Journal of Multimedia Information System VOL. 9, NO. 3, September 2022 (pp. 201-208): ISSN 2383-7632 (Online)
https://doi.org/10.33851/JMIS.2022.9.3.201

A Study on the Users' Response to Privacy Issues in Customized Services

Sunwoo Park[1], Jeongyun Baek[1], Yeajoo Yoo[1], Dongwhan Kim[2*]

Abstract

Customized service is a vital and mandatory element for apps in improving their technical performance and app customer analysis. While apps require users' consent for their data extraction and usage, many of the terms and agreement forms are written intricately, making it harder for users to fully understand the whole concept of users' data collection for customized services. Ever since the Facebook-Cambridge Analytica scandal, personal data privacy has been re-examined, forcing many app companies to reinforce a reliable solution to data privacy issues. However, there has not been a secured solution, which worries many people about the future advanced issues when metaverse platforms are actively used in daily apps. The research aims to collect the reactions and behaviors of everyday app users who utilize apps with customized services to understand the nature of privacy data issues and the users' opinions about the future implementation of metaverse platforms. The method of the research was an online questionnaire that targeted university students. The study revealed many fearful and anxious reactions about personal data and further metaverse issues where most app users were uneducated about how current apps collect and utilize users' private data.

Key Words: Customized Services, Data Privacy, Security Issues, Metaverse Data, Personal Data.

I. INTRODUCTION

As the internet environment developed, the types of online services naturally increased with the advent of various platforms. As a result, various internet services and platforms have emerged, including e-commerce, OTT services, social media, online advertising, and metaverse. Personalized services are commonly used among app companies to increase attention and marketing for their services. With the exponential increase in the amount of information available online, it has become an important function of the system to select and provide the most appropriate information for customers. Personalized services typically include functions that provide users with an optimal environment for collecting, storing, and analyzing personal data. This helps users to quickly choose what they want while reducing the time to explore and making it possible for companies to set targets effectively [1], for example, Netflix's drama/movie recommendation service, customized advertising, and metaverse character design.

To provide such services, a vast amount of user information and analysis must be the basis. The problem related to this are the privacy issues arising from collecting and utilizing private and sensitive information. Most data like eye movement and pulse records, sensory data, real-time user reactions and experiences are already being extracted from users. Due to such extraction of sensitive and private data, the users' security is under irrevocable vulnerability. Accordingly, policies and security technologies for hardware to prevent information leakage are being developed. Although provisions and technologies related to this exist, questions about how data is collected and used continue to be raised, and concerns of users persist.

Ethical issues derive from the data collection of current most-used apps. In many social media services, an abundance of user-generated data exposes users' private information and puts them in danger of "potential risks ranging from persecution by governments to targeted fraud" [2]. Instagram, one of the top-used social media apps, has ethical issues that most users are unaware of. With the users' consent, Instagram has full access to their users' "browsing history, location, banking details, contact details, fitness levels and more" to monitor and share with third parties. The study by pCloud (a cloud storage firm) revealed that Instagram is the "most invasive app" that shares 79% of its users'

Manuscript received August 2, 2022; Revised August 29, 2022; Accepted September 14, 2022. (ID No. JMIS-22M-08-024)
Corresponding Author (*): Dongwhan Kim, +82-2-2123-3990, dongwhan@yonsei.ac.kr
[1]Underwood International College, Yonsei University, Seoul, Korea, sunwoo29@yonsei.ac.kr, jjyyuunn@yonsei.ac.kr, gracieu105@yonsei.ac.kr
[2]Graduate School of Communication and Arts, Yonsei University, Seoul, Korea, dongwhan@yonsei.ac.kr

data with third parties. Meanwhile, Instagram shares most of its data with its parent company, Meta (Facebook), the company that had previous controversial issues with data privacy: the data scandal in 2018. This concludes as an ethical issue because users are not regularly alerted that 79% of their data is shared with third parties [3]. Also, on Twitter, privacy-related issues arise as the 'retweeting' system decisively facilitates the spread of information. According to examinations on a TweetDeck desktop client, there is no indication that the tweet is protected or locked. When the user tries to retweet a protected message, there is a notification warning that the tweet is protected yet still facilitates the action [4]. Netflix also had an issue with privacy as well. With their Netflix prize contest, "Netflix publicly released a dataset containing movie ratings of 500,000 subscribers", which led to the de-anonymization attacks by adversaries [2].

In the study of customers' attitudes towards data collection and privacy infringement, most users showed comparative optimism. Comparative optimism refers to the tendency for people to report that they are less likely than others to experience adverse events. Due to this belief that their privacy is secured and would not be misused, studies show that young users are less likely to display privacy-protective behaviors [5]. Such studies prove that consumers are unaware of the severity of privacy violations and are not concerned about highly protecting themselves, emphasizing the need to awaken people to the importance and dangers of privacy violations.

Additionally, apart from the customers' attitudes, there are issues in the privacy settings that lead to privacy violations. A survey among Facebook users revealed that the user's privacy settings did not match their sharing intentions. While a vast amount of information was being collected, users were unaware of the visibility of their profile to strangers and network members and whether their profile was searchable. Such results led to the conclusion that the current approach to privacy settings is fundamentally flawed and cannot be fixed. Privacy protection is no longer up to the users' capability as they cannot fix such errors. Therefore, the recommendations presented include an improvement in the default privacy settings of Facebook. The platform gathers an abundance of profile data, and they do not clearly inform the users on how to restrict the visibility of such data, which leads to privacy leakage without the users being aware of it [6]. An actual application of third-party data sharing appears between social media and digital news apps where "digital activity is monitored, measured, and fed back into news production" [7]. While the news is not just a materialistic product that can be "unethically" personalized to its customers, the news is a "vital foundation of democracy." Several main ways social media affect journalism are that it divides newsreaders into groups according to the user's political belief or that it directs more attention to a specific news topic shared among other people on social media. Such potential of third-party sharing within social media apps is immensely worrisome and alarming as it can even influence the political perspective of people. This information should be directly informed and educated to the app users. However, these "privacy policies are long, with vague and complicated stipulations" and freely take advantage of users.

Based on background research related to the issue of privacy on the Internet, the paper will explore through literature reviews and our research questionnaire. The paper finds the answer to the question, "What are users' attitudes toward collecting and managing personal information for customized services?" Ultimately, our study searches privacy issues for customized services that are currently widely used and observes users' reactions to the use of personal information in those services.

II. LITERATURE REVIEW

Through a chronological approach, this literature review aims to look at studies that provide the context of privacy issues within apps and explores the answer to our research question: what are users' attitudes toward collecting and managing personal information for customized services? This review will divide into three subsections that overview our research, which starts with the study of 1) privacy issues, 2) customized services, and 3) data collection in metaverse platforms.

2.1. Privacy Issues

We were initially interested in data privacy through the Facebook-Cambridge Analytica scandal in March 2018, where data extracted by Facebook was utilized to influence the polls of the UK's Brexit referendum and Donald Trump' s 2016 election to the presidency of the US. 'Big data' was a commonly used key term in explaining the data privacy of Facebook users, signifying "the capacity of today's computers to capture and store enormous quantities of data" [8]. This century's advancement in technology has made users' personal information a necessity for the financial compartment of app companies, leaving their customers vulnerable due to the possibility of data leaking and infringement. While gathering information is necessary, companies like Facebook acknowledge the terms and conditions "protected by long, complicated privacy statements," making it difficult for users to fully understand data collection and naturally leading them to consent to the terms and conditions.

Supposedly, companies assume users to naturally understand the basics of the complicated concept of personal data collection and its application to customer services, thinking that their notice in consent sufficiently informs the "benefits and costs of data acquisition" [8]. There is an increased

use of complex and opaque data-mining techniques: a complicated interrelatedness of personal data and the unpredictability of potential harms from the ubiquitous data collection in which all of these are not actively informed and noticed to users. It is commonly uninformed that major factors could break users' security and privacy, mainly cybercrime and the breaking of an individual's anonymity. The lack of information and active notice about these vital details significantly contribute to the specific attitudes of the users towards data collecting.

2.2. Customized Services

Personalization and customization of services are major compartments for "business[es] to understand the patterns and behaviors of their customers." Within the Customer Relationship Management (CRM) department, the business uses its tool and strategy to analyze its customer's interactions with the business, allowing them to predict its customers' needs [9]. Businesses' big data sources are gathered from these channels: social networks, voice/video recording, image processing, open government data, and online customers' activities [9]. These multi channels inform how much information is gathered and needed for businesses. Apart from that, the CRM department is extended to using social media for a "more precise analysis" of the customers, ultimately allowing them to generate accurate programs that fit their customers' preferences. Customer profiling is the most vital building block of "CRM' life cycle (sales, marketing, and customer service)" as businesses are always busy competing with other similar companies which makes it essential for them to provide the best experience for their customers so that they continue using their service. Thus, within their marketing strategies, the targeted audiences can see "advertisements, social media posts, or events that have emotional relation to the audience" through the offered personalized and customized services.

2.3. Data Collection in Metaverse Platforms

As security issues around personal data usage have not been fully solved and secured, many apps, including Facebook, Minecraft, Roblox, and Mesh, are already implementing metaverse platforms and services. It is a crucial issue as metaverse platforms require even more personal data that could potentially put many app users close to more harm. "A constant and boundless supply of data from the developing sensory systems" like VR and AR is highly needed [10]. Metaverse will be an unimaginably developed platform that will interact with the users through sensory services surreally, meaning users will be the main product surrounding this platform's availability. Accordingly, the metaverse will track our body movements, physiological responses (brainwaves), and real/virtual interactions with the surrounding environments. Such collection of exclusive user data leads to imminent risks related to the users' privacy, such as spying and stalking, coordinated harassment and raiding, shaming, cyberbullying, video call bombing, and other cyber-aggressions. However, many other studies provided the need for metaverse platforms and their positive remarks regarding their extensive diversity. Metaverse could be the first platform that allows global collaboration with a more advanced surreal experience. The platform may enable many social events with unlimited spaces and virtual worlds that current technologies could not allow.

There exist several reliable suggestions for countermeasures to those cyber-risks [10]. The first suggestion was the creation of a mannequin or multiple clones of one's avatar to shadow their activities and how the concept of incognito mode works. Next, a private copy of the public space was suggested for the exclusive use of the users so that they could be protected from the public spaces. Finally, the availability of teleportation among different virtual spaces allows the mode of invisibility. While these are minimal suggestions, they somewhat offer realistic solutions that could prevent the many privacy issues of data leakage or infringement. However, there still must be secured and dependable solutions to these issues offered by legitimate governance for the ethics and politics of the metaverse.

Now extensively discussing AR and VR applications, which are vital components in the metaverse platform, there is also the potential of data leakage due to AR applications requiring users to upload images or video streams. Sensitive and exclusive personal data may be leaked while those contents are shared with third parties that lack authentication and voice or gesture access protection. AR/VR technology should be advanced in these two aspects: computational offloading (where both a trusted execution environment and federated learning are utilized) and adversarial machine learning techniques [11]. These suggestions may sound complex, but they mainly fortify the data delivery system from user devices. Specifically, adversarial machine learning refers to implementing a defense mechanism based on outlier detection techniques. However, although these solutions are suggested, new problems may appear like data poisoning and interference attacks, where malicious users may train and create replica "models based on mislabeled or manipulated data" to disrupt the original solutions. As the mass of sensitive personal data is collected for advanced metaverse technology, more of these feasible solutions must be practiced and experimented with frequently.

III. RESEARCH

3.1. Research Design and Methods

Our primary research is discovering users' attitudes

toward collecting and managing personal information for customized services. The study was conducted using a questionnaire method, one of the quantification methods. The survey was conducted online through google surveys and was implemented in Korean and English. We collected data from the 53 students that responded. Within our 14 questions, we asked users' opinions about customized services, personal information, privacy issues, attitude toward terms and conditions, and personal data handling in the future (data handling in metaverse). The research was conducted on students at Yonsei University for one week from the starting day. The respondents are recruited by distributing online survey links to university community online platforms; Kakao Talk, Instagram, and other social media apps.

The strength of this research design is that it widely covers diverse aspects of our research question and that we got to cover the topic of unique questions of the metaverse, which is still a novel topic to many people and researchers. In addition, we collected straightforward and honest responses because all the respondents were active users of customer service apps. However, although the survey was intended to be widely conducted including diverse nations using our questionnaires written in English and Korean, our minimal respondents made it difficult for us to observe and understand deeper. Our most significant limitation was that we couldn't receive more respondents due to our short response collection period being affected by our university semester finals.

3.2. Results

The questionnaire was composed of 14 questions, divided into three parts – customer reactions to customized services, terms of service and privacy issues, and data collections of metaverse platforms (Table 1). The set of questions used a mixed method with both closed-ended and open-ended questions to collect data from students as precisely as possible. Table 2 is the summary of the results of the survey.

3.2.1. Reactions to Customized Services

The first six questions investigated whether students were familiar with customized services. We began with the question "Do you know about customized services?" to check whether students had heard of the term and whether they knew what the service was. 38 out of 53 students responded, "Yes." Consequently, the survey explained the term - any service that is tailored to the needs of individual customers.

75.5% of the students, 40 people, responded that they were currently using customized services. In comparison with the first question, it is shown that two of the students were not familiar with the term even though they were utilizing the service. Surprisingly, the remaining 24.5% of the total respondents answered that there were no customized services they use often. Many applications including social media services and OTT platforms contain personalization algorithms which are default services, meaning the users cannot remove them. Thus, this proves that approximately one-fourth of the respondents either rarely or do not use the previously mentioned applications or use them without perceiving that they include such algorithms.

Of the 40 responses, 29 answered that YouTube is a customized service they most often use, followed by various OTT services, Instagram, online clothing stores, and delivery services. Customized services can now be seen in diverse applications, regardless of the products. Of the several services, it was shown that video platforms, including

Table 1. Questions included in the questionnaire.

Variables	No	Questions
Customized services	1	Do you know about customized services?
Customized services	2	Are there any customized services that you use often?
Customized services	3	Choose your own opinion to the customized service.
Customized services	4	What do you think about the need for personalized algorithms?
Customized services	5	Which value do you think is more important, customized services or privacy?
Customized services	6	Do you think it is fair for companies to collect a variety of users' data to provide customized services?
Privacy issues	7	Have you ever felt that your personal information has been leaked?
Privacy issues	8	Do you actually read the terms of service (TOS) and Personal Information Collection and Use Agreement when using a service?
Metaverse platforms	9	Have you heard of any metaverse platforms (Gather, Zepeto, Sandbox, etc.) taking one's physical data yet? Or leaking any physical data?
Metaverse platforms	10	How willing are you with metaverse platforms taking data about your physical body (face expressions, behaviors, eye movement, heartbeat) even if it's for the better of the service of apps?
Metaverse platforms	11	What scares or worries you the most about the misuse of users' physical data?

Table 2. The summary of the results of the survey.

No.	Results
1	Over half of the students (38 out of 53 students) already knew the term: customized services. 38 out of 53 students responded, "Yes" to the question.
2	75.5% of the students responded that they were currently using customized services. YouTube is a customized service respondent most often use (29 out of 40 students), followed by various OTT services, Instagram, online clothing stores, and delivery services.
3	Although the recommendations and algorithms are convenient and useful, they cause concerns about personal information exposure.
4	64.2% of the respondents answered that customized services are "only needed for some services."
5	On a scale of 1 to 5, 1 is customized services and 5 is privacy. 22.6% chose 1 and 2, 41.5% chose 4 and 5, and 35.8% stayed neutral (the two values are equally important). Twice as many people claimed that their privacy was more important than the service.
6	26.4% answered unfair while 24.5% answered fair. 49.1% selected neutral, meaning they think it is partially fair yet unfair at the same time. Majority of users are not as unwilling to share their information with the companies.
7	Over half of the participants (56.6%) responded that they had already felt that their personal information had been leaked. It proves the anxiety and instability the services induce.
8	Over 90% of the respondents answered that they do not read the terms and conditions agreement (TOS) before using the service. The reason for this: "it was too long", "knew they would eventually use the service regardless of the terms".
9	Only 39.6% responded that they were familiar with the collection of data performed by metaverse platforms.
10	60.3% responded that they were unwilling to the platforms to take their physical data, while only 13.2% responded willingly. No one answered that they were 'absolutely' willing to offer physical body information.
11	44 respondents stated, "Other third parties freely using my information," followed by "data leaking," "vulnerability under hackers," "imposters," and "stalking."

YouTube and Netflix, were the most highly utilized. YouTube, Netflix, and Instagram have been considered the top used services by people in their 20s, especially undergraduates, proving that most apps we use in our daily lives contain recommendation systems.

The participant's reactions to the previous services were that although the recommendations and algorithms are convenient and useful, they cause concerns about personal information exposure. Therefore, even users who effectively utilize such services are aware of the dangers and feel anxious that their information could be leaked.

When investigating people's demand for personalization services, 64.2% of the respondents answered that they are "only needed for some services." Contrary to our expectations, most consumers think that personalization algorithms are necessary only for products that are truly useful and essential for their convenience.

This could question the fundamental necessity for this specific service as customized services are not a matter of choice. It is now a built-in function within the application, where users cannot choose to reject the recommendation technology, nor can they control the level of recommendation. However, the problem exists of people feeling uncomfortable due to inaccuracy and limitations and customers having to endure the anxiety of their personal information being leaked. This is a severe flaw as services are meant to provide convenience rather than making the customers always feel insecure and worried.

Such results conveyed the limitations in the coexistence of personalization and security. Accordingly, we investigated what customers value more – customized services or privacy. On a scale of 1 to 5, in which 1 is customized services, 22.6% of the people chose 1 and 2, while 41.5% chose 4 and 5. 35.8% of 19 stayed neutral, stating that the two values are equally important. Thus, it is shown that nearly twice as many people claimed that their privacy was more important than the service of the apps. However, compared with the previous results, it was shown that their eagerness for privacy protection was not enough to stop them from utilizing the applications with customized algorithms completely.

Similarly, when investigating whether the respondents think it is fair for companies to collect various personal information for customized services, 26.4% answered unfair while 24.5% answered fair. 49.1%, nearly half of the participants selected scale 3, meaning they think it is partially fair yet unfair at the same time. While the previous question showed that an overwhelming number of people valued privacy over customized services, this result indicated that users are not as unwilling to share their information with the companies. Their concerns are not about sharing the information with the companies - instead, they are worried that

third parties would misuse or spread the personal information. Overall, the results showed users' inner conflicts between the two values. Simply put, customers are willing to provide the companies with their information yet expect them to use it only for the services while guaranteeing privacy protection.

3.2.2. Reactions to Terms of Service and Privacy Issues

Unfortunately, it is almost impossible to satisfy both convenience and privacy, as the users must give up one or the other. To our surprise, 56.6%, over half of the participants responded that they had already felt that their personal information had been leaked. They have felt this in various ways, including Instagram recommendations, YouTube algorithms, spam messages, and other customized advertisements. They mentioned how scary it is that services gather a tremendous amount of information in an instant without us even noticing. Regardless of whether their privacy has been leaked or not, the fact that the customers feel this way proves the anxiety and instability the services induce.

Further, this reveals the reality that people have already given up their privacy and learned to come to terms with their situation. The results have shown that although people are afraid of privacy leakage, most showed willing reactions in continuing to utilize the services. Thus, we decided to investigate users' attitudes towards the terms of service (TOS) to see the cause of this problem.

As we predicted, over 90% of the respondents answered that they do not read the terms and conditions agreement before using the service. The reason why they did not read them was that it was too long and because they knew they would eventually use the service regardless of the terms. Examining those who read the terms and agreement and found the terms unfair, their attitude was to remain silent and either agree or refuse to use the service rather than report the issue. There were no instances in which the users reported the issue or attempted to inform the public. Although it is the social responsibility of corporations to protect their customers' privacy, it is equally important for the customers to maintain an assertive attitude towards their information. The survey results have shown that most consumers have not taken the time to go over the terms and act upon their injustice.

3.2.3. Reactions on Metaverse Platforms

While the previous set of questions tackled users' attitudes towards gathering personal information meaning their name, age, gender, and address, we began to question whether their attitudes would differ when collecting physical information. Recently, several metaverse platforms such as Gather, Zepeto, and Sandbox have started taking one's biological data, including facial expressions, behaviors, eye movements, and heartbeat. Unlike the previous results, participants showed a much adverse reaction to the data collection. It was first shown that not many people are aware of the current service, as only 39.6% of the people responded that they were familiar with the collection of data performed by metaverse platforms.

60.3% of the respondents, 32 people in total, responded that they were unwilling to the platforms to take their physical data, while only 13.2% responded willingly. Surprisingly, not a single participant answered that they were 'absolutely' willing to offer information on their physical body. This proves that people react more sensitively when it comes to physical information.

When investigating the reasons behind their concerns about sharing biological data, 44 of the respondents stated, "Other third parties freely using my information." Then came "data leaking," "vulnerability under hackers," "imposters," and "stalking." Their worries have become more serious, reaching severe crimes such as stalking and impersonation, showing the lack of credibility of this data collection as well as consumers' worries based on previous experiences. We figured corporations would have to devise an effective way to improve data security and ensure their customers earn their consent and execute the service.

IV. DISCUSSION

Putting together the literature review and survey results, this was the answer to our research question: users indeed show an adverse reaction towards providing personal information yet eventually agree to all the policies and continue to utilize the services.

The findings of this study included the fundamental flaw in the function of the personalized services, as well as users' ambivalent reactions. When collecting users' opinions of personalized and customized services, there were various negative opinions apart from the ones related to security. Most responded that the inconvenience of the lack of diversity of personalized services was because the recommendations they received were only of their taste. For example, the main page of an online shopping website could backfire by showing a whole page of clothes that look the same and have similar designs. On a different note, some users complained that the recommendations did not match their authentic tastes and were wholly contrary. Thus, we questioned whether users truly need customized services and who the primary beneficiary of this system is. Such confusing and unmatched customized services prove that there must be a reorganization and examination of the services' systems to refine the existing issues.

Now discussing privacy, the results showed that customers deeply value privacy over customized services and even worry for their safety. However, most respondents recorded

that they were not as cautious about protecting their safety as they did not fully read the privacy policies and understand the whole concept of data sharing. The reasons made for the avoidance of reading the policies was that the forms were intricately written in long document forms and a time-consuming nuisance apart from convenient mobile use. Consequently, this made us question whether most users may have reacted differently if the terms agreement were displayed in a shorter and more readable form. We also questioned the true motive of customized service apps as to why the privacy policy and consent forms needed to be written so complicatedly. It was difficult to ascertain why companies couldn't offer a simpler method when asking for customers' consent by spreading awareness and educating about data sharing and leakage for the better of their customers.

Despite the readability and length of the terms, the fact did not change that although users are afraid and anxious that their information could be leaked, they remain a passive attitude by giving up their complaints and dissatisfactions. However, considering precedent cases such as the Facebook-Cambridge Analytica scandal and the advent of metaverse platforms, privacy issues are becoming more serious, thus causing a rise in consumer insecurity.

Therefore, we came up with the following suggestions: a reinforcement of data security, customers' assertive behaviors, or possibly a change in the customization system itself. Companies must present robust solutions for privacy protection, such as multiple steps for verification or mandatory password changes, to guarantee customer safety and satisfaction. Further, the consumers must be more informed and show an assertive attitude towards scandals and cases of privacy infringement, claiming justice. Lastly, we felt the urgent need for a reinspection in the customization service itself - as it currently contains several issues, corporations must develop a way to improve their deficiencies. Especially for metaverse platforms, while technicians' confidence that metaverse is going to be an unimaginably developed platform is highly ambitious, they must first secure trust and credibility that their service is genuinely beneficial and convenient.

V. CONCLUSION

To wrap up, through our initial interests in problems around app users' data privacy, we were able to conduct research surrounding our research question: users' attitudes toward collecting and managing personal information for customized services. As our research derived from our literature review about the Facebook-Cambridge Analytica scandal, customer services, and the significantly harmful data issues of using metaverse platforms, we decided to study people's reactions to customer services and the concept of data collection and usage.

Ultimately, our findings from our survey responded by 53 Yonsei students were greatly helpful in understanding the nature of people's reactions and behaviors to data privacy issues. We could deeply comprehend how and why privacy issues occur from the users' side because they ultimately hold the power to consent to data collection. Users have the key to allowing apps to collect their private information and utilize it for optimizing customer services. Our findings showed that many users were conflicted about their willingness to the app's customer service. Around the critical concept of consent, there needs to be a bold line of trust between the users and apps, which was absent in the case of the Facebook-Cambridge Analytica scandal. Although it is a conclusive fact that many apps' unjustness and problematic management of their users' data should undoubtedly be restored, we cannot fully state that users do not have partial responsibility for possible data leakage or infringement.

The main issue we found from our research was that many people feared having their data leaked but still were willing to share their information, while most had not even properly read the terms and agreement. It is essential to notify the complexity of the many app services' terms and agreement. However, we learned how much users' personal education about data privacy is even more significant. Users are also responsible for educating themselves and understanding the specifics of their apps' data collection and usage. On the other hand, as we have mentioned in our Results and Discussion, apps also hold primary responsibility for restoring and strengthening their security system. As they may need reinforcement of data security and changes in their customization system of advanced steps for verification steps, they must, most importantly, encircle their app business aim not only around their financial gain but around the security of their app users.

In conclusion, through this research study, especially with metaverse services where the tech industry is strongly growing and aiming towards that platform, we learned that more app users need to be informed and educated about the current data privacy issues while apps suggest bolder solutions.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program (2021R1I1A4A01059550) through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, and the Yonsei University Research Fund of 2021-22-0320.

REFERENCES

[1] C. Kim, J. Lee, and W. Kwon, "Grounded theory approach to the procedure of customized service experiences," *Journal of Information Technology Applications and Management*, vol. 29, no. 1, pp. 39-51, Feb. 2019.

[2] G. Beigi and H. Liu, "A survey on privacy in social media: Identification, mitigation, and applications," *ACM/IMS Transactions on Data Science*, vol. 1, no. 7, pp. 1-38, Mar. 2020.

[3] A. Cuthbertson, Instagram is 'Most Invasive App', New Study Shows, Mar. 2021. https://www.independent.co.uk/tech/instagram-invasive-app-privacy-facebook-b1818453.html.

[4] B. Meeder, J. Tam, P. G. Kelley, and L. F. Cranor, "RT @IWantPrivacy: Widespread violation of privacy settings in the Twitter social network," in *Proceedings of the Web*, 2010. vol. 2, no. 1, p. 2.

[5] Y. Baek, E. Kim, and Y. Bae, "My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns," *Computers in Human Behavior*, vol. 31, pp. 48-56, Feb. 2014.

[6] M. Madejski, M. Johnson, and S. M. Bellovin, "The failure of online social network privacy settings," *CUCS*, 2011.

[7] P. C. Adams, "Agreeing to surveillance: Digital news privacy policies," *Journalism & Mass Communication Quarterly*, vol. 97, no. 4, pp. 868-889, 2020.

[8] M. Fuller, "Big data and the Facebook scandal: Issues and responses." *Theology*, vol. 122, no. 1, pp. 14-21, 2019.

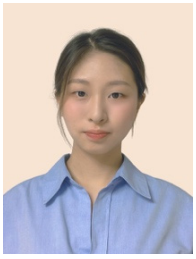
[9] M. Anshari, M. N. Almunawar, S. A. Lim, and A. Al-Mudimigh, "Customer relationship management and big data enabled: Personalization & customization of services," *Applied Computing and Informatics*, vol. 15, no. 2, pp. 94-101, 2019.

[10] R. Di Pietro and S. Cresci, "Metaverse: Security and privacy issues," *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. *IEEE*, 2021.

[11] M. Xu, W. C. Ng, W. Y. B. Lim, J. Kang, Z. Xiong, and D. Niyato, et al., "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges", *arXiv Preprint arXiv:2203.05471*, 2022.

AUTHORS

Sunwoo Park is an undergraduate student majoring in Creative Technology Management at Yonsei University.
Her research interests include social computing and strategic marketing.



Jeongyun Baek is an undergraduate student majoring in Information and Interaction Design at Yonsei University.
Her research interests include social computing and UX/UI design.

Yeajoo Yoo is an undergraduate student at UIC, Yonsei University, majoring in Creative Technology Management.
Her research interests include data analysis, social computing, and financial management.

Dongwhan Kim is an assistant professor in the Graduate School of Communication and Arts at Yonsei University. He obtained his Ph.D. in Communication from Seoul National University in 2017.
His research area includes Human-Computer Interaction, social computing, computational journalism, information visualization, and UX/service design.