Data Security: Privacy Calculus on Social Media

Lee Fong Yee, Mohd Afizi Mohd. Shukran, Fatimah Ahmad

ABSTRACT--- Privacy breaches are rampant on social media and there are many cases of companies and users that have been hit tremendously. The study aims to explore the personal data disclosure and privacy concern over social media in Malaysia. Three focus groups of undergraduate students were conducted to explore the issues faced. The data collected from the focus group were transcribed into basic transcription and thematically analysed. The result shows that majority of the participants think of the social and financial benefits outweigh its perceived risks. The findings of the study will benefit all companies and users on social media which bring up the current critical situation of the privacy arguments and suggestions for improvement.

Index Terms--- Data breaches, data privacy, data security, privacy calculus, privacy-conscious, privacy paradox, privacy risks, self-disclosure, self-withdrawal.

I. INTRODUCTION

Malaysia Data Privacy is the main concern for users of online media nowadays since data breaches and issues of privacy are on the rise. Facebook (FB) is involved in a scandal of political data, about 87 million FB user data are garnered via a quiz application by the employed psychologist. He sold those user data to Cambridge Analytica and the users' details are allegedly used in Donald Trump's political election campaign [1].

Barkly reported 10 biggest data breaches in 2018, unexpectedly the largest data breach incident stated was not Cambridge-Analytica FB Scandal. Instead, it was ranked the fifth in the list. The largest scale of data breach was the incident of "Aadhaar", with a payment as cheap as 500 rupees (approximately RM28), the unidentified sellers provide service to access any Aadhaar number (unique 12-digit identifier) of citizen in India. By gaining access to the Aadhaar, the payer could also access personal data such as name, address, mobile number and e-mail; if the payer is willing to top up another 300 rupees (approximately RM17), an advanced access is granted to print any ID card with its Aadhaar number. The incident is believed to have leaked the personal details of 1.1 billion India citizens [2].

Since there are many major data breaches all over the world, many privacy regulations have been strengthened and enforced especially in Europe where the data privacy debates heat up. The General Data Protection Regulation (GDPR) governs personal data processing by individuals and companies or personal data organisation in Europe. According to "The Australian Financial Review", there are new cyber security laws were in force in China, Vietnam and Singapore; besides these, privacy and data protection laws are currently put into effects in Indonesia, Japan, Philippines, Malaysia, Singapore, South Korea and Taiwan. Some new privacy laws are reviewed by Asian countries such as India, Hong Kong and Thailand which particularly incorporate criminal sanctions; hence leaders of companies must be cognisant and vigilant when dealing with personal data [3].

After the revelation of the incident of the Cambridge-Analytica, FB has offered easy access to the privacy tools as follows: (i) Privacy settings menu on mobile devices will be easier to be found and located; (ii) Shortcut menu of privacy with simple taps are provided; (iii) More secure authentications are given; (iv) More control on personal data that allow user to control what to be shared; (v) Options are given to what advertisements to be presented to user; (vi) Controls are given on who can see the posts and personal profile; and (vii) Most importantly it allows you to delete unwanted content or even to remove your account permanently [4].

The aftermath of the Cambridge-Analytica FB Scandal is great impact,hashtag of "#deletefacebook" has been embraced by many users and businesses until now. They deleted their FB account for good [5]. Based on a United State's survey done by the Pew Research Center [6], there are 54% FB users who age 18 and older have changed their FB privacy settings in recent 12 months; 42% of the respondents have stopped checking their FB for few weeks or more; 26% of the respondents have already removed their FB accounts. The survey also reported that majority of the young adults have quit using FB after the incident of Cambridge-Analytica FB Scandal.

Social media users are now awakened to a higher state of data privacy-consciousness. As a wise user, it is crucial to learn and understand how the online companies collect, use and share its private data. In United States, public requests "rights to be forgotten" and citizen in Europe have petitioned the search engines e.g. Google and Yahoo to remove certain unfavourable results which include many wrong, irrelevant or excessive information about them. There are 250,000 takedown requests for Google in Europe, 840,000 links removal requests according to an online poll survey [7]. However, Google has only removed the results from Europe search engine database and the results are remained searchable outside the domain as Google disputed that it invades the right to free expression if they are to apply "right to be forgotten" globally [8].

Revised Manuscript Received on May 15, 2019.

Lee Fong Yee, Faculty of Communication and Creative Design, SEGi University, Petaling Jaya, Selangor, Malaysia.

MohdAfiziMohd. Shukran, Faculty of Defence Science and Technology, UniversitiPertahananNasional Malaysia, Kuala Lumpur, Malaysia.

Fatimah Ahmad, Faculty of Defence Science and Technology, UniversitiPertahananNasional Malaysia, Kuala Lumpur, Malaysia.

Even though online media users are aware of all the privacy risks; however, they do not know what do their data has been used by the third parties that are involved in the businesses. In other words, social media users are now more sensitive and careful when it comes to online personal data disclosure. Majority of the young adults in United States have already deleted their FB accounts since most of the online users are now privacy-conscious; however, it is important to explore how the Malaysian young adults react to the current data privacy issues and incidents.

II. METHODOLOGY

The study explores the user perception on the social media that is in related to personal data disclosure and privacy matters. The study answers the following questions:

RQ1: What are the perceived benefits of social media which the users are willing to disclose their personal data?

RQ2: What are the privacy concerns on social media?

Three focus groups are formed and each group consists of 6-8 participants. Participants are undergraduate university students in Malaysia who age between 18-23. They are the Generation Z and they are born in digital age where technology is already ubiquitous in their daily lives. The focus groups interview focuses on the two facets of their experiences on social media: (i) Perceived values or benefits gained and (ii) Privacy risks. The focus group interview questions are as follows:

1. What are the values or benefits of social media to you?
2. What is your privacy concern over social media?
3. How often would you read privacy policy of the social media?
4. Under what circumstances would you disclose your personal information in exchange of convenience or benefits gained from the social media services?
5. In overall experience, do you think the convenience gained or benefits gained on social media outweigh its privacy risks?

The focus group interview sessions are semi-structured, audios of the group conversation were recorded and consents are obtained from all the participants. Data collected are transcribed, coded, thematically classified and analysed with qualitative data analysis software.

A. Theme: Perceived Benefits

The types of social media used by the participants are FB, WhatsApp, Snapchat, Instagram, WeChat, SinaWeibo, QQ and Reddit. The activities on social media in their daily lives include sharing pictures, posts, videos, news, chatting, updating profiles, shopping, commenting on post, following social celebrities, and checking on how friends are doing. Besides these basic functions, participants inform that there are too many benefits and values using the social media.

A few participants use the social media as business platforms for years and they have their own FB business pages. They get benefits from many seller groups on social media and they get to advertise their products effectively on FB. They frequently update their profiles and posts for customers to check out the latest products and to make purchase order.

A participant follows his favourite local celebrities and job recruitment social group to secure a part-time job on social media. In a rare case, a participant told the researcher that he is in dire need to get blood and need immediate help and he manages to find blood donor by reaching out to his FB network. For some participants, social media is a great platform to maintain social relationships, meeting new friends and seeking for new social partners. A participant manages to reconnect to her long-lost primary school friend on FB.

A participant uses the social media for collaborative learning. For every group assignment, he usually creates a group on WhatsApp as it is convenient to discuss the tasks of assignments. Participants are able to get a lot of useful information from the social media group which helps them to complete their tasks efficiently and quickly. The social media also provides relevant linked information which improves social confidence and making the right shopping decision.

B. Theme: Privacy Concern

Few participants express the same opinions that they never buy anything from social media because they do not trust the information so much; instead, they will buy items from the official online shopping cart such as the biggest e-commerce website, namely Taobao. Few participants also shared their bad experiences especially their social media accounts are hacked and stolen. One of the participants is blackmailed by the hacker after his account is hacked.

When the participants are increasingly aware of the online data breaches, they feel insecure as they have no idea on how their personal data are given to and shared by third parties somewhere in the world. When personal data are sold to the business advertisers, users will often receive various promotions, newsletters and limitless advertisements; worst still, relatives and friends from the same network will also suffer from telecom fraud.

A few female participants have similar bad experiences; they are offended by strangers who are trying to chat with them even though they already expressed that they are not keen to make friends with those strangers. One of the female participants found it annoying when there are many men asking her if she wants to have sex on social media. There is a stranger who approaches one of the female participants on social media, he tried to flirt with her to suggest in a deeper relationship with her; he gives her sweet compliment and check her out whether she is single and asked her out on a date.

Participants found that the personalised recommendation such as product advertisements are annoying especially those products that they are not interested in. At times, it does get annoying when it keeps popping out on their screens.

A participant expressed her recent concern on getting weird strangers calling her and she has no idea where they got her number from. There is a stalker who she had a conversation with created in total nine Instagram accounts just to check on her and stalk her. She blocked him each time she realised he used fake

identity to stalk her on social media.

A participant considers data breach as a great threat to him as he usually gets spam messages, phone calls and e-mails. Worst still, if it affects his entire social network and they also suffer from this kind of frauds, he fears there may be possibilities that people are using his personal information for illegal activities.

C. Theme: Personal Data Disclosure

Many participants admitted that they will disclose their personal data in exchange of accessing the features of the social media and monetary related incentives offered to them.

"Yes, I would disclose my personal information in exchange of taking part in social media." (P8, line 886)

"I will disclose my personal data in exchange to stand a chance to win prizes." (P13, line 901)

"I applied a membership on an online shopping cart in order to get product discounts on my birthday month. I will definitely provide them my personal contact and information." (P2, line 479-481)

Minority of the participants are pleased with the personalised recommendation, they do not mind giving out their personal data in order to receive promotions or news updates of the products they like. However, participants were annoyed by frequent updates of the unwanted advertisement.

"For me, I love this kind of online personalised recommendation. Whenever I shop at Lazada, I also wish to see the products and stuff on my Facebook because it gives me more options and there might be more promotions and discounts on Facebook. On the other side, it might be a bad idea when you receive many advertisements that are not helpful and sometimes, I find it annoying." (P11, line 741-745)

Besides self-disclosure of personal information, user settings and preferences are stored in cookies. Google and FB use cookies in advertising. It bothers the participants as personalised advertisements are presented to them even though after they switched to different social media.

"I have to admit that I shared all of my personal information with Google. Therefore, I feel like sometimes, when have watched some video on YouTube and I check something on Instagram a few minutes later, it recommends me something I never searched on Instagram at all but I did watch related content on YouTube. What bugs me the most is how they listen and track my browsing history, it bugs me a little and this irritates me when it happens." (P8, line 683-688)

"Yes, I totally agree with P8 because I also experienced the same thing specifically games that I searched online… Whenever I go to Instagram and the advertisement is presented to me which is related to something I was looking for, so it is kind of weird in a way, but as what P8 said, it is not that something that I can be bothered with but it is still kind weird." (P11, line 689-694)

A few participants voiced out that they do not mind disclosing their personal preferences provided it is a trustworthy website.

"I will only give my personal information to website of big company and never give it out to small shady websites." (P8, line 844-845)

"It depends on where the products are being sold from e.g. Lazada. I will only disclose my personal details only to reliable websites. If it is a trustworthy website, I do not mind giving out my address and other personal information which enable me to enjoy more benefits from the services." (P11, line 864-876)

Participants who are privacy-conscious understand the consequences of personal data disclosure will lead to getting series of promotions over the phone and e-mail.

"When you give your personal information to a particular website, e.g. your e-mail, you will definitely expect them to send you stuff from time to time. Companies collected your e-mails and phone number through events. If you were to give them your phone number then you should expect phone messages on product promotions. Therefore, you should not blame on others or any system for privacy invasion because you voluntarily gave out your personal details in the first place." (P10, line 774-782)

A few participants pointed out that they will certainly would not give out their personal data if they suspect the discount offer is a scam or other kind of sneaky approaches to steal personal details.

"I would not disclose my personal data in exchange for products and services discounts on social media as I am quite skeptical about those offers. Sometimes, it is not real deal and I do not trust that information that much." (P7, line 467-469)

"I would only disclose my personal data if it is a genuine offer. Most of the time there are some sly marketing on social media and it may cause you pay more. It is better to think whether the discount offer is reasonable and realistic, e.g. If someone is selling a laptop at RM300 and the brand-new laptop from the official dealer is RM800, you definitely could smell that something is fishy and that is a catch. Do not buy it because it is a jaw-dropping cheap deal or you might fall into the trap." (P10, 859-863)

Minority of the participants would not simply disclose their personal data for product discounts or cash incentives.

"Generally speaking, I would not simply disclose my personal information on Internet even though they give me discount on products." (P1, line 485-486)

"I won't give out my personal data even though some companies offer me cash incentive in return.I know it is already happening, there are many free app and people do not need to spend a penny for the services and you should have already known that their personal information is being sold for cash to the third parties." (P8, line 962-965)

D. Theme: Privacy Paradox

Privacy paradox refers to online users claim to be very concerned about their data privacy but they behave contradictory to their privacy concern [9]. Participants voiced out their fear and concern on privacy issues; however, none of them have actually bothered to read and understand a privacy policy of social media.

"I usually do not read the privacy policy." (P7, line 345)

"There is too much information in the privacy statements." (P2, line 346)

"Reading the privacy policy is too boring to me." (P2, line 348)

E. Theme: Privacy Calculus

Privacy calculus theory suggests that individuals would share their personal details by weighing the risks and benefits [10]. The results of the study show that majority of the participants think that the benefits outweigh its perceived risks. Thus, participants are willing to trade their personal information for social and financial benefits. The results of the study are aligned with the results of the past studies [11], [12].

"For me, I think benefits on social media are definitely more, the pros are more than cons. But it really depends on you how to use it. If you keep giving out everyone your e-mail address, your password then your account is vulnerable to many scams and spams. It's your own fault to simply give out your personal details." (P14, line 1525-1528)

"I think the benefits and convenience gained through social media outweigh its privacy risks." (P7, line 545-546)

"For me, I think benefits offered by social media is greater than its risks." (P3, line 555-556)

"I think the benefits gained from social media have brought great convenience and benefits to my life. Although there will be leakage of privacy, it is only a few cases. Social media will strengthen its security and take measure to protect personal data. I think the benefits outweigh the risks." (P1, line 562-565)

F. Theme: Privacy Settings

Participants who are privacy-conscious will definitely adjust their privacy settings especially when it comes to who can see their contents. They also turned off the unwanted advertisements.

"This is very simple, we can turn off the notification on social media if we really don't want to see the recommended products and services." (P6, line 313-314)

"My friends and I like to adjust the settings on who can add us as friend. We like to hide our public profiles from people we don't know and only allows "friends of friends" to send a "friend request." (P4, line 447-449)

"For me, only people who are friends with me can see my profile, posts and comments. However, strangers can still look me up through my phone number and account name… As for my phone number, public can only access it if they are able to answer few security questions about me." (P1, line 453-458)

Besides, participants feel insecure if they are to show their phone numbers to public. A participant believes that if he is to show his house address to public, this may invite dangerous parties to his house and this may jeopardize his safety.

"I hide my phone number, it is vulnerable and dangerous if strangers get to know your phone number and they start calling you." (P13, line 825-826)

"I won't show my address, I am very insecure about people knowing my address. After all, it is a recipe for murder, robbery and that is not fun." (P13, line 827-828)

G. Theme: Self-Withdrawal

Participants vary in their responses to data breaches on social media. Some participants choose to maintain status quo; some participants have become more vigilant in sharing personal information; some participants choose to embrace "#deletefacebook" and remove their account for good.

Majority of the participants are still having faith on social media regardless of its perceived risks.

"Anyway, I will still use it regardless of the privacy risks on social media." (P7, line 362)

"I will continue using it even though there are cases of hackers, because I believe there are ways to stop these hackers." (P9, line 1029-1030)

"If my account were to be hacked, I would just change my password but I won't stop using the social media." (P13, line 1027-1028)

A participant states that he is taking a break until the social media come out with a countermeasure for the data leakage issue.

"I stopped using it for a while because I believe the social media companies will figure out what the problem is and make it right. The leakage of personal information could be quite scary, but I believe we should share only basic information on social media." (P9, line 791-793)

A participant is very privacy-conscious, he has reduced the frequency of using FB and he will only occasionally check it out for new updates on products.

"I've already stop myself using Facebook regularly. I only use it to check up new stuff occasionally. I started to refrain myself from it even before the scandal of selling personal information, I have already known that Google does invade our privacy too." (P8, line 788-790)

Majority of the participants also feel that popular services such as Google and FB have good functions; therefore, they will continue to use their services even their personal data were to be sold or used for consumer profiling.

"When it comes to Google products, I would not stop using their services." (P2, line 382-383)

"If it is Google or Facebook, I am not going to stop using it. Although my personal data has been exposed, their functions are too good and those cannot be replaced by other alternative applications." (P1, line 387-389)

Minority of the participants will choose to remove their social media accounts if they find out their personal data are sold to the third parties as they do not share too much information online.

"If it happens to me that my personal information is sold, I would probably delete the account and create another new account because I usually browse through the posts without posting much about myself." (P3, line 372-374)

"Yes, I would stop using it if my account is hacked or my personal data is leaked to other companies." (P4, line 587-588)

A participant voices out that if the privacy infringement causes him a financial loss, he will definitely stop using the social media.

"If my general personal information was leaked to third parties, it is fine. I am just worried if my payment information was stolen, in that case I will stop using it, I will just go offline." (P8, line 1033-1035)

Majority of the participants who are vigilant on social media do not put their private information, e.g. school name, phone number, id number and password online. Hence, they have nothing to lose if their personal data are leaked.

"Well for me, I do not mind because if my personal data was being sold. It's not a big deal for me since I only put up basic stuff about myself." (P11, line 799-800)

"I would not withdraw from social media if my personal data was leaked to third parties because I usually do not share much personal information." (P2, line 614-615)

III. CONCLUSION

This study explores the perceptions of Malaysian on privacy issues over social media. This study found out that the participants weigh the benefits and the perceived risk to determine whether to disclose personal information on social media. The result shows that majority of the participants believe that the social and financial benefits outweigh its perceived risks. All participants like to set the privacy settings on who can see their content and which advertisements should be presented to them. However, as compares to the United State's survey done by the Pew Research Center [6], participants in this study appear to be less resistant to use FB, only two participants would consider deleting their FB accounts and the other two participants have taken a break and reduce the frequency of checking on FB; majority of the participants would continue using FB and they are not influenced by the recent Cambridge-Analytica FB Scandal. Future studies to mitigate privacy concerns are related to (i) Studies privacy control settings to enhance the effectiveness of advertisements personalisation; (ii) Ignorance about privacy policy of online media and (iii) in-depth study on the self-withdrawal and reasons why FB users deleted their FB accounts following the #deletefacebook movement.

REFERENCES

1. T. James, Psychologist whose company sold users' data to Cambridge Analytica leaves Facebook. 2018, Available: https://www.telegraph.co.uk/technology/2018/09/06/psychologist-whose-company-sold-users-data-cambridge-analytica/.
2. D. Bisson, The 10 biggest data breaches of 2018... so far. 2018, Available: https://blog.barkly.com/biggest-data-breaches-2018-so-far.
3. N. Abraham, and J. Lennon, The Australian financial review - Nick Abrahams and Jim Lennon. 2018, Available: http://www.nortonrosefulbright.com/news/169094/the-australian-financial-review-nick-abrahams-and-jim-lennon?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.
4. E. Egan, It's time to make our privacy tools easier to find Facebook Newsroom. 2018, Available: https://newsroom.fb.com/news/2018/03/privacy-shortcuts/.
5. N. Peterman, Search Twitter - #deletefacebook. 2018, Available: https://twitter.com/hashtag/deletefacebook?lang=en.
6. A. Perrin, Americans are changing their relationship with Facebook. 2018, Available: http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.
7. M. Trujillo, Public wants 'right to be forgotten' online. 2018, Available: https://www.bsgco.com/insights/public-wants-right-to-be-forgotten-online.
8. S. Ghosh, Google is fighting a big, messy battle over whether expanding the 'right to be forgotten' amounts to censorship. Available: https://www.businessinsider.my/google-fights-european-court-right-to-be-forgotten-expansion-2018-9/?r=US&IR=T.
9. B. Brown, Studying the internet experience. 2001, Available: http://shiftleft.com/mirrors/www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.
10. M. Culnan, and P. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," Organization Science, 10(1), 1999, pp. 104-115.
11. E. Aguirre, A. Roggeveen, D. Grewal, and M. Wetzels, "The personalization-privacy paradox: Implications for new media," Journal of Consumer Marketing, 33(2), 2016, pp. 98-110.
12. M. Culnan, and R. Bies, "Consumer privacy: Balancing economic and justice considerations," Journal of Social Issues, 59(2), 2003, pp. 323-342.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication