International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

Web Social Media Privacy Preferences and Perception

Aziz Alshehri[1], Jebreel Alamari[2]
[1]Computer Science Department, Umm Alqurah University, Alqunfuthah, Saudi Arabia
aaashehri@uqu.edu.sa
[2]Computer Science Department, Umm Alqurah University, Alqunfuthah, Saudi Arabia
joammarey@uqu.edu.sa

Abstract—The proliferation of social media websites has led to concerns over privacy breaches, as these sites have access to users' sensitive and personal data. This study sought to investigate users' perceptions and concerns for social media websites, with the aim of developing a system that meets their requirements. To achieve this, a questionnaire was designed for privacy permissions on eight popular social media websites, and 425 completed answers were analyzed. The results revealed that users' concerns were diverse and differed across different social media platforms. Gender, age, education level, and IT proficiency were found to be weakly correlated with privacy concerns. Women expressed greater concerns than men, particularly for Twitter and Snapchat, while older users expressed greater levels of concern for Snapchat and Instagram. As education levels increased, users tended to express greater levels of concern, especially on WhatsApp and Snapchat.

Furthermore, this study identified four hierarchical clusters of users based on their preferences and concerns regarding permission privacy for social media websites. The results revealed that the majority of participants (214 users) were highly concerned about privacy on social media, indicating that they were aware of the potential risks associated with sharing personal information online which represents the third cluster. The first and fourth clusters were the most unconcerned groups regarding permission privacy, consisting of a small number of users. The second cluster, comprising 124 participants, had an average score of 1.6, indicating that they were the second most concerned about privacy. Overall, the findings of this study could be useful for social media platforms in developing privacy policies and settings that align with users' concerns and preferences.

Keywords- Social media websites, Privacy concerns, Privacy permissions.

I. INTRODUCTION

In the recent years reports have highlighted how companies are collecting personal data from citizens without their knowledge or consent. This has raised serious questions around the world regarding digital privacy, and security on the internet. In some cases, this collected information is being used to manipulate people for political gain or even sold off in bulk to third-party companies with questionable intentions. As a result, citizens are becoming increasingly aware of their online activity and taking steps to protect themselves from unwanted surveillance.

The availability of social media applications through the web, opens a new kind of privacy concerns. The open nature of the web makes user tracking on social media even more pervasive. As, the web browser is the most ubiquitous application, it gives users a quick access to their social media accounts on the go without the need to install the app on their devices.

Web sites have been tracking users since the down of the WWW in the nineties. As the privacy in the web is deteriorating having social media applications available in the browser could be a real danger to private information [1].

Web browsers typically adhere to W3C web standards and guidelines for data protection so as to ensure user privacy; however, foreign code may be able to execute in the local machine without the knowledge or permission of users [2]. This could potentially allow malicious actors access to private information stored in their device's memory or use local resources available through JavaScript APIs.

Access can be gained through reading data stored locally on the browser local storage or by trying to access device hardware using JavaScript APIs. For example, a web page could read audio devices available in the system and then use them for playing sound without user's permission. This type of attack is known as "audio jacking".

Special attention has been paid to the creation of policies, procedures, and tools that help an end-user manage and interpret their personal data. Nevertheless, these methods make the erroneous assumption that users can correctly configure every produced setting and that they all share the same privacy requirements. Due to their varied privacy attitudes and expectations, users actually have a diversity of privacy concerns and requirements [3] For instance, some users think that sensitive information like age, address, and gender should be kept out of public view [4]. Also, it is not realistic to assume that all members of a population will adhere to the same privacy norms [4].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

Regarding website policies P3P (Platform for Privacy Preferences Project) was created [5]. It is a technology that enables websites to communicate their privacy policies to web users in a standardized format. P3P was developed by the World Wide Web Consortium (W3C) as a way to provide transparency and control to users over their personal information on the web.

P3P allows website owners to create machine-readable privacy policies that describe how user information is collected, used, and shared. These policies are displayed in a standardized format that can be easily understood by web users. Users can then configure their web browsers to automatically compare a website's privacy policy to their own privacy preferences and make informed decisions about whether to disclose their personal information on that website.

However, P3P has not been widely adopted and is no longer actively maintained by the W3C. Despite its potential benefits, the complex implementation process and lack of enforcement mechanisms have made it less appealing to website owners. Nonetheless, the P3P standard has paved the way for other privacy-enhancing technologies and practices that continue to shape web privacy today.

Hence, before creating a privacy protection system, it is crucial to consider users' worries about data sharing with applications. While users' levels of concern vary from person to person, some earlier study used the assumption that users have a single level of concern. Hence, a survey is created to learn about and comprehend users' problems and what demographic aspects affect users' decisions.

This paper is organized where is has five sections. In Part 2, the background literature is reviewed. The method of data collection is described in Section 3. The section 4 of the report discusses data analysis and findings. The results and recommendations for further research are included in Section 5.

II. BACKGROUND LITERATURE

In this section we can find an overview of existing privacy solutions is given in this section. Since privacy occurs whenever personal information or sensitive information is disclosed, numerous studies on privacy have recently been published in a variety of domains, including social networks, mobile applications, and websites. However, because it is pertinent to the suggested system, this part only concentrates on a mobile platform.

An article titled Disclosure Management on Social Network Sites: Individual and Contextual Determinants of Information Visibility by Masur and Scharkow examines the factors that influence users' decision to disclose personal information on social networking sites (SNSs) and how these factors impact their disclosure management [6]. The authors conducted an online survey and found that both individual and contextual factors affect users' decision to disclose personal information on SNSs. The study provides insights into the complex process of disclosure management and suggests that SNS users need to be aware of the risks associated with disclosing personal information.

"Control What You Include!: Server-Side Protection Against Third Party Web Tracking" proposes a server-side protection mechanism against third-party web tracking [7]. The authors introduce a system that allows users to specify their tracking preferences and block unwanted trackers by controlling the server's inclusion of third-party content. They demonstrate the effectiveness of their approach through experiments and highlight its advantages over traditional client-side tracking protection mechanisms. The paper provides valuable insights into how server-side protection can be used to address web privacy concerns and empower users to control their online tracking.

The paper "Tor: The Second-Generation Onion Router" by Dingledine et al, shines the light on how Tor technologies could be utilized to protect data in the web [8]. This can help protect users' privacy online and prevent third-party entities from tracking their online activities and collecting personal information. The paper demonstrates the value of privacy-enhancing technologies like Tor in protecting web privacy and providing users with greater control over their personal information online.

Adnostic: Privacy Preserving Targeted Advertising by Haeberlen et al. presents a privacy-enhancing technology called Adnostic that enables targeted advertising without compromising users' privacy [9]. Adnostic uses cryptographic techniques to enable advertisers to serve targeted ads to users without collecting or storing any personally identifiable information.

Their research demonstrates the potential of privacy-enhancing technologies like Adnostic in protecting web privacy while still enabling online advertising. By providing a way to serve targeted ads without collecting or storing personally identifiable information, Adnostic can help protect users' privacy while still enabling online platforms to generate revenue through advertising.

Securing the Web Browser Local Data Storage by Osam Salim et al. highlights the urgent need for an encryption process for personal accounts on web browsers to prevent intruders from stealing sensitive information [10]. The paper proposes an extension layer on the Chrome browser that uses the user's encryption key and the RSA algorithm, which is considered a strong encryption algorithm. The paper uses a 2048-byte encryption key to increase the strength of the encryption. Finally, the paper tests the proposed model by applying it to an experimental application and WhatsApp.

"Protecting Cookies from Cross-Site Scripting Attacks with Dynamic Path Construction" by Chen et al. - This paper

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

proposes a new approach to protecting cookies from cross-site scripting (XSS) attacks [11]. The approach involves dynamically constructing the cookie path at runtime, which makes it more difficult for attackers to steal cookies.

An Empirical Study of Web Cookies written by Aaron Cahn et al. presents an empirical study of web cookie characteristics, placement practices, and information transmission [12]. The study collected over 3.2 million cookies from two crawls, separated by 18 months, of the top 100,000 Alexa web sites using a lightweight web crawler. The paper examines privacy implications by analyzing specific cookie attributes and placement behavior of 3rd party cookies. The paper finds that 3rd party cookies outnumber 1st party cookies by a factor of two and identifies a connection between domain genres and cookie attributes. The paper also finds that less than 1% of entities that place cookies can aggregate information across 75% of web sites. Finally, the paper develops a mathematical framework to quantify user information leakage for a broad class of users and presents real-world domain findings on the issue of information transmission and aggregation via 3rd party cookies.

In a paper titled *Towards a user-centric personal data ecosystem The role of the bank of individuals' data,* discusses how personal data has the potential to become the new currency for the digital world [13]. However, the current "organization-centric" approach to managing personal data has limited the full exploitation of its potential. The paper proposes a "user-centric" model that would allow individuals to control the gathering, management, use, and sharing of data about them. The proposed model is centered around the concept of a "Bank of Individuals' Data" (BID), which would provide personal data management services to enable people to exploit their personal data. The paper argues that this role is similar to how commercial banks manage money, hence the use of the term "Bank."

III. RESEARCH METHODOLOGY

This research was conducted in three phases as following:

A. Collection of Permissions Settings

The first phase of the study involved collecting permission settings for eight popular social media websites, including WhatsApp, Facebook, Instagram, Twitter, YouTube, TikTok, Telegram, and Snapchat. This was done through Google Chrome, and the data collected included information on the types of permissions that each website requested, such as access to the camera, microphone, and location.

B. Designed Questionnaire

The second phase involved designing a questionnaire to assess users' concerns and preferences regarding permission privacy for these eight social media websites. The questionnaire consisted of two main sections, including demographic questions such as gender, age, education level, and IT skill level, and a section that examined users' worries about privacy-related issues for the social media sites.

C. Publish and Analysis Dataset

The third phase of the study involved collecting and analyzing the data. The survey was distributed through various channels, including email, social networks, and community centers, and participants were informed that they could leave at any time before submitting their answers. A total of 425 completed responses were received, which were then analyzed to identify clusters of users based on their privacy concerns and preferences. The findings of the study were published, and the dataset was made available for further analysis by researchers in the field.

IV. DATA ANALYSIS

A. Demographic information

We gathered demographic information from the study participants through a series of questions, which included inquiries about their gender, age, occupation, and educational background. This data was subsequently used to conduct an analysis of the study findings. However, it is worth noting that the researchers did not implement any specific controls over the age ratio or other demographic characteristics of the study participants.

The study participants consisted of a diverse sample of individuals, with 58.8% of the respondents identifying as male and 41.2% as female. The study also examined the age distribution of the participants, and the results revealed that individuals between the ages of 18 and 24 represented 27.8% of the total sample, whereas those between the ages of 25 and 34 comprised 16% of the participants. The largest age group among the study participants was the 35 - 44 age group, which accounted for 28.8% of the sample.

It is worth noting that the prevalence of younger participants in this study aligns with the demographic makeup of the larger Saudi population. According to data from the Saudi Statistical website, young people aged 25 to 34 years old represent approximately 67% of the population in Saudi Arabia (Saudi Statistical, 2020).

Furthermore, given the context of the study, the vast majority of the participants had attained higher education degrees, with nearly 82% of the participants reporting that they held a bachelor's or postgraduate degree. Of these individuals, the majority held a bachelor's degree, as illustrated in Table 1 of the study. These demographic characteristics provide valuable insight into the sample population and help contextualize the study's findings.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

TABLE I. SUMMARY OF RESPONDENTS' DEMOGRAPHIC CHARACTERISTICS

Factor	Category	Count	Percentage
Gender	Male	250	58.8%
	Female	174	41.1%
Age	18-24	118.5	27.80%
	25-34	68	16%
	35-44	123	28.8%
	45-54	107	25%
	55+	9	2.1%
Occupation	Student	120	28.3 %
	Employed Full time	257	60.42%
	Unemployed	43	10.16%
	Retired	0	0%
Education	High school and lower	70	16.47%
	Diploma	4	1%
	College certificate	298	70%
	Postgraduate	52	12.2%

Wisniewski et al. assert that there are significant variations in the ways users comprehend and utilize various privacy mechanisms, depending on their level of knowledge [14]. This underscores the critical need to take into account users' knowledge levels. As such, it is imperative that this survey incorporates a measure of users' knowledge levels, as nearly half of the population falls within the intermediate to advanced range. By doing so, we can gain a more understanding of users' privacy attitudes and behaviors, and tailor privacy mechanisms that are more effective and user-friendly.

B. Analyze users' preferences

To examine users' preferences, the responses were converted into a numerical scale ranging from one (highly concerned) to five (not concerned at all). The findings were then visualized using 2D heat maps, representing the average preferences of all 425 participants in a data matrix, as depicted in Figure 1. Brighter cells on the heat map indicate a greater degree of concern, while darker blue cells suggest a lower level of concern.

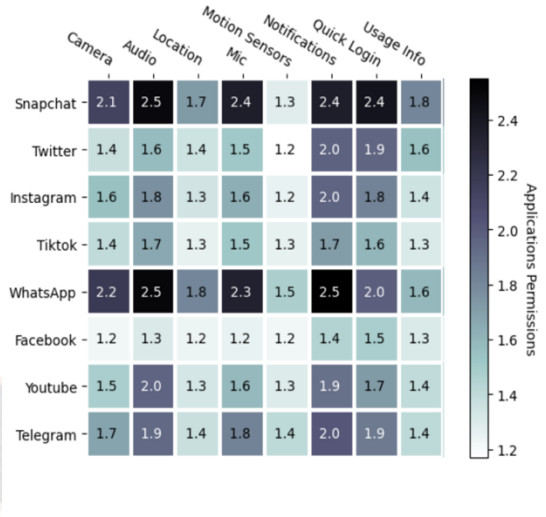

Figure 1. Average Preferences for Participants.

The websites social media that elicited the highest levels of concern, Facebook and TikTok, had the same average score ($\mu = 1.3$). Within the Facebook website, participants expressed the greatest level of concern for the camera and motion sensor ($\mu = 1.22$). In the TikTok app, the motion sensor and location information ($\mu = 1.3$) raised the highest level of concern. Overall, location information consistently represented the primary area of concern across social media websites. This suggests that users still harbor concerns regarding location information, despite improvements in privacy permissions within Google chrome.

On the other hand, Snapchat recorded the lowest level of concern ($\mu = 2.07$), with a majority of its cells appearing as darker blue on the heat map. The second-lowest level of concern was observed in the WhatsApp ($\mu = 2.05$). Participants may generally exhibit lower levels of concern when website necessitates access to personal information directly associated with its core functionality. Hence, when designing a solution, it is crucial to differentiate between website permissions related to core functionality and those unrelated.

Although the average preferences of participants provide a useful starting point for understanding current privacy concerns, the lack of diversity in user privacy preferences across all participants is notable. This contradicts findings from the existing literature, which indicate variations in users' privacy preferences. Consequently, as depicted in Figure 2, considerable effort was required to identify differences in user preferences within each platform.

In Figure 2, the darker shades of blue imply greater variation in participants' worry ratings for different social media websites. The variance result reveals that participants' preferences are definitely diverse. Despite the fact that Figure 1 demonstrates that respondents are unconcerned regarding their data being shared by the WhatsApp website, the variance result signifies that respondents' preferences for the WhatsApp website

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

are in fact varied, and that the WhatsApp website reflects the highest variation among the people. By looking at data type across all websites, the notification and quick login show the highest diversity among the participants. This variance in the indicates that information could not adequately be captured by a one-size-fits-all default approach. Moreover, there are different attitudes and different preferences towards this data because the level of privacy required differs from user to user.

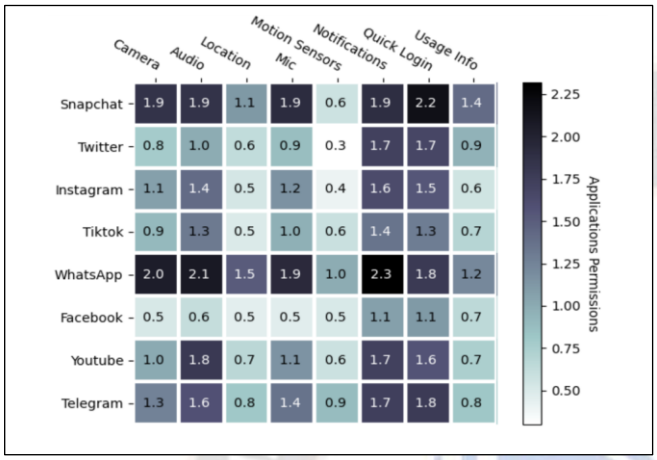

Figure 2. Variance in User Preferences

C. Correlation between Preferences and the Demographic Characteristics

Statistical analysis was another technique used in this study to look into the relationship between the preferences of participants and their demographic characteristics. The R program was chosen since it is one of the statistical tools that researchers most frequently employ to conduct complicated statistical analysis. In order to determine whether there is a relationship between user demographics and social networking web, a Spearman's test was performed. Figure 3 shows that women may be more concerned about social media website privacy than men specially for Twitter and Snapchat. This result is consistent with other studies, such as, a 2019 study by the Pew Research Center found that women were more likely than men to express concern about how their personal information was being used by companies and advertisers on their smartphones [15]. Additionally, another study found that women were more likely than men to be concerned about the impact of their online activity on their personal privacy. The study also found that women were more likely than men to take steps to protect their online privacy, such as using privacy settings on their devices and deleting their browsing history. [16].

In the context of other demographic factors, we found a correlation between age and privacy concerns on certain social media platforms, specifically Snapchat and Instagram, with older users expressing greater levels of concern. However, the impact of age on privacy concerns related to social media platforms is relatively low. The results also indicates that there is a correlation between education level and privacy concerns on certain social media platforms. Specifically, as education levels increase, users tend to express greater levels of concern, especially on WhatsApp and Snapchat. In contrast, there is no discernible correlation between IT proficiency and privacy concerns on other social media platforms. In general, the correlations between privacy concerns and demographic factors tend to be weak., as illustrated in Figure 3.

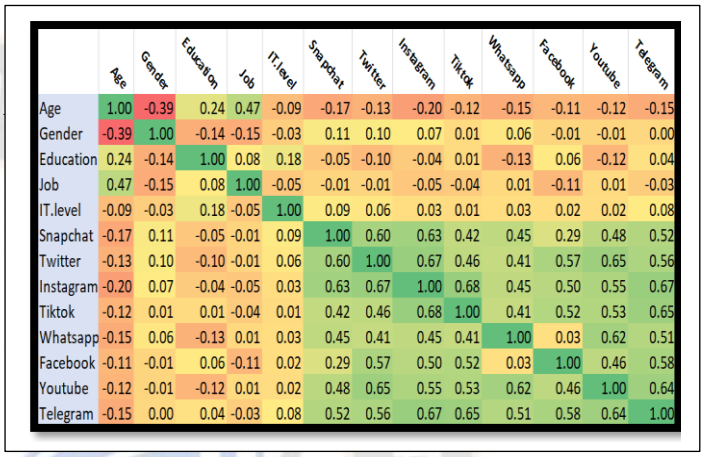

Figure 3. Correlation between users' demography and social media apps

C. Clustering Method

For more analysis, clustering method was performed to group the user population into subcategories based on similar preferences, which can serve as a basis for designing preliminary interfaces. Hierarchical clustering employs several techniques to calculate the dissimilarity between observation sets, including average, single, complete, and ward methods. Consequently, it's crucial to identify the most suitable approach for measuring the distance between pairs of observations. Nonetheless, R code has a function that generates the agglomerative coefficient, which quantifies the degree of clustering structure in the data (higher values indicate a stronger clustering structure). Table 2 presents the agglomerative coefficient for each method. As per Table 2 Ward's method exhibits the most robust clustering structure among the four methods evaluated.

TABLE II. AGGLOMERATIVE COEFFICIENT

Average	Single	Complete	Ward
.5433	.3223	.676	.895

Following the implementation of Ward's method, a dendrogram was utilized to depict the cluster hierarchy. Figure 4 presents the resulting dendrogram generated by the aforementioned clustering settings, where red color denotes the four clusters.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

This study examined identified four hierarchical clusters based on their responses as illustrated in Figure 5 and 6. The first cluster, which consisted of 39 participants, had an average score of 2.8 for all privacy permissions, making them the most unconcerned group regarding permission privacy. This group may include users who are less sensitive to sharing their personal information on social media or who have a low awareness of the potential risks associated with sharing such information.

The second cluster, which had 124 participants, had an average score of 1.6, making them the second most concerned about privacy. This group may include users who are aware of the potential risks of sharing their information online and are cautious about the permissions they grant to social media platforms but may not be as proactive in taking measures to protect their privacy.

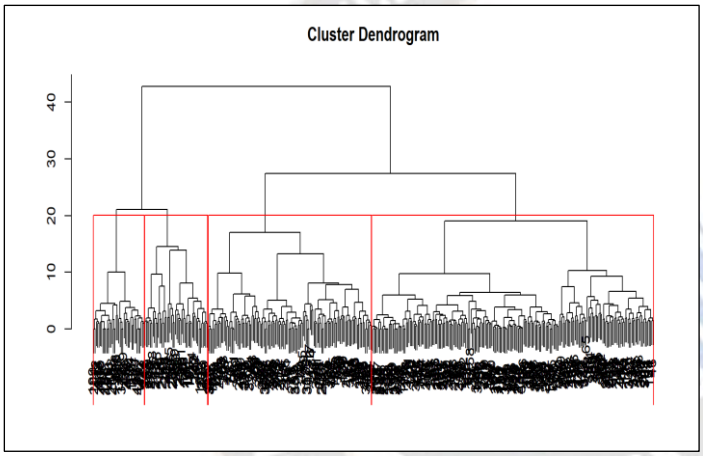

Figure 4. Hierarchical Dendrogram for four clusters

The third cluster had the largest number of participants, with 214 users, and their average score was 1.5, indicating that they were the most concerned about privacy. This group may include users who are highly aware of the potential risks of sharing their information online and are cautious about the permissions they grant to social media platforms. They may also be more proactive in taking measures to protect their privacy, such as using privacy settings or avoiding sharing certain types of information altogether.

The fourth cluster consisted of 48 participants, and their average score was 2.7, making them the second most unconcerned group regarding permission privacy. It is possible that this group consists of users who are comfortable sharing certain types of information but are cautious about sharing others. They may also trust the social media platform to handle their data responsibly or may not fully understand the risks involved in sharing their information online.

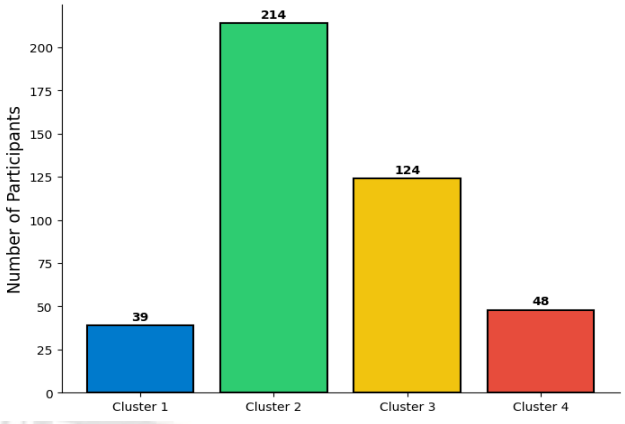

Figure 5. Participants in each cluster

It is important to note that the clusters identified in this study provide valuable insights into users' preferences and concerns regarding permission privacy for social media websites. Social media platforms can use this information to design more tailored privacy settings that cater to users' specific needs and concerns. For instance, they may offer different levels of privacy settings for different clusters of users or provide more targeted educational resources to users who are less aware of the risks associated with sharing their information online.

Cluster	Snapchat	Twitter	Instagram	TikTok	WhatsApp	Facebook	YouTube	Telegram	Average	
Cluster 1	3.0	2.4	2.7	2.6	3.9	1.6	3.2	3.2	2.8	
Cluster2	1.9	1.4	1.5	1.5	2.1	1.1	1.4	1.6	1.6	
Cluster 3	1.9	1.5	1.5	1.5	1.8	1.1	1.3	1.4	1.5	
Cluster4	2.5	2.6	2.6	2.6	1.8	3.7	2.4	3.3	2.7	

Figure 6. Average Preferences for each cluster

VI. CONCLUSION AND FUTURE WORK

In conclusion, this study aimed to investigate users' concerns and perceptions for social media websites in order to develop a system that meets users' requirements. The results showed that users' concerns are diverse and different, and there are weak correlations between privacy concerns and demographic factors. Women may be more concerned about social media website privacy than men, and there is a correlation between age and education level and privacy concerns on certain social media platforms.

Moreover, the study identified four hierarchical clusters based on users' preferences and concerns regarding permission privacy for social media websites. The majority of users were concerned about privacy, and there were two clusters of users who were more unconcerned about permission privacy.

As a future direction, this research could extend explore how the identified clusters based on users' preferences and concerns

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8082
***Article Received:** 22 June 2023 **Revised:** 20 August 2023 **Accepted:** 03 September 2023*

regarding permission privacy for social media websites could be utilized to develop tailored privacy settings for each cluster. This approach could involve creating different permission options that align with the privacy concerns of each cluster, allowing users to customize their privacy settings according to their preferences. Additionally, it would be interesting to investigate how these clusters evolve over time and whether new clusters emerge as social media platforms and users' privacy concerns continue to evolve. This research could ultimately contribute to the development of more user-centric privacy settings that align with users' diverse concerns and preferences, leading to increased user trust and engagement with social media platforms.

REFERENCES

[1] J. R. Mayer and J. C. Mitchell, "Third-Party Web Tracking: Policy and Technology," in 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA: IEEE, May 2012, pp. 413–427. doi: 10.1109/SP.2012.47.

[2] "Web Design and Applications - W3C." https://www.w3.org/standards/webdesign/ (accessed Dec 30, 2022).

[3] Agarwal, S., & Hall, C. M. (2012). A framework for understanding the impact of social media on tourism. Tourism Management, 33(1), 162-170.

[4] Song, Y., & Hengartner, U. (2015, October). PrivacyGuard: A VPN-based platform to detect side channel attacks on smartphones. In Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security (pp. 144-155). ACM.

[5] "P3P and Privacy FAQ." https://www.w3.org/P3P/p3pfaq.html (accessed Feb 15, 2023).

[6] P. K. Masur and M. Scharkow, "Disclosure Management on Social Network Sites: Individual Privacy Perceptions and User-Directed Privacy Strategies," Social Media + Society, vol. January-March 2016, pp. 1–13, Feb. 2016, doi: 10.1177/2056305116634368.

[7] D. F. Somé, N. Bielova, and T. Rezk, "Control What You Include!: Server-Side Protection Against Third Party Web Tracking," E. Bodden, M. Payer, and E. Athanasopoulos, Eds., in Lecture Notes in Computer Science, vol. 10379. Cham: Springer International Publishing, 2017, pp. 115–132. doi: 10.1007/978-3-319-62105-0_8.

[8] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The {Second-Generation} Onion Router," presented at the 13th USENIX Security Symposium (USENIX Security 04), 2004. Accessed: May 15, 2023. [Online]. Available: https://www.usenix.org/conference/13th-usenix-security-symposium/tor-second-generation-onion-router

[9] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas, "Adnostic: Privacy Preserving Targeted Advertising".

[10] O. Salim and T. Al-Rousan, "Securing the Web Browser Local Data Storage," vol. 9, pp. 75–82, Feb. 2021, doi: 10.30534/ijeter/2021/11922021.

[11] R. Putthacharoen and P. Bunyatnoparat, "Protecting cookies from Cross Site Script attacks using Dynamic Cookies Rewriting technique," Jan. 2011.

[12] Sunil Kumar, M. ., Kumarasamy, M. ., Madhavi, N. B. ., Dhariwal, S. ., Sampath Kumar, R. ., & Oyebode, O. J. . (2023). Reinforcement Based Concrete Modelling in Commercial Buildings Using Machine Learning Simulations. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 118–126. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2578

[13] A. Cahn, S. Alfeld, P. Barford, and S. Muthukrishnan, "An Empirical Study of Web Cookies," in Proceedings of the 25th International Conference on World Wide Web, Montréal Québec Canada: International World Wide Web Conferences Steering Committee, Apr. 2016, pp. 891–901. doi: 10.1145/2872427.2882991.

[14] Ms. Mayuri Ingole. (2015). Modified Low Power Binary to Excess Code Converter. International Journal of New Practices in Management and Engineering, 4(03), 06 - 10. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/38

[15] C. Moiso and R. Minerva, "Towards a user-centric personal data ecosystem The role of the bank of individuals' data," presented at the 2012 16th International Conference on Intelligence in Next Generation Networks, ICIN 2012, Oct. 2012, pp. 202–209. doi: 10.1109/ICIN.2012.6376027.

[16] Wisniewski, A., Cranor, L. F., Sadeh, N., & Sadeghi, A. (2017). A survey of parental control apps for mobile devices. ACM Transactions on Privacy and Security (TOPS), 20(4), 1-35.

[17] Ghazaly, N. M. . (2020). Secure Internet of Things Environment Based Blockchain Analysis. Research Journal of Computer Systems and Engineering, 1(2), 26:30. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/8

[18] Pew Research Center. (2019, January 14). Americans' opinions on privacy and information sharing. Retrieved from https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data

[19] Rowan, Mark, and Josh Dehlinger. "Observed gender differences in privacy concerns and behaviors of mobile device end users." Procedia Computer Science 37 (2014): 340-347.