International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020
ISSN: 1475-7192

Online Privacy Literacy (OPL) and Privacy Management Behavior (PMB) Among University Students in Malaysia

[1]Dr. Wan Puspa Melati, [2]Hafizul Amin, [3]Ayeshah Aqilah

Abstract*—Cybersecurity issue is exacerbated in the current trend towards Industry 4.0 with its design of interconnection between machines, devices and people through the Internet of Things (IoT) or the Internet of People (IoP). To ensure the safety of users and to devise action plan, it is imperative for policy makers to first understand the level of awareness and behavioral pattern of its users. The current research surveyed 180 university students in Malaysia using the Online Privacy Literacy Scale [OPLIS] created by Masur, Teutsch, and Trepte (2017). The aims of this research paper are 1) What is the online privacy literacy level among university students and 2) In what ways do university students engage in online privacy management? Based on the findings, it was found that online privacy literacy level is generally low among university students especially on the dimensions of knowledge about institutional practices and knowledge about technical aspects. However, the students were found to engage in general privacy management behavior, but not taking additional preventive measures. Suggestion on innovative and inclusive module for online privacy literacy and privacy management behaviour has been proposed to better inform and protect these students in the inevitable participation of the virtual world.*

***Keywords*—** *Online Privacy Literacy (OPL), Privacy Management Behavior (PMB), Cybersecurity, Online Privacy Literacy Scale (OPLIS), University Students*

I. INTRODUCTION

In this digitalization era, the information that is being shared online is constantly circulated beyond boundaries. It is a concern for some users especially those who are conscious of the information sharing processes and what information are accessible to others which in turn may be abused for personal gain or for malicious intent. Between 2005 and 2011, it has been reported that the users privacy-concerned behavior has increased especially on Facebook and other social media platforms (Stuntzman, Gross & Acquisti, 2012). Eventhough the users on Facebook do have

[1] Affiliation, SEGi University, Malaysia
[2] Affiliation, SEGi University, Malaysia
[3] Affiliation, SEGi University, Malaysia

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

control on their Facebook account privacy settings, there are possibilities that the information users shared online can be accessed and privacy settings compromised due to the open network features. Facebook is known for its role in gathering massive data from its users for third party applications and avertisers through one's browsing patterns and social media interactions such as "clicks" performed by users (Grimmelmann, 2009)

Search engines such as Bing, Yahoo, Ask.com and Google also collect various information about its users by applying the technique call 'Spidering'. According to howstuffworks.com (2018), spidering technique is a wonder of technology where it helps the internet search engines to collect data about web sites and web pages as to display in response to search request. This is why users are able to have links on the web pages and how other web pages are linked to users' accounts. It is extremely useful in getting one's website found by the search engines. The main reason of this features is to create personalized user experience and beneficial for companies to increase revenue by producing marketing strategies in relating to the users' interests. However, the downside is that information that those company can attain are those from simple personal data to wide-ranging history of users' searches and devices used to login.

The dilemma to date is, despite the knowledge of how vulnerable online users are, heavy reliance on digitalization especially entering the industry 4.0 is inevitable. This is more pressing for younger generation who are considered as the digital natives and view technology and digital world as part of the their own lives (Howe & Strauss, 2000; Palfrey & Gasser, 2008; Solove, 2008. As a consequences, children and teenagers are under increasing surveillance at home and school, facilitated by Internet filters, mobile phones, and other monitoring technologies (Berson & Berson, 2006; Hope, 2005).

II. LITERATURE REVIEW

Online Privacy

The concept of privacy need to be discussed before one can further discuss on online literacy and behavior. The term privacy has been extended from the famous idea of the right to be let alone (Warren & Brandeis, 1890) and the right to control information of oneself (Westin, 1967). According to Westin (1967), privacy can be defined as

> [C]laim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or smallgroup intimacy, or, when among larger groups, in a condition of anonymity or reserve (p.24).

Every individual has their own preferences when it comes to disclosing their personal information online but these preferences are also constrained with the requirements and stuctures of applications these days. When registering account for social media for example, the users are unable to avoid disclosing personal questions such as name, home adrress, age, phone number, email address, occupation, work address and the like. In fact, when users accidentaly missed out some questions, they will not be able to proceed with registration of the social media account or applications

and unable to use its features. Scholars have also highlighted that many users are unable to differentiate between the concept of privacy and the right to privacy (Solove & Schwartz 2009).

A literature review by the Harvard Berkman Klein Center (2013) argued that young adults or students are concerned about their privacy, especially keeping information from their parents. Therefore these young adults still share their information online but would select the audiences and what information to be made public via privacy settings available on applications used. A recent Pew Research study supported this by highlighting that the issue of privacy is more of a concerned among young adults than the elders and that the young adults tend to use filtering features and more careful in their selection of the access towards their posts. However, the issue of fake accounts used by others to gain access to information or stealing of personal data is still an issue that is prevalent due to non-selectiveness of online posts by these young adults.

Online Technology

The concerns over new technologies can be divided into three categories: (1) monitoring and tracking, (2) dissemination and publication, as well as (3) aggregation and analysis (Nissenbaum, 2009).

The first category includes the widespread monitoring facilitated by surveillance technologies such as closed-circuit television systems (CCTV), RFID tags, electronic toll collection, facial recognition systems, marketing (Andrejevic, 2007; Monahan, 2006; Turow, 2006). These technologies are used by both governments and private companies to perceive and track the behavior of individuals and larger populations. Second, the spread of computer technologies, communication networks, and digital information has shaped an environment in which personal details are more readily available than ever before (Cullen & Reilly, 2007; Palfrey & Gasser, 2008). It is common for people to disclose, knowingly or unknowingly, personal information online. Third, aggregation and analysis involving large databases are increasing the possibility that individual privacy may be invaded in new and more substantial ways. The increasing use and dissemination of personal information creates a "Kafkaesque world of bureaucracy, where we are increasingly powerless and vulnerable, where personal information is not only outside our control but also subjected to a bureaucratic process" (Solove, 2004, p. 35).

Thus, both these area of studies then point towards the question of to what extent do the young adults or students are concerned about their privacy online, know about their online privacy and what do they do in the effort to manage online privacy. These are the focus of this study that will be further discussed in the following sections.

III. METHODOLOGY

For the purpose of this study, quantitative method was used to quantify attitudes, knowledge and behaviors. E-survey was used for the data collection method by using Google documents. Links were shared to 17 institutions, selected randomly and constituted both public and private universities. 180 respondents partook in this survey.

The questionnaire has been developed to answer the research questions: 1) What is the online privacy literacy level among university students and 2) In what ways do university students engage in online privacy management?

There are three sections for this questionnaire, namely; Section A, which include demographic data; Section B which tap into online privacy literacy, and Section C which covers privacy management behavior.

Section B was adapted from Online Privacy Literacy Scale [OPLIS] created by Masur, Teutsch, and Trepte (2017). However the content of knowledge on protection law was modified to suit the Malaysian setting. Some of the sentences were also edited to make it more direct and better understood for our study population.

Section C was adapted from study by Weinberger, Bouhnik & Zhitomirsky-Geffet (2017). However, only 12 items were selected which are relevant for this current research.

SPSS software was used for data analysis of this study.

IV. FINDINGS

The 180 respondents studied in this research are predominantly female (67%), the majority of them are between 21 – 24 years old (62%) and currently are studying their bachelor degrees (67%). In terms of race, the majority of them are of Malay decent (62.8%) followed by Chinese (18.3%), Indian (12.2%) and other racial categories (6.7%). These students are from 17 institutions which include both private and public institutions.

These respondents generally reported that their computer or internet proficiency level is average (66.7%). Only about 27% of them reported that they are highly proficient, 6% of them confessed of low proficiency and with less than 1% of them claimed that they are not proficient at all.

In terms of perceived online safety, about 66% of them believe that the internet in somewhat safe, followed by those who claimed that it is safe (19%). There are about 13% of them who claimed that internet is unsafe and 1.7% of them claimed that internet is very safe. It is found that majority of these respondents are either highly concerned of protecting their personal information online (46%) or moderately concerned (33%). About 21% of them are slightly concerned and 1.1% of them are not concerned at all.

Online Privacy Literacy Knowledge level among University Students

It is found that the university students have low level of knowledge about online institutional practice which accounts for 63% of the sample. Only 12% of them falls into the category of high level of knowledge as shown in Table I below.

TABLE I. knowledge level on institutional practice

Item	Knowledge about Institutional Practices		
	Level of Knowledge	**F(x)**	**%**
PRA 01-05	Low	114	63.3
	Moderate	44	24.2
	High	22	12.2

A similar trend was also found in regards to the technical aspects of privacy management in which the majority of the respondents were found to have low level of knowledge (42.2%) followed by moderate level (29.4%) and high level (28.3%). The data is as per summarized in Table II below.

TABLE II. knowledge level about technical aspects

Item	Knowledge about Technical Aspects		
	Level of Knowledge	**F(x)**	**%**
TEC 01-05	Low	72	42.2
	Moderate	53	29.4
	High	51	28.3

Table III shows that the respondents are divided into those who scored low in regards to knowledge on data protection law in Malaysia and those who scored high in their knowledge – they account for about 40% each category.

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

TABLE III. knowledge level on data protection law

Item	Knowledge on Data Protection Law		
	Level of Knowledge	**F(x)**	**%**
GES 01-05	Low	72	40.0
	Moderate	35	19.4
	High	75	40.6

TABLE IV. knowledge level about data protection strategies

Item	Knowledge about Data Protection Strategies		
	Level of Knowledge	**F(x)**	**%**
STR 01-05	Low	56	31.1
	Moderate	37	20.6
	High	87	48.3

Contrasting data were found in regards to knowledge on data protection strategies as summarized in Table IV. Almost half the respondents were categorised as possessing high level of knowledge regarding the data protection strategies (48.3%). This is followed by those who scored low which accounted for 31.1% of the respondents studied.

Reported Behavior that University Students Engage in Privacy Management

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

TABLE V. reported privacy management behavior

Item	Reported Privacy Management Behavior		
	Behavioral Statements	**M**	**SD**
1	I use simple passwords so I can remember them	2.67	1.040
2	I use "save password" option to ease my online log in	2.51	1.165
3	I always change my log in password	2.19	1.003
4	I am willing to pay for services that will guarantee the protection of my personal information	2.69	0.965
5	I tend to read the "privacy policy" statement before proceeding with my online activities (browsing, downloading etc)	2.44	1.031
6	I tend to download software and content that is important to me even from unfamiliar websites	2.50	0.966
7	I tend to do online shopping	3.02	0.969
8	I am willing to share my personal details on social networks application to get messages and services that customizes to my personal interests	2.28	0.992
9	I use online banking services only to check my balance	2.93	1.078
10	I tend to use the same password for all of my online activities	2.68	1.000
11	I tend to open "pop-ups" even though I am unsure how safe they are	1.81	0.979

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

Item	Reported Privacy Management Behavior		
	Behavioral Statements	**M**	**SD**
12	Generally I will do all I can to protect my information security	3.45	0.772

Based on the Table V, the findings show that on average, the respondents claimed that they disagree on the following statements which is important towards ensuring their online privacy management - They do not use simple passwords (M=2.67, S.D.=1.040), they do not save password to ease log ins (M=2.51, S.D.=1.165), they do not use the same password for all online activities (M=2.68, S.D.=1.000), they do not tend to download from unfamiliar websites (M=2.50, S.D.=0.969), they are not willing to share personal details on social networks just to get messages and services that customizes their personal interests (M=2.28, S.D.=0.992), they do not open "pop-ups" even though they are unsure how safe they are (M=1.81, S.D.=0.979). They have also claimed to generally do whatever they can to protect their information security (M=3.45, S.D.=0.772).

However, these respondents also engaged in the following behavior that may compromise their privacy management, without much realization. They claimed that they do not tend to change their log in password regularly (M=2.19, S.D.=1.003), they are not willing to pay for services that guarentee protection of persoanl information (M=2.69, S.D.=0.965), they do not read the "privacy policy" statement before proceeding with online activities (M=2.44, S.D.=1.031), they tend to do more than just checking banking balance (M=2.93, S.D.=1.078) and even engage in online shopping (M=3.02, S.D.=0.969).

V. DISCUSSION

The data presented above provided useful insights and vital information on online privacy literacy and privacy management behavior among the respondents. Similar to what was previously argued, the respondents of this study also show high concern towards their online safety. This may reflect in their relatively high knowledge on privacy management behavior and even agree to have engaged in basic means to secure their privacy management online.

However, the authors would like to draw the attention to the low level of knowledge on how institutions practice their data protection online whereby he respondents mainly answered "Do Not Know" for most of the items from who can have access despite our privacy setting to the processes through which the information is being handled by these organizations.

Similarly, on the technical aspects, the respondents do not know the related basic terms and what it does. The lack of knowledge is a concern and perhaps this is why the majority of the respondents claimed that internet is a relatively safe place.

On the up side, the findings also reveal that though the respondents are unsure of the concepts of internet technologies and data sharing, most of the respondents are careful when it comes to password creation and download practice. They also do not save their passwords for all online activities or save their log in details, among other efforts.

The concerns of the authors surround the issue that the respondents tend to not read their privacy policies before using any applications or registering onto any sites, do not change password regularly and engage in various online activities which involve payment gateways. All these activities can make these students susceptible to the threat of cybersecurity that they may not be aware of.

VI. CONCLUSION & RECOMMENDATIONS

Based on the data obtained from 180 university students in Malaysia, the findings provided an important insight on how they perceived online privacy, their knowledge level and what type of privacy management behavior they engaged in. It is evident that majority of them are concerned about their online privacy and engaged in some basic ways to maintain their privacy. However, some behaviors that may compromise their privacy have not been carried out perhaps due to their lack of knowledge on the institutional practices and technical aspects of online privacy.

Internet has become a necessity for the millennials in their daily life and they spend a growing amount of their time online, hence they depend on internet almost on everything. Because of that they are more confident to share their privacy online although they are not sure with the consequences. Since the usage of technology and embarking on digitalization is inevitable for these students, merely controlling or hindering them from using will lead to more disadvantages onto these youth than guiding their embrace.

It is recommended that this realization and knowledge would propel parents, educationists, policy makers and civil societies to encourage for more exposure and educational programmes instead to better equip these students. Educating the students on the technical aspects of how the computer networks and system works would allow a more critical mind of these students and to be more aware of their usage risks. Providing the knowledge on how institutions works and even legal aspects are all important information that all users should be aware of. The repercussion of the lax mentality should also be further discussed even at the elementary phase of education.

Future researches can include larger sample size and include an in-depth interview or focus groups with respondents to further complement this research findings. Stratified sampling would also be useful to compare the different groups of respondents as well as to infer to the population at large. More analysis is planned to further establish the validity and reliability of these measures.

Received: 03 Dec 2019 | Revised: 21 Jan 2020 | Accepted: 18 Feb 2020

ACKNOWLEDGMENT

Alhamdulillah and praise to Allah for this opportunity and for providing us guidance and strength to complete this research. We would also like to express our deepest gratitude to SEGi University for sponsoring and organizing the International Conference on Industry 4.0 : A Global Revolution in Business, Technology & Productivity as this is a platform that is timely and supportive of academicians to contribute towards academic endeavor. We would like to also thank members of our faculty, FoCCD, for their constant support and encouragement that enabled the smooth running of this research and report writing. Lastly, we would like to thank all of the respondents who had taken their time in providing useful information and partaking in this study.

REFERENCES

1. Stuntzman, F., Gross, R. & Acquisti, *A.* (2012). Silent Listeners: The Evolution of Privacy and Disclosure on Facebook, 4 J. *Privacy & Confidentiality* 7, 8–9.

2. Acquisti, A., John, L. K. & Loewenstein, G. (2012). The Impact of Relative Standards on the Propensity to Disclose, *Journal of Marketing Resolution*, 49, 160 -172

3. Acquisti, A., John, L. K. & Loewenstein, G. (2011). , Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Resolution*, 37, 858-864

4. Leon, P. G. et al. (2013). What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers, Symppsium On Usable Privacy and Security 9.

5. Birnbaum, M. H. (2000). SurveyWiz and FactorWiz: JavaScript Web pages that make HTML forms for research on the Internet. *Behavior Research Methods, Instruments, & Computers*, 32(2), 339-346

6. Cho, H., & LaRose, R. (1999). Privacy issues in

7. Internet surveys. *Social Science Computer Review*, 17(4), 421-434.

8. Abril, P.S. (2008). A (My) Space of One's Own: On Privacy and Online Social Networks. *Northwestern Journal of Technology and Intellectual Property*, 6(1), 73.

9. Acquisti, A. & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Lecture notes in computer science, 4258, 36–58.

10. Addington, L.A. (2009). Cops and Cameras: Public School Security as a Policy Response to Columbine. *American Behavioral Scientist*, 52(10), 1426-1446.