Jld. 25, Bil. 1, 2023: 67–80 | *Vol. 25, No. 1, 2023* (Special Issue)*: 67–80*
https:10.22452/jpmm.vol25no1.6

Analysis of Privacy Awareness Among Social Media Users in Malaysia

Chung Jia Ee
Tunku Abdul Rahman University of Management And Technology
chungje-wk18@student.tarc.edu.my

ABSTRACT

Social media has slowly taken over our privacy to exchange the accessibility of platforms. This study is to raise awareness to the public about the importance of privacy invasion and alert them to take action on it. It concludes users' privacy awareness level is high, but they are not cautious enough which leads to unsharp opinions, and they do not have any idea of protecting their privacy. The results show the majority are willing to disclose family and financial information as they think that social media is safe if respondents only allow friends, they know to view their social media.

Keywords: ***privacy invasion, privacy, privacy awareness, private information, social media***

INTRODUCTION

The YouGov research (Ho, 2019) found that six in ten Malaysians are not willing to delete their social media accounts permanently, even if they are offered money. Besides, their main intentions for being obsessive in social media is to stay up to the latest events or news which has the highest percentage of 72%, followed by social interactions (69%), sharing content with friends (51%) and engage with entertaining information (48%). However, with the deep obsession with social media, users' privacy concerns have strengthened in recent years (Ho, 2019).

Social media sites often encourage users to share their daily activities online and it is often called "oversharing" as they are putting themselves online easily with just a click. For example, social media users have been sharing personal information in various ways such as posting family photos, friendships, updating emotional status or even "check-in" to locations they have visited. Unfortunately, this simple act could lead to a security problem known as stalker paradise. A stalker can easily look into your profile and view everything you have shared online. The more information you share, the more they know about you (Heffernan, 2017).

These stalkers could hack into your personal social media accounts and build up every piece of information you shared. For example, there are possibilities that your family or friends

will tag you into a photo, with this, stalkers are able to trace the relationships between you and your family or friends for more details. Moreover, users nowadays love to add hashtags on the caption like #ClassOf2021 or #DinnerWithFamily, stalkers could quickly trace for these hashtags and find out the name of your high school or the location you are currently at. Thus, it could be concluded that the stalkers are using your posts against you (Patel, 2020).

Viasat Savings found that nearly 50% of respondents chose to keep their social media private, while another half chose to keep their social media public without activating any privacy settings (Wachtor, 2019). The residential and business telecommunications specialist, Autumn Knowles also mentioned that different age ranges will have different views on social media privacy where the age range of 45-54 kept their social media accounts more private than any other age group. On the contrary, respondents aged above 54 kept their accounts public without choosing any privacy settings (Suciu, 2020). The study (Wachtor, 2019) even stated a high number of respondents (71%) took time to check on privacy settings, thus, it could be noticed that the privacy awareness of social media users is getting higher where it is a good sign that users would take control of their privacy if they were provided opportunities to.

Social media is taking over our personal details including photographs, location, religious belief, relationship status, contact information, and others. More applications have emerged, and these have given more opportunities to get invaded. According to the Personal Data Protection Act 2010 (PDPA), s.2{1}{a} and {b}, social media users are legally protected by the Malaysian Government from having their personal data used without consent. This law also applies to social media companies that have a local office and processes users' data for commercial transactions purposes. Social media platforms like Facebook require new users to agree to their terms and conditions before allowing access, thus it can be argued that social media has already provided consent with the users despite it is still illegal for any third parties to view a user's private conversations. Nevertheless, social media could still get users' data from tracking date, engagement time, location or even phone numbers (Turner & Amirnuddin, 2018, p. 35).

It could be argued that social media platforms do ask for permission to the privacy policy before the social media users agree to it. Yet, in the US, only one in five adults (22%) say they always or often read the privacy policy while around 36% of individuals never read them all the way before accepting it. With this, it could cause the public to have a lack of understanding about the privacy policies (Brooke et al., 2019). This situation occurs in Malaysia as well, especially when it comes with the long and complex languages offered in social media platforms. An article written by Marcus (2017) claims that "whenever you have signed the policy, you are unable to escape it", as agreeing on the policy means establishing the legal relationship (Marcus, 2017).

Based on research conducted by Pew Trust, 80% of social media users are worried about the accessibility of businesses and advertisers towards their privacy information and social media posts. These privacy concerns have urged social media platforms to tighten the regulations where they have hired professional cybersecurity to be responsible for the safeguarding process upon users' personal data. Majorities are uncomfortable and unconfident with their data being used by the unknown (Smith, 2017). Lewis (2021) stated that when users' personal information falls into a criminal's hand, the outcome would be severe. One of the consequences could be hacking the users' account and users would be unable to access their social media accounts permanently, thus losing all their memories, posts, histories, and conversations in the relevant platforms. Moreover, it is attractive to the

criminal to target on social media platforms as it possesses a huge amount of personal data with limited governmental oversight (Lewis, 2021). Throughout the research, this study aims to identify the privacy awareness level of Malaysians on Social Media sites and the result will show the truth behind the curtain by finding out how social media spies on the users and what they do with the data they collect, thus, benefit the users in protecting their privacy personally. By understanding privacy awareness, it could raise awareness to the public, especially parents or teenagers to be conscious of the importance and the impact of privacy invasion. It is important to raise users' privacy awareness as there are no specific borders in defining privacy.

Research Objective:

1. To find out how social media invades the privacy of a netizen.
2. To find out the privacy awareness level among Malaysians.

Research Questions:

1. How did the privacy invasion happen?
2. Are social media users aware that their privacy is leaking to unknown parties?

LITERATURE REVIEW

Privacy is a concept that protects human dignity and sets a fundamental barrier to protect our human rights. Past examinations have concentrated on several privacy concepts when it comes to the relation with social media. It is possible to argue that there is a relevant subjectivity and variety of privacy equal to the size of the community. Deniz (2020) states that one of the dominant effects that are influencing the social media society has been privacy. We have publicised plenty of our personal information that should be protected due to how we use social media. This is because individuals were affected by the social media world that emphasises vision and beauty, hence, they are craving in creating ideal profiles and slowly they disclosed their information unconsciously. Deniz concluded that the privacy awareness of a user will strongly affect their usage of social media (Deniz, 2020, p. 157).

Although social media does increase many meaningful encounters for the users, it is undeniable that threats to privacy have darkened the users' life where it is also damaging the quality space of social media. Redmiles et al. (2019) have conducted a study upon the safety perceptions of social media. It was found that there are different elements of threat towards the safety perceptions of social media such as security, privacy, and community, while the biggest threat experienced by the participants was privacy settings. It was discovered that social media users are more eager to tailor their privacy control on their posts and profile details as these settings would make them feel safe and secure. Besides, Redmiles et al. (2019) states that social media users lack understanding around the personalization settings because when individuals do not know how the content and advertising is tailored personally due to their preferences, they often will report it as an inappropriate tracking or accessing to their social media accounts. Yet, it was claimed that the personalised content is based on the user's demographic information and their clicking behaviour when surfing on social

media (Redmiles, Bodford & Blackwell, 2019, p. 414). Hence, this literature argues about the factors affecting the privacy awareness of social media users and hopes to educate the users to increase their understanding upon content targeting practices.

Turner and Amirnuddin (2018) have investigated the privacy argument which appears to be two-sided. The first side stated that privacy may or may not be invaded by third parties which the users are knowingly knowing what information they disclose to them. Secondly, it states that privacy may or may not be invaded by third parties which the users lack understanding of the terms and conditions that they agreed on. The literature argued that by providing clarity to the social media users, it would enable the privacy invasion to be determined and find out whose responsibility it is when it comes to protecting user's privacy on social media (Turner & Amirnuddin, 2018, p. 33). Turner and Amirnuddin (2018) also view privacy from the legal perspective in Malaysia. They argued that there is only one Act legally protecting user's privacy and personal information which is the PDPA 2010 that was mentioned earlier in the introduction. PDPA protects users' information from third parties without their consent yet, it is still blurry that it needs to depend on the details of instructions and purposes in order to get protected legally by the Act. It is arguable that the user's personal information will only be protected if the Act is more specific. Furthermore, they also highlighted the limitation of legal provision about privacy invasion in Malaysia (Turner & Amirnuddin, 2018, p. 35).

Another concept stated by Scoglio (1998) in the book entitled Transforming Privacy has differentiated privacy into four different dimensions which are physical, informational, decisional, and formational. Physical privacy refers to an individual who enjoys physical protection in his residence or body. Informational privacy determines the control of accessing information an individual has about themselves. Decisional privacy concerns the decisions and choices an individual has over their personal privacy. While formational privacy is the main dimension of privacy that is evaluated by the individual's interest in self-reflection or their critical interiority. Although different dimensions are emphasised, the control over personal information of an individual still comes into question. Scoglio (1998) stated four categories to protect personal information from being violated which are: (a) the right to control personal information, (b) The freedom of personal autonomy, (c) The right to control personal property, (d) The right to control physical space (Scoglio, 1998). From here, social media privacy could be categorised as Informational Privacy and Decisional privacy where users still have the right to control their personal information.

Southerton and Taylor (2020) have studied about the trustworthiness of social media among young people during 2020 and emphasises on the habitual disclosure of an individual. Social media sites who claim to safeguard user's information have ended up leaking data to public or private organisations such as scandals relating to Facebook's privacy violations, Cambridge Analytica's data brokerage, data leaking from online dating sites and retailer websites. The ethics of social media data collection has raised questions from the users in the safeness of their privacy (Southerton & Taylor, 2020, p. 1). From the study, the scholars argue that social media platforms encourage their users to share personal information through habitual or routine relationships. They are embedded into young people's daily routines to find out their habitual actions like pushing the like button, commenting on interesting posts, seeking interaction between users, or checking to see if a friend of theirs has seen the message. The continuous failure of protecting user's privacy did not result in the users resisting using the social media platform. The scholars found that the platforms put effort into creating a

comfortable and pleasurable social environment from observing the habitual and routines of users in order to blindfold them in concerns about the platform's responsibility to protect the privacy of users (Southerton & Taylor, 2020, p. 9). Besides, Southerton and Taylor (2020) argue young people fail to be responsible in managing their disclosure to privacy risks even if there are repeated privacy issues. The scholars even describe them as ignorant in their daily practices as they seek familiarity, pleasure, intimacy, and comfort that could be crucial in providing private information to the platforms. A participant named Emily depicts her data being gathered and presented back to her in personalised advertisements as scary, yet she reassures herself that personalised advertisements are not that harmful and Emily concludes that she has the responsibility to avoid this process (Southerton & Taylor 2020, p. 4). Hence, it is arguable that social media is embedding to the lives of individuals by checking their habitual, engagement and repeated "checking in," in order to reduce their privacy awareness on the great surveillance of the platforms.

Becker (2019) has debated on the meaning of privacy as it always comes blurriness in the definition. There are overall two privacy concepts to be distinguished which are descriptive conception and normative conception. Descriptive conception of privacy refers to natural privacy where it describes the desirable degree of privacy in whether an individual has exclusive control over their own information. In another word, it describes the degree of privacy you ought to have. While the normative conception of privacy concerns the ground of why privacy is so important to have a fulfilling life (Becker, 2019, p. 307). Becker (2019) stated that these concepts should not distract us from viewing privacy as a positive connotation and accepting the fact that it is not a neutral concept. The scholar mentioned that discussing the concept somehow brings the violation of privacy into question, asking why privacy should be protected, in fact, it belongs to something valuable that is worth to be cherished. In the digital age, big applications and cloud computing are broadly recognized, while it also raises the dangers to privacy (Becker, 2019, pp. 307-308).

Algorithms in social media, which are always defined as the technical side of summarising relevant posts or evidence to prioritise content to reach a personalised platform, have been collecting data on users through activities like profiling, including the location or demographic information. The platforms unconsciously seduce or convince the users to participate in certain activities for reasons and gather the information that is advantageous to the platforms and the third parties to meet their own interests (Becker, 2019, pp. 308-309). Becker (2019) debates that using algorithms in the decision-making process has intensified the loss of autonomy in two aspects. Firstly, algorithms are used to track a user's behaviour without any human or observer actually viewing the user's profile. However, this invisible tracking device increases the accuracy of the user's behaviour, and here, humans lose autonomy in managing privacy issues (Becker, 2019, p. 309).

Sarikakis and Winter (2017), who conducted an article entitled *Social Media User's Legal Consciousness and Privacy*, debated that privacy is not a right but it is a commodity to exchange benefits from the users such as exchanging personal information to gain access with friends online. Scholars have focused on the degree to how people are aware of the violation of privacy and surveillance technology in this era. They explore how much individuals understand the conceptualization of privacy and the information-sharing decision on the platforms. The results showed that social media users were overestimated by platforms about their knowledge on privacy policies and this could lead to the consequences of trafficking personal information and fundamental rights (Sarikakis & Winter, 2017, p. 4).

Marwick et al. (2017) have found that youth maintain critical standards towards the online information flow. They set boundaries to know what kind of messages are suitable for different contexts, thus, overturning the argument about "young people do not care about privacy" (Marwick et al. 2017, p. 2). Marwick et al. (2017) are surprised by the results that young people are aware of what they post online and conclude that it is an individual's responsibility to choose what to disclose. From family members tagging them in photos to friends embarrassing them by naked graphics, they critiqued the vulnerables' behaviour in being careless of the content they posted. Some respondents even feel responsible in making sure their posts do not offend any party as the online world is just like face-to-face interactions, where we do not say anything that comes to our mind. When discussing online surveillance, the study claims that most individuals know the existence of the surveillance online, and the impacts are said to be avoidable (Marwick et al. 2017, p. 5). Yet, there is still a weak form in this study, as the respondents are all of low socio-economic status, most of them consider physical surveillance way more important than online surveillance, thus claiming that online surveillance is a type of class privilege.

Data Sharing Model

There are many statements interpreting how social media is invading the privacy of a netizen, yet most of them are predictions with no relevant proof. A Data Sharing Model (2018) that was developed by Conger shows the relationship of how privacy of a netizen could be violated between users, social media platforms and third parties, which is mostly the advertisers (Nyoni & Velempini, 2018, p. 2). In the beginning, the social media users trusted social media platforms like Facebook and provided them with their personal data. In order to access a new Facebook account, a number of personal information will be disclosed to the platform for identification purposes. Thus, users have to trust the platform before giving away their personal data. Next, the social media platform will take the risks of holding onto users' personal data such as emails, phone numbers and demographic information. These data will be stored in a variety of storage servers that are not in gigabytes but in petabytes or terabytes (Nyoni & Velempini, 2018, p. 2).

The following procedure is the social media platform providing users' data to hosted third-party applications. People might be curious on what kind of data is sent to the third party while based on social media marketing research by Pixlee, social data was collected and sent to the third party (Pixlee, 2021). Social data refers to the data of how a particular user shares, views and engages with the content. Based on the number of shares, increase of likes and view time, the platform will categorise what the user prefers by using algorithms and thus, help the advertisers to target the accurate users to reach the efficient marketing results. In the end, the users' data is passed to online advertisers in order to create a personalised advertisement. This Data Sharing Model has shown users lack awareness of what privacy has been stored by social media platforms and slowly lead to the privacy invasion issue (Nyoni & Velempini, 2018, p. 2). Figure 1 shows the Data Sharing Model that depicts relationships between social media users, social media platforms and online advertisers.

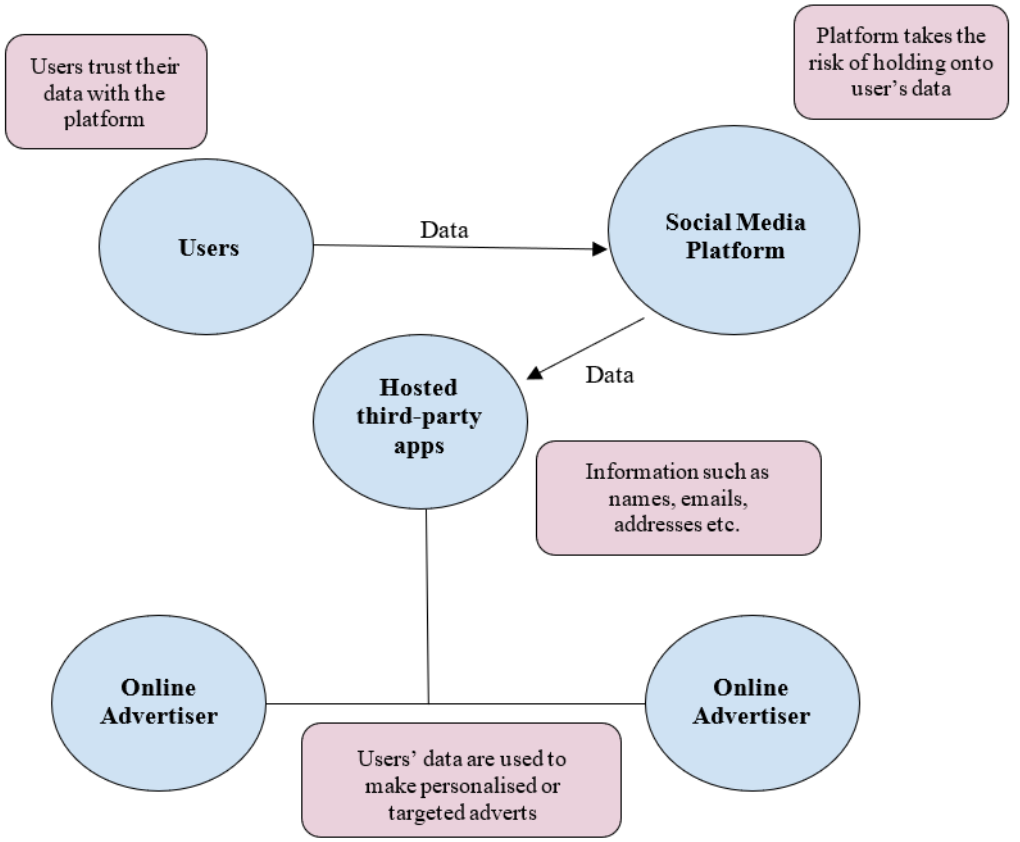

Figure 1. Data Sharing Model

Theoretical Framework

This research uses Communication Privacy Management Theory (CPM) to measure how social media users are regulating their private information in social media platforms. CPM was first introduced by Sandra Petronio in 1991 and was used to find out the management of private information from individuals. It provides an understanding of how people regulate their private information in daily life, and it also argues that some individuals believe they have the right to own their private information. CPM theory further developed by Petronio and Child (2020) explains how privacy information will be managed if it is divulged, and who will be responsible for the mistakes (Petronio & Child, 2020, p. 76).

Gruzd, Jacobson and Dubois (2020) argued that CPM has five different factors to influence users' privacy considerations which are Gender, Culture, Motivation, Context and Risk-Benefit Ratio. They extended the CPM theory and confirmed that the privacy boundaries that affect private data to be publicly available in social media have become fuzzier (Gruzd, Jacobson and Dubois, 2020, p. 9). Besides, Petronio (1991) outlines that when an individual shares his or her personal data with others, the receiver has the responsibility to guard the information (cited in Gruzd, Jacobson and Dubois, 2020, p. 10). With this, Gruzd, Jacobson and Dubois (2020) utilised it on social media platforms, where it shows third parties such

as Advertisers or Researchers that use personal data provided by social media, have the similar responsibility to guard the information. It was concluded that because social media is publicly available, it does not mean people have to be publicly exposing their personal data on the platforms (Gruzd, Jacobson and Dubois, 2020, p. 10).

CPM theory could be applied in many fields including E-Commerce, Metzger (2007) has dedicatedly focused on CPM theory to investigate the regulation of privacy management when it comes to disclosing personal data like credit card information or email addresses (Metzger, 2007, p. 335). The study examines how and why users decide to reveal their personal information and it results in that the disclosure consists of both benefits and risks. The benefits of disclosing information are to develop self-expression, social control, and relationship development while the risks include losing control over something that should belong to them. It was said that users must balance their needs and disclosure for privacy, thus allowing users to know the best way of protecting personal information (Metzger, 2007, p. 336).

This study applies CPM theory to social media users to understand information disclosure in social media platforms, focusing on how people make use of their privacy in action while surfing in social media, thus, reflecting their privacy awareness. The CPM theory depicts users to balance both privacy needs and disclosure of information, for instance, users need to fulfil social needs while protecting their personal information in order to uphold their privacy. Third parties such as advertisers or researchers that use users' personal data provided by social media for their own benefit also have similar responsibility to guard the information from leaking. CPM theory leads us to erect boundaries whether what should be private and public, therefore control who has the right to control the information and set expectations for co-ownership of information. With this theory, we are able to measure how social media users regulate their private information and to what extent they are aware that their personal data is leaking to the unknown. It is theorised that CPM claims that individuals make decisions based on their desire to protect or disclose personal information. In this way, this research could discover the privacy awareness level of an individual by depending on the social media usage of the particular individual.

METHODOLOGY

This research concentrated on Malaysians aged between 18 to 29 years old that are social media active. The age range is selected because they have more mature and rational thinking according to research on psychosocial maturity (McCue, 2018). Besides, the researcher chose to focus on active social media users as they are exposing themselves more to social media, which it also means that accurate data can be obtained through this group of people. The research conducted mixed methods which are quantitative and qualitative methods.

An online survey method was used for a number of 100 respondents who are able to meet all the conditions stated above. Besides, the respondents must own at least one social media account as this study is related to social media privacy awareness and conducted using Google Form due to the Movement Control Order (MCO) to stay at home or work at home. Besides, an in-depth interview method is conducted to explore more detailed information about the person's thoughts and behaviours. With in-depth interviews, the respondents could have more opportunity and time to express their thoughts upon the issue of privacy awareness. Follow-up questions are asked based on the doubts remaining in the survey questionnaire

to offer a complete picture of the research objective. The interview was conducted one by one, and a total of eight people are participating in this interview by using Zoom Meeting due to the pandemic.

Google Form link was shared on various social media platforms such as Facebook, Instagram, and WhatsApp to reach the target audiences that are selected in the sampling process. The Google Form was closed once the results reached 100 respondents. Non-probability sampling was used in this study. Convenience sampling was adopted by finding respondents that are conveniently located around the researcher. In this sample, the researcher searched for respondents that are easy to contact or reach, thus confirming that the respondents are all qualified in the criteria needed for the study. If a respondent fails each of the criteria, he or she is eliminated from the study.

FINDINGS

It can be concluded that all respondents are eligible to participate in the study and be able to categorise them into different categories such as age, gender and education level. Among 100 respondents, 91 of them own more than three social media accounts. For the in-depth interview, it is known that four interviewees are from the 21-25 age group, two from the 18 to 20 age group and another two from the 26 to 29 age group.

It shows a high percentage of 75% of respondents use social media more than four hours a day and most of the respondents own more than three social media accounts which are mostly Facebook, YouTube, and Instagram. Results show most of the respondents spend half of their daytime using social media for entertainment purposes, keeping up with current events and staying connected with others.

Findings also indicate that respondents are willing to disclose career-related information they claim could help them to expand their career path and meet more new connections via social media.

> "I have noticed that sometimes employers like to find out about their interview candidates' social media profiles to kind of get a hold of what kind of person that they are dealing with. For example, platforms like LinkedIn are popular for employers to look at the profiles of their candidates. I have a lot of friends who were discovered by different businesses for a potential job opportunity through linked in." (Participant E)

> "I think career information is not personal but something that could be exposed to the public and would help in my career path, especially in searching jobs." (Participant F)

It is surprising that the results show a high number of people willing to disclose family information (44%) and financial information (23%). According to the interviewees, it could be concluded that respondents are of the opinion that social media is safe if respondents only allow friends they know to view on their social media. By exposing financial information, respondents claim they can attract more customers when the respondent uses social media as a business platform.

> "I only share hobbies and interests, so, I do not worry about privacy leaked out even if my account was set to the public." (Participant A)

> "Social media is a safe platform for me, as I just add friends from the person I know or close to me." (Participant C)

> "I use social media as a business platform for marketing purposes and will disclose financial information to let the public know how many orders and income, I had made this month to build the sense of trust from the public. I set it into a public account in order to promote my business on social media." (Participant B)

Majority of the respondents were very aware and extremely aware of their information being exposed on social media. They claimed that they have seen too much news reporting about cybercrimes, scamming or hacking incidents and most of them come with monetary or reputation damage.

> "Number of cybercrimes are actually increasing year by year, apparently after social media exists. It has given ground to the 'Malaysia Cyber Security Strategy 2020-2024' plan to build up in order to secure a better cyber environment as more people are relying on digital tech." (Participant A)

> "I am aware of it because I actually saw a lot of news regarding cyber crimes where people are being scams. And I have watched a documentary that talks about social media and privacy, so I am very aware of this issue." (Participant C)

Majority rarely realise how privacy gets invaded**.** Respondents claimed that social media tracks them instead of clearly knowing the exact way their information gets invaded by the platform.

> "I know that social media goes through data scraping to gather information from social media profiles, as well as other accounts. They track our data based on their systems." (Participant B)

> "Social media tracks my activities online like the products I had searched for or any posts I shared online. I think they invade my privacy by tracking online behaviour." (Participants C)

> "Social media will always recommend me to follow users who have similar followers or similar information as I do. For example, if a user goes to the same school or owns some mutual friends with me on the platform, the social media will display the user profile in the 'recommended friends' category. So, I believe that the back-end system does make use of my personal information but I'm not sure how." (Participant H)

65% of respondents rate themselves as extremely aware or very aware, indicating that they have a high level of privacy awareness. However, results still tend to show that although most of the respondents have a high level of privacy awareness, they are still not cautious enough to protect their privacy online. Respondents appear to be aware of the issue, but they do not know how it happens (with a prove of 47.9% within the 100 respondents, they do not know how social media invades users' privacy); they do not have the intention to find out why (with a prove of a high percentage of 67% within the 100 respondents, they do not know what to do when they experience privacy leakage), causing them to have an unsharp

opinion when answering the question. Besides, a high percentage (71% of respondents) do not take time to look at the privacy policies, as they claim that the terms and conditions are too lengthy and contain professional phrases that are hard to comprehend.

> "It is too long and too complicated, and you would not get a choice to agree nor disagree if you wish to use that platform." (Participant G)

> "I would spend time reading the policies but only scan through the first three pages as I always feel that all terms and conditions are the same." (Participant A)

With this, although the respondents claimed to be aware of privacy invasion and rate themselves as having a high level of privacy awareness, they do not have the intention to secure their privacy or even find out how the platform is invading their privacy, which leads to conflicting results due to the unsharp opinions of the respondents.

DISCUSSION

Communication Privacy Management Theory (CPM) that was proposed by Sandra Petronio has been used in this research. The theory helps to measure how social media users are regulating their private information on social media platforms and thus provides an understanding of how people regulate their private information in daily life. It also claims that individuals make decisions based on their desire to protect or disclose personal information. With this theory, CPM can bring attention to research to examine how respondents make use of their privacy in social media, therefore reflecting the privacy awareness of the respondents.

Referring to the findings, it shows that privacy awareness among respondents is high as they are aware that social media or some unknown parties would monitor or steal their information online. They are also regulating their private information by choosing what to disclose and what to keep within themselves. The respondents have made their decisions based on how much they are willing to disclose to the online platform. For example, interviewees tend to disclose their career information on social media because they believe social media could help them to expand their career and meet more new connections. They consider career information to be not personal but something that could be exposed to the public.

Besides, respondents who claim to have a high privacy awareness level believe that social media contains dangerous activities such as data scraping, online tracking and online behaviour studying on the users. However, for respondents who have a moderate or low privacy awareness level, they feel social media is a safe and secure platform and these people are willing to expose their information online as they think tragedy would rarely happen to them. In this way, it clearly reflects on the CPM theory that how individuals make use of their privacy is reflecting on their level of privacy awareness. Therefore, the findings have shown relevant to the theory which could be proved to be applicable to this research. It shows well implicated to the study which helps to discover the privacy awareness level of respondents by depending on the social media usage individually.

CONCLUSION

In a nutshell, this study has fulfilled the research objective and research questions which find out how social media spies on the users and how much do the users acknowledge it. Taking privacy awareness into consideration, it could help to raise awareness in the public about the importance and impact of privacy invasion. This study has concluded that the users' privacy awareness level is considered high, yet the users are not cautious enough to take action in protecting their privacy online and do not have the intention to find out why. The results also showed that the respondents are aware of the issue but ironically, it does not mean that they will take cautious action on it. With this, it leads to the target audience being unsharp in their opinion when it comes to the issue of sharing private information. However, many of the results are still related to the study, and it is well applied to the CPM theory.

Throughout the findings and discussion, there are a few suggestions and recommendations that could be applied to improve the study. First, a high percentage of respondents did not know how social media invades their privacy on social media, and a high percentage of respondents did not know what to do if they experienced privacy leakage. With this, social media could have provided more information to their users about what to do and the reason why. It is the social media's responsibility to ensure a good user experience with abundance of the user's knowledge. Social media could have many ways such as providing Public Service Announcement (PSA) on online crime or contacting users immediately through email or message when they notice unusual activities on their account. Besides, researchers should also provide a deeper insight into questions on the survey questionnaire to make sure respondents have deeper thinking processes and become sharp with their opinion when examining their privacy awareness level.

REFERENCES

Becker, M. (2019). Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology*, 21(1), 307-317. https://doi.org/10.1007/s10676-019-09508-z

Brooke, A., Lee, R., Anderson, M., Perrin, A., Kumar, M. & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bull Guard (2021). *Privacy violations – the dark side of social media.* https://www.bullguard.com/bullguard-security-center/internet-security/social-media-dangers/privacy-violations-in-social-media

Call, K. (2015). *Connected big brother: Are we being spied on online?* https://www.business.com/articles/connected-big-brother-are-we-being-spied-on-online/

Deniz, S. (2020). Is somebody spying on us? social media users' privacy awareness. In S. Kir (Eds.), *New media and visual communication in social networks* (pp 156-172). IGI Global.

Gilmer, M. (2020). *Nearly 90% of the world's internet users are being monitored*. https://sea.mashable.com/tech/7267/nearly-90-of-the-worlds-internet-users-are-being-monitored

Gruzd, A., Jacobson, J. & Dubois, E. (2020). Cybervetting and the public life of social media data. *Social Media + Society*. 6(2). https://doi.org/10.1177/2056305120915618

Heffernan, L.E. (2017, December 6). *Oversharing: Why do we do it and how do we stop?* Huffpost. https://www.huffpost.com/entry/oversharing-why-do-we-do-it-and-how-do-we-stop_b_4378997

Ho, K. (2019). *Malaysians spend almost a quarter of their day on social media.* YouGov. https://my.yougov.com/en-my/news/2019/04/30/malaysians-spend-almost-quarter-their-day-social-m/

Kaos, J. (2021). Cybercrime increasing as more people rely on digital tech during pandemic, says PM. *The Star.* https://www.thestar.com.my/news/nation/2021/06/28/cybercrime-increasing-as-more-people-rely-on-digital-tech-during-pandemic-says-pm

Kemp, S. (2020). *Digital 2020: Malaysia.* https://datareportal.com/reports/digital-2020-malaysia

Kemp, S. (2021). *Digital 2021: Malaysia.* https://datareportal.com/reports/digital-2021-malaysia

Khoros (2021). *The 2021 Social Media Demographics Guide.* https://khoros.com/resources/social-media-demographics-guide

Lewis, K. (2021). *How social media networks facilitate identity theft and fraud.* Entrepreneurs' Organization. https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Marcus. (2017). What happens if you sign a contract without reading it in Malaysia? *Ask Legal*. https://asklegal.my/p/what-happens-if-you-sign-a-contract-without-reading-it-in-malaysia

Marwick, A., Fontaine, C. & Boyd, D. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society,* 3(2), https://doi.org/10.1177/2056305117710455

McCue, J. (2018, January 22). *A parent's guide to why teens make bad decisions*. The Conversation. https://theconversation.com/a-parents-guide-to-why-teens-make-bad-decisions-88246

McGinness, A. (2021). *Anonymity on social media is Ending.* https://www.idmerit.com/blog/anonymity-on-social-media-is-ending/

McLeod, S. (2019). *What's the difference between qualitative and quantitative research?* https://www.simplypsychology.org/qualitative-quantitative.html

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2), 335-361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Nyoni, P. & Velempini, M. (2018). Privacy and user awareness on Facebook. *South African Journal of Science*, 114(5/6), 1-5. https://doi.org/10.17159/sajs.2018/20170103

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Petronio, S. & Child, J. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, 31(1), 76-82, https://doi.org/10.1016/j.copsyc.2019.08.009

Pixlee. (2021). *Why social media data collection is essential for marketing*. https://www.pixlee.com/blog/why-social-media-data-collection-is-essential-for-marketing/

Redmiles, E., Bodford, J. & Blackwell, L. (2019). "I Just want to feel safe": A diary study of safety perceptions on social media. *Proceedings of the International AAAI Conference on Web and Social Media*, 13(01), 405-416. https://doi.org/10.1609/icwsm.v13i01.3356

Sarikakis, K. & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media + Society*, 3(1), 1-14. https://doi.org/10.1177/2056305117695325

Scoglio, S. (1998). *Transforming privacy: A transpersonal philosophy of rights*. Praeger.

Singh, S. (2018). *Sampling techniques*. https://towardsdatascience.com/sampling-techniques-a4e34111d808

Smith, A. (2017, January 26). *Americans and cybersecurity*. Pew Research Center. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Southerton, C. & Taylor, E. (2020). Habitual disclosure: Routine, affordance, and the ethics of young peoples social media data surveillance. *Social Media + Society*, 6(2), 1-11. https://doi.org/10.1177/2056305120915612

Suciu, P. (2020, June 26). There isn't enough privacy on social media and that is a real problem. *Forbes*. https://www.forbes.com/sites/petersuciu/2020/06/26/there-isnt-enough-privacy-on-social-media-and-that-is-a-real-problem/?sh=3ced502444f1

The Financial Express (2020). *Privacy VIOLATION: After Facebook, Google is now in a soup over user privacy*. https://www.financialexpress.com/opinion/privacy-violation-after-facebook-google-is-now-in-a-soup-over-user-privacy/1981683/

Turner, J. J. & Amirnuddin, P. S. (2018). Social media privacy and the law: perspectives from Malaysian and UK consumers. *The Journal of the South East Asia Research Centre*, 10(2), 31-58.

Patel, D. (2020, May 19). The dangers of sharing personal information on social media. *Penn Today*. https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media

Wachtor, L. (2019). *Are more people public or private on social media?* Viasat. https://www.viasatsavings.com/news/blog/are-more-people-public-or-private-on-social-media/

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science, 1*(1), 3-20. https://doi.org/10.1515/opis-2017-0002