber attacks. Furthermore, these consequences can also affect the economic growth and resilience. Hence, from a micro lens, this study assesses the perceptions of users regarding cookies and targeted advertisements.

1.3. Literature Gap and Rationale of the Study

Despite valuable results, there are several gaps in the existing papers. This literature, however, does not consider the perception of users with regard to cookies and target advertisements. Furthermore, the concept of behavioural economics could be brought in with more detail, and emphasis on traditional economics is displayed and enforced. However, behavioural economics, such as nudge theory and the cognitive biases, can be brought in to understand how business manipulate their web pages to convince consumers to accept cookies and other data-driven tools

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

This study is necessary since cookies and targeted advertisements have become essential parts of companies' marketing strategies and our lives. Many of the purchases are influenced by this advertising method, even though it remained unnoticed. Companies can reach large and specific audiences quickly for their products, resulting in a higher conversion rate. Cookies pose significant privacy risks due to their nature. Understanding the economics of cookies and targeted advertisements and their cybersecurity risks can improve user awareness and potentially make them more conscious of their online presence. Hence, this study aims to understand the economics behind cookies and targeted advertisements, with a focus on their cybersecurity risks and subsequent impacts.

2. Methodology

2.1. Research Aim & Objectives

This research investigates the “behaviour and perceptions of consumers/users with regards to cookies and targeted advertising". For the analysis of the same, this study explored the below given objectives.

- “Assessing the user behaviour towards the acceptance of cookies and awareness regarding the targeted advertising.”
- “Examining the consumers’ willingness of consumers to accept cookies due to purposeful disclosure.”
- “Analysing the association between acceptance of cookies and exposure to targeted advertisements.”
- “Evaluating the behaviour of users related to cookies and targeted ads among those individuals who reject or conditionally accept cookies.”

2.2. Data Collection Tool and Process

This research uses a structured questionnaire to gather the primary cross-sectional data. The questions that were asked from the respondents were kept concise, clear, and easily understandable, emphasising on collecting the perception of users towards cookies and targeted advertisements. For the data collection procedure, a convenience sampling method was used which involves the random distribution of the survey to local and known respondents within the community. The data for 40 volunteer consumers from Delhi is used for the analysis. These respondents were adults of age 18 years and above. Other demographic information has not been collected to ensure anonymity.

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

2.3. Data Analysis Method

The data that has been collected from the survey is analysed using the visualisation method. The responses were graphically represented through pie charts. Pie charts were created to show the patterns and distribution of responses in an easier manner. With the help of pie charts, percentage distributions were also evaluated and justified to compare the responses in different groups.

2.4. Ethical Considerations

Ethical considerations were effectively addressed throughout the research process. The study maintained ethics in regards to confidentiality, anonymity, and informed consent. The personally identifiable details of the respondents, such as their names, contact details, address, and other demographics, were not questioned in the survey. In addition, all responses were stored in a secure environment, with the researcher being the only one authorised to access them for analysis. Therefore, the data collected was used only for research purposes and not by any third party. In the end, participants were informed of the study's purpose, their voluntary participation, and the choice to withdraw at any time without penalty.

3. Results & Discussion

Figure 1: "Pie chart showing the percentage of respondents who accept cookies"

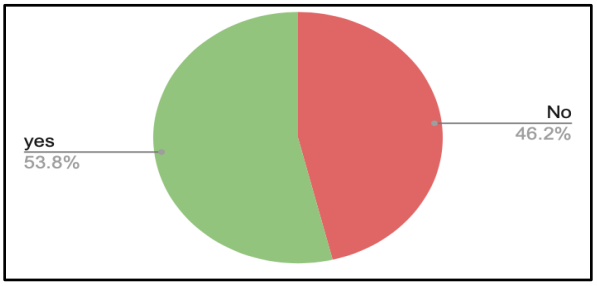
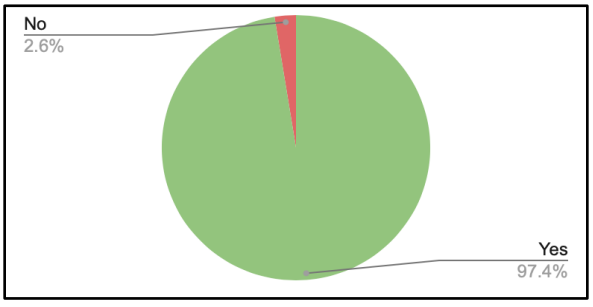


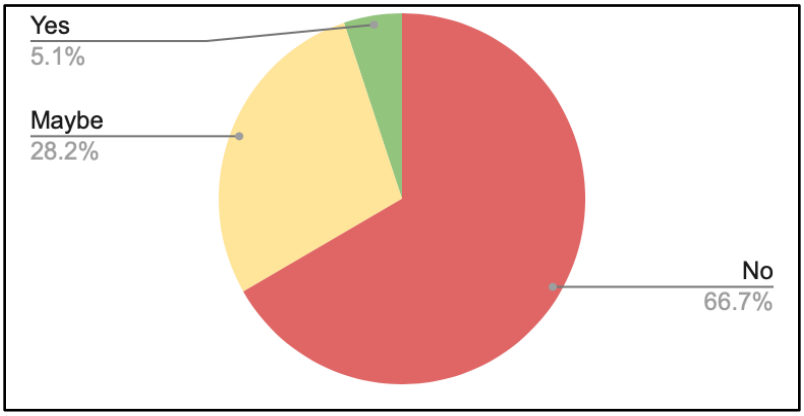
Figure 2: "Pie chart showing the percentage of respondents who have experienced targeted advertising"



ISSN: 2455-8834

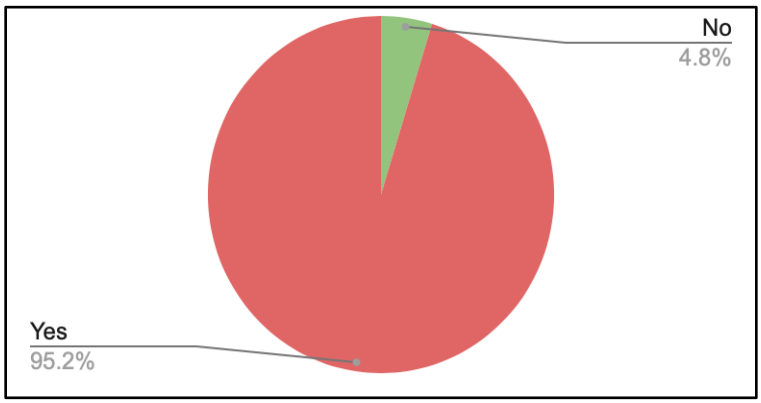
Volume:10, Issue:10 "October 2025"

Figure 3: "Pie chart showing the percentage of respondents who will accept cookies only if the purpose is disclosed"



The above graphs in Figures 1, 2, and 3 depict the overall percentages of participants regarding cookie acceptance and targeted advertisement. Moreover, results for a hypothetical question as to whether consumers would accept cookies for pre-disclosed purposes, such as marketing, have been shown. It can be seen in Figure 1 that out of the 40 people who responded to the survey, 53.8% accepted cookies, while 46.2% did not. Additionally, Figure 2 represents the distribution of respondents who have experienced targeted advertisements irrespective of accepting cookies. Out of all the respondents, 97.4 percent have experienced personalised ads. Lastly, from Figure 3, it is shown that 66.7 percent of the individuals do not accept cookies if the purpose is disclosed, 5.1 percent will accept, while 28.2 percent may accept depending on the purpose. To further evaluate the data, the responses were categorised into two groups based on cookie acceptance: those who accept cookies and those who do not.

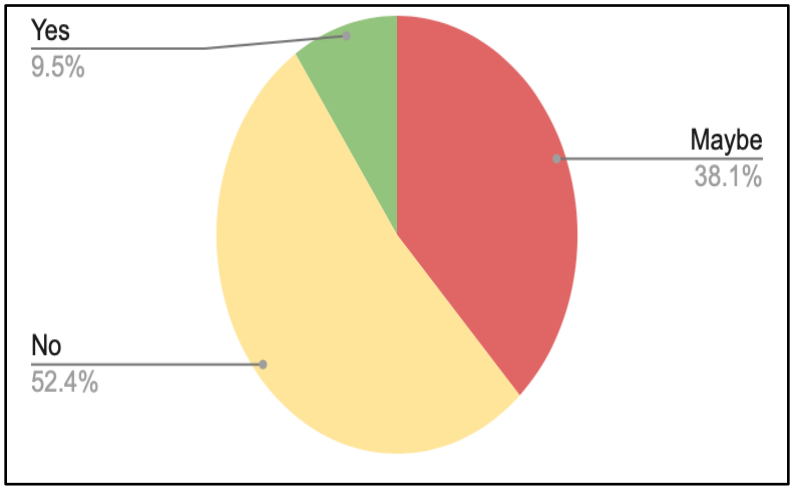
Figure 4: "Pie chart showing the percentage of respondents who accept cookies and have experienced targeted advertising"



ISSN: 2455-8834

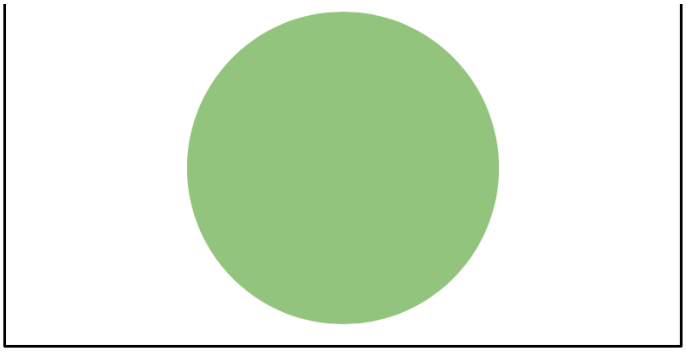
Volume:10, Issue:10 "October 2025"

Figure 5: "Pie chart showing the percentage of respondents who actually accept cookies only if the purpose is disclosed"



Figures 4 and 5 represent the perception of those participants who accept cookies. Of the people who accepted cookies, over 95.2% have experienced targeted advertising, showing a link between accepting cookies and receiving targeted advertising. Furthermore, from Figure 5, it is noted that only 9.5% of people were willing to accept cookies if the purpose was disclosed; however, it is important to consider that there were over 38% of respondents said maybe to the question. Hence, purpose disclosure might not play a role in accepting cookies for this group. In fact, these individuals might reject cookies if the purpose is disclosed. Finally, a direct link between accepting cookies and receiving targeted advertising cannot be definitively established, as other factors may influence ad exposure, including the use of different online services, acceptance of terms unrelated to cookies, and the specific websites visited by users. This is also supported by Figure 6.

Figure 6: "Pie chart showing the percentage of respondents who do not accept cookies and have experienced targeted advertising"



ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

Figure 7: "Pie chart showing the percentage of respondents who do not accept cookies but will accept if the purpose is disclosed"

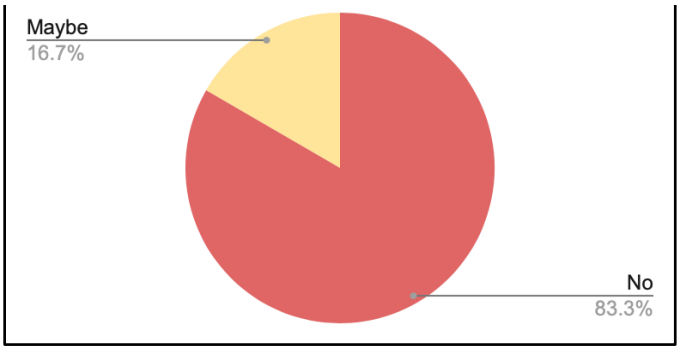


Figure 6 demonstrates the percentage of respondents who do not accept cookies and have experienced targeted advertising. A unique point that came from the population that clicked no is that 100% of respondents have experienced targeted advertising even though they don't accept cookies. Therefore, this can be due to other settings and factors that the users may have enabled, or demographic-related settings and information, such as location. However, it is apparent across all three graphs (Figures 3, 5, and 7) that respondents are hesitant to accept cookies even when the purpose is disclosed. From Figure 7, it is noted that over 83% said no, and 16.7% said maybe, with zero respondents in this section saying yes to accepting cookies even if the purpose is disclosed.

People tend to accept cookies for several major reasons, which can be attributed to behavioural economics and the concept of nudge theory [14]. Apps and websites that use cookies nudge users into accepting them through complex behavioural strategies that understand how human psychology works. For example, the status quo bias, a cognitive bias in which one does not want to change their current state of affairs [15], rather than rejecting cookies, a consumer accepts them since they don't want to read all the options and disable all options, therefore accepting all for convenience and saving time. Moving back to nudge theory, websites design their cookie pages to be extremely complex, for example a websites may have multiple options to disable cookies, they may have multiple sub options based on specific indicators such as who you want the data to get and what data should be tracked, further the accept all button is extremely bright or colourful, therefore "nudging the consumer" to accept all cookies. However, as the above research presented, people can also tend not to accept cookies; this could be because of increased awareness of data security. Users want to keep their data private and secure. Further, this justification could depend on the age demographic. Assuming that the younger respondents were more aware of cookies and their implications, they do not tend to accept them. However, due to the survey being anonymous, this information can't be verified for this research.

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

Another point that was brought up during the research is the increasing presence of targeted advertising. Targeted advertising is defined as promotional content directed at individuals based on their demonstrated interests, demographic characteristics, online behaviours, or stated preferences [3]. These advertisements can be delivered through analysis of browsing data, use of cookies, search queries, and demographic information, which may have been shared with the provider. The primary objective of targeted advertising is to enhance advertising effectiveness by reaching audiences with a higher likelihood of interest in the promoted product or service, instead of distributing it to a wider and more general audience. Targeted advertising is a major tool used in marketing by numerous firms to tap into new customer bases. Further, these advertisements can be based on data that a consumer may not have wanted to share.

4. Conclusion

In conclusion, it is noticed that cookies and pop-ups have become a component in the world of digital tools and techniques. As the usage of the internet increases, cookies and pop-ups are also showing an upward trend. Given that, engaging with them can pose multiple consequences to users as well as the companies. For the companies, cookies can gather users' data and track their behaviour, which in turn helps businesses to gain insights into consumer preferences. On the other hand, users might experience targeted advertisements, data breaches, privacy concerns, and security risks. While targeted advertisements can elevate users' experience through personalisation, they can also result in privacy concerns. Thus, this study aimed to investigate the perceptions and experiences of consumers with regards to cookies and one of their consequences, i.e., targeted advertisements. To evaluate the same, primary data has been collected from 40 respondents through a survey. Using the graphical representations, the results showed that despite knowing the consequences, the majority of the respondents accepted cookies. Moreover, 97.4 percent of the overall participants have experienced targeted advertisements irrespective of cookie acceptance. A high proportion of respondents (66.7%) reject cookies even if the purpose is disclosed, but only slightly (5.1%) will accept them, and 28.2% may agree depending on the reason. Furthermore, most of the participants who accept cookies have experienced targeted advertising, indicating a possible connection; however, purpose disclosure has a nebulous influence on their acceptance. Hence, there is no conclusive evidence that cookie acceptance correlates with targeted ads, as there are other factors that can impact this outcome, such as online behaviour and service usage patterns. Additionally, even users who decline cookies are still able to view targeted ads, suggesting that factors other than cookie acceptance play a role in delivering ads. Despite disclosing the purpose of data collection, respondents exhibit a high level of resistance to accepting cookies. The findings of the survey led to the discussion that cookies are largely accepted due to cognitive biases and behavioural economics such as the status quo biases, complex cookie pages that take time to navigate and other physiological techniques, all

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

designed to make users accept cookies, and nudge theory can be applied here as users are "nudged" to accept cookies using nudges such as colouring the accept button.

5. Policy Implications and Limitations

The results of this research can be used to understand the economic and behavioural aspects of cookies on consumers. Using the behavioural economics principles, it becomes evident how consumers can be induced to accept cookies, often without conscious consent or awareness. Therefore, to ensure the ethical usage of cookies and respect for their privacy, policy measures are required to be undertaken. Enforcing that cookie pages follow a uniform structure to ensure they are not confusing and are designed to nudge people into accepting cookies. The data from cookies can be provided to verified sources and third parties through an online verification created by the government, ensuring data security and privacy.

The limitations of the study are as follows. Various demographics could have been collected and compared in this research, which has limited the results. In addition, the economic value of cookies and personalised ads was not quantified because it entails far too many intricate and dependent variables, which are beyond the study's focus. Nonetheless, in order to fortify the credibility of results, it is suggested to increase the sample size in future studies in order to provide a more accurate and representative analysis.

References

[1] K. Jerath and K. Miller, "Consumers' Perceived Privacy Violations in Online Advertising," *SSRN Electronic Journal*, 2024, doi: https://doi.org/10.2139/ssrn.4736957.

[2] M. Wheeler, S. Saka, and S. Das, "User Perception and Actions Through Risk Analysis Concerning Cookies," Nov. 2022, doi: https://doi.org/10.48550/arXiv.2211.07366

[3] K. LaCroix, Y. L. Loo, and Y. B. Choi, "Cookies and Sessions: A Study of What They Are, How They Work and How They Can Be Stolen," *IEEE Xplore*, Jul. 01, 2017. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8392612 (accessed Oct. 27, 2022).

[4] A. Farahat and M. C. Bailey, "How effective is targeted advertising?," *Proceedings of the 21st international conference on World Wide Web - WWW '12*, 2012, doi: https://doi.org/10.1145/2187836.2187852.

[5] S. Bhagavatula, L. Bauer, and A. Kapadia, "What breach? Measuring online awareness of security incidents by studying real-world browsing behavior," *European Symposium on Usable Security 2021*, Oct. 2021, doi: https://doi.org/10.1145/3481357.3481517.

ISSN: 2455-8834

Volume:10, Issue:10 "October 2025"

[6] W. Jendrzejewska, "The consent fatigue phenomenon on online platforms and its effects on the implementation of the General Data Protection Regulation," *Uj.edu.pl*, Feb. 23, 2025. https://ruj.uj.edu.pl/entities/publication/af672bb2-8edc-4860-a223-8d113d7333c6

[7] J. Pierson and R. Heyman, "Social media and cookies: challenges for online privacy," *info*, vol. 13, no. 6, pp. 30–42, Sep. 2011, doi: https://doi.org/10.1108/14636691111174243.

[8] Smah Almotiri, "Security & Privacy Awareness & Concerns of Computer Users Posed by Web Cookies and Trackers," *ResearchGate*, Dec. 22, 2022. https://www.researchgate.net/publication/374198854_Security_Privacy_Awareness_Concerns_of_Computer_Users_Posed_by_Web_Cookies_and_Trackers

[9] R. Anderson and B. Schneier, "Guest Editors' Introduction: Economics of Information Security," *IEEE Security and Privacy Magazine*, vol. 3, no. 1, pp. 12–13, Jan. 2005, doi: https://doi.org/10.1109/msp.2005.14.

[10] A. Goldfarb and V. Que, "The Economics of Digital Privacy," Feb. 2023, doi: https://doi.org/10.3386/w30943.

[11] Nidhi Sonkar, "An Empirical Study on the Economic Impact of Cybersecurity Breaches and Computer Fraud on SMEs," *Journal of Information Systems Engineering and Management*, vol. 10, no. 7s, pp. 730–735, Jan. 2025, doi: https://doi.org/10.52783/jisem.v10i7s.986.

[12] A. Wirth, "The Economics of Cybersecurity," *Biomedical Instrumentation & Technology*, vol. 51, no. s6, pp. 52–59, Sep. 2017, doi: https://doi.org/10.2345/0899-8205-51.s6.52.

[13] "Open Knowledge Repository," *Worldbank.org*, 2025. https://openknowledge.worldbank.org/entities/publication/4ec1bf22-3658-4d69-b9d3-43122254bc66

[14] C. R. Sunstein and R. H. Thaler, *Nudge : Improving Decisions About Health, Wealth and Happiness*. London: Penguin, 2012.

[15] W. Samuelson and R. Zeckhauser, "Status Quo Bias in Decision Making," *Journal of Risk and Uncertainty*, vol. 1, no. 1, pp. 7–59, Mar. 1988, doi: https://doi.org/10.1007/bf00055564.

