

Assessment of Personal Information Shared by Facebook Users

Jeanky Salenga-Mendez ^{a*}

^{a*} Holy Angel University, Philippines

Abstract

Few studies that document Filipino users' understanding, practices, experiences, and coping strategies in relation to their Facebook privacy setting. The aim of this study was to find out about the respondents' (1) privacy behaviors, (2) knowledge and privacy concerns, and (3) experiences and coping strategies. The majority of respondents typically disclosed their basic details, such as their real full name and real photos with their birthdays, gender, educational history, and hometown, according to the results. The respondents also mentioned that they are aware of Facebook privacy settings and privacy adjustments. The study also revealed that the majority of respondents had not had any unpleasant experiences with Facebook, but had only heard stories about privacy settings that made them suspicious of their personal details and settings. The researchers used a descriptive study design to verify the results based on the participants' feedback. A survey will be used to gather data from Facebook users' personal details that they have shared in their accounts. Finally, the results of this study show that the respondent has generally good practices and a wide range of knowledge and coping strategies, but further action is required to raise their awareness and develop other practices that could threaten their protection. CCS Concept: Software and its engineering □ Software creation and management □ Search-based software engineering □ Recommender System, Collaborative Filtering, Usability..

Keywords: Facebook, Awareness, Privacy settings.

1. Introduction

Facebook is a platform for social networking, where users can post comments, share photographs and post news links or other relevant content on the web, talk live and watch short video [16]. Facebook turned into a simple tool for socialization, presenter of personal identity, and a tool for network building of the users in their everyday life. FB's main purpose is to inspire people to share and to make the world more accessible and connected. It was launched on 4 February 2004, by Mark Elliot Zuckerberg.

In the news, posted last January 3, 2019, inquirer.net, Facebook's breach of privacy may have been pushed a bit too far, the growing attention on privacy issues is being driven by various cyber security attacks that have led to massive personal data breaches. Also, it was reported in the news that Facebook shared user information with partners like Microsoft, Netflix, and Spotify that they gave personal data more intrusive access than previous ones. It allows them to read and delete private messages, as well as see someone on a message thread and view friends list without the consent of the real FB account owner. This is precisely the reason why data privacy is imperative to the Facebook users because a breach of personal information can damage an individual's rights and freedoms, including the chance of identity theft and the other types of scam [10].

Previous studies have shown that general knowledge of the unseen aspect of Facebook, such as media reporting/coverage and live video uploads on Facebook, has a significant on self-disclosure and understanding privacy issues. Self-disclosure awareness will address the question of how much personal information should be released and how you should react when other people post it on their page. In Padyab [2], Facebook users

need to aware of how to manage personal information from other people as each time a friend shares something they have to determine whether to share it and how to share it. Users of the FB may accidentally share personal information from others when posting their content. Privacy awareness is described as the degree to which users on the Online Social Network (OSN) are informed about privacy issues, breaches, and procedures.

Information privacy also known as data privacy is one feature of information technology (IT) that contracts with the ability of an organization or individual user to determine what data or information in a computer system can be shared with third parties [23]. Data privacy is concerned with the proper management of data that deals with consent, notice, and regulatory obligations of each user. Particularly, data privacy focuses on whether or how data is shared with third parties, how data is legally collected, stored and shared, regulatory restriction such as General Data Protection Regulation (GDPR), National Privacy Commission (NPC), or Health Insurance Portability and Accountability Act (HIPAA).

In the article of NortonLifeLock [17], data is one of the most significant assets of any organization as data use grows, companies find tremendous value in the collection, sharing and use of data as transactional data is increasingly valuable for businesses, allowing them to achieve flexibility and optimize their operations for the highest quality outcome. Now, if the data are in wrong hand bad things may happen to the user's accounts owner, such as: (1) breach at a corporation can put proprietary data in the hands of a competitor; (2) personal data sharing that can be used by another user for personal intention; and, (3) a breach at school student's information in the hands of the criminals who could commit identity theft. However, with the widespread use of the internet and the popularity of social media such as Facebook, WhatsApp, Instagram, and Twitter the data-sharing possibilities are exceptionally enormous.

Social media is a computer-based application that enables the exchange of ideas, feelings, and knowledge through virtual networking and community building. Uploading and sharing content such as personal information, videos, and images via computers, tablets, or smartphones over web applications or websites [9].

The majority of Filipinos are internet users and the Philippine Internet population uses over 80 percent of social media. In the research of Universal McCann's 2008 Wave four (4) studies on social media finds that the Philippines has the highest penetration of social networking among Internet users of 83%. Filipino online users prefer using Facebook over Twitter, Tumbler, and Pinterest among others, with 92% having a profile and with women as the most active users [4].

Nonetheless, FB users who do own their account in any social media identify the user's information – the person's right to control information about him or her. In the context of social media, this refers to a person's selective control over who accesses his/her personal information, which viewed, who uses, including contact details and personal communication, and control over the contexts in which information can be shared and be used [17].

However, one of the essential parameters of privacy awareness is the users' expertise on the application in customizing and changing privacy settings to restrict the information they receive and to protect their account protection. Therefore, users' should know how to setup their privacy settings for their own advantage. In addition, Facebook users should know the privacy policies that FB is introducing to increase understanding of their rights and privileges and the implication that could result from this.

First, privacy threats such as psychological distress, unwanted spam communications or junk emails and misuse of personal information have increased the degree of privacy issues, which is why data privacy education needs to increase young adolescents awareness and knowledge of technical solutions, such as setting up a junk email filter or strict privacy settings on social networking sites as a straightforward solution. Setting up a junk email filter or using tight privacy settings on social networking sites will allow young adolescents to monitor what personal information is revealed to whom, when, and under what situations.

Lastly, the use of a social media website, without the complete and proper knowledge and awareness about its privacy and issues, safeguards, policies, limitations will lead to innumerable privacy violations. Despite its popularity, there are also several risks for Facebook's younger users.

This research is essential to university students and employees. For them to know that apart from the social advantages of these social networking sites, more than sufficient use of the web will pose potential hazards for their private lives. It will also allow them to guide and raise awareness of privacy setting and proactive coping strategies in relation with privacy issues with their Facebook account.

2. Review Related Literature

Information technology advantages communication through instant messaging, emails, voice and video calls, and people all over the world have enjoyed the benefits of using technology nowadays despite long-distance,

race, and even religion [24]. Now, by using online social networking platforms like Facebook, Instagram, Twitter, and so on, these obstacles will no longer hinder the flow of data, information, and awareness in much easier, cheaper and much more effective ways.

In Khan [1], with all of the cloud computing successes, security in data privacy remains a crucial problem in the cloud computing paradigm. Such issues include the loss, leakage, and disclosure of privacy of user’s secret data such as health and financial data.

Data privacy is defined as the “right to be let alone”. Privacy threats affect not only law and computer science but social, psychology, and economics [5]. Information protection or data privacy is a data security division concerned with the proper handling of data relating to how information or data should be handled based on their relative importance. In addition, data privacy refers to individuals the ability to monitor or exert some power over their own data.

In the article of Nyoni [18], the following criteria are formulated as ideal behaviors for users to be completely aware of their own privacy:

2.1 Personal Information on Social Media Disclosure

Data is important in any kind of transaction. Facebook users provide and complete their personal data information by offering specific personal details such as name, address, birthday, images for a profile picture (optional), and contact details before the user will have a personal account. The information can be disclosed by the FB users and can be classified into two categories: a.) personal information, such as data includes their complete names, nicknames, schools, place of birth, birthdate, information from work, email address, and so on. This information is given a hint for the combination of the personal identity to be used as their password and username similarly in guessing their bank details, b.) Location, FB has features for geolocation and geo-tagging it is a method or technique for identifying a person's or devices' geographic location via digital information transmitted over the Internet in real-time activities of the FB users. Although for some, accountability and accessibility may be relevant, the risks of geotagging should now be apparent, providing constant public location notifications, exposing users to unauthorized users who know their locations [4].

The article posted by securedatarecovery [20] states those users 'loss of personal information will result in some undesirable consequences such as snooping and cyber-stalking and identity theft. For instance, providing personal information in using another website that may trick the user into volunteering entering personal data.

2.2 Social Media Sites: Facebook User Activity and Access

At the beginning of this year, the Philippines have a total population of over 100 million, and 46% of the population is engaged in using the Internet. Facebook users in the Philippines statistics show that there are more female users than men. As of January 2019, there were 74,850,000 Facebook users which considered 68.6% of its entire population, and the majority of them were women with a percentage of 52.6%. In addition, aged 18 to 24 years of age has a great size in the group of user (25,000,000) [15].

Based on the diagram FB users can connect with friends and family, play games, exchange content over the network, along with many activities, the statistics show the most activities as of September 2016 [25]. The "like" button had been identified as the most common Facebook features used as of the first quarter of 2016. It's about 80 percent of worldwide FB users reported using the "like" button in just one month. Other common activities involving using FB include watching a video, reading a post, one-to-one chatting or group chatting with friends, and reading new stories.

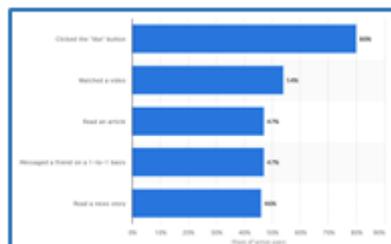


Figure 1: Facebook: most popular user activities 2016

(Posted by: statista2020, Retrieved March 29, 2020, from (statista.com, 2016))

2.3 Third-Party Content on Facebook

In Debatin [7], user perception on Facebook subscription with their privacy settings are aware of restriction to “friends-only” despite-off, students are still uploading and sharing a lot of personal information including uploading personal images with families. According to the study of Deng & Tavares students using Facebook have a blend of both socialization and learning functions within the universities. On the perception of the students, Facebook is an important platform in communicating and sharing information from their school, including seeking help. Also, for the students, it is natural for them to create posts, share information, and conduct an online discussion on Facebook [8].

In Conger [22], the model presented the personal information privacy (PIP) on the new technologies and privacy issues addresses that it includes not only transactional data gathering, the model provided Personal Information Protection (PIP) on emerging technology and privacy issues tackle the fact that it requires not only transactional data processing, but also organizational data exchange with the aid of new technologies such as radio frequency identification chips commonly known as RFID, geographic positioning or GPS, and smart notes. In addition, one of the categories defined by these parties as theft is the use of intentional, unauthorized, and often unethical and illegal users resulting in data leakage and loss. These are users who steal and leak other users' names, email addresses, and personal information without asking permission to the owner of the data.

Furthermore, Facebook announced information on a hacked attack that more than 50 million users have been affected by a stolen access token. The access token is the equivalent of digital keys that hold users signed into Facebook so that they do not have to re-enter the main user's password. The effect of stolen access is that the attackers already managed and used a portion of the victim's list of friends, the attackers also accessed the name and communicate with friends, as well as viewing the username, gender, relationship status, hometown, birthday, people recently tagged in, website visited, people or pages they followed and the user 's recent searches. Following a thorough investigation by the NBI and Facebook's management security team, they gave assurances to the users affected that they would receive a notification of the attack [22].

Privacy in social media sense is less known and has resulted in growing cases of privacy violations occurring in online spaces directly commenting on the Facebook wall and using an account's privacy credentials. Facebook founder and CEO Mark Eliot Zuckerberg are facing various issues with abuse such as election interference and misinformation campaigns. Last January 4, 2018, the CEO guaranteed to hit a solution multitude of Facebook security and data privacy issues [17].

The innovativeness and actions taken by the Philippine government to upsurge the level of awareness of users in social media, the government enacted the Data Privacy Act (DPA) of 2012 also known as the Republic Act No. 10173. It is the law that promotes, standardize, and monitor data privacy compliance of both Government and Private Institutions. Also, data privacy can be defined as the want of every user to control or influence information one's self [6]. Also, the National Privacy Commission (NPC) was set up to look and impose the DPA 2012. The NPC is regulated by a privacy commissioner and chairman, and two deputy privacy commissioners having these laws mandates all private organizations and government agencies that have 250 or more employees and with more than 1,000 personal data.

In the study of Velstsos [27], discussion of Facebook scams that a picture of sick babies alerted lots of users about the prank images. The Facebook quick response by taking down the offending images and explained why it was needed for their deletion:

“In addition to Facebook’s regular ongoing improvements to our automatic spam detection systems, we are looking specifically at these types of violations and how they can be more quickly and efficiently taken down. We are very aware of the baby charity scam issue and are looking at some technical solutions that will make their removal quicker and more comprehensive” [21].

Evidence of user details being made available exist for example, in the news by the CNN Philippines last December 30, 2019, at 11:55: 04 AM it was stated that the Cyber Security Philippines – CERT warned Filipinos against opening “malicious” greetings on Facebook messenger on the holiday season. The CERT team stated that once the message is open it will redirect into a different website that will ask the users to enter their personal information and that will lead to access to their data CNN [14].

Another attacked from hackers; a man allegedly hacked Facebook account of a woman last November 04, 2019, and asked her close friends for money to pay medical bills. The hacker allegedly logged in an unauthorized way to a woman's social media account and tried to collect money from friends by sending multiple links from a phishing website and stole the victim's Facebook account user ID and password. On the victim's statement she cannot log in to her Facebook account anymore and cannot retrieve some friends [26].

Considering the article Pappas [19] about “Social Media Cyber Bullying Linked to Teen Depression” says that victims tend to agonize in silence, it is hard for the parents to identify and address what problem they are facing, these are suffering from Cyberbullying on a social media. Furthermore, online youth victims have received a higher degree of attention, particularly after a series of high-profile teenage suicides that were allegedly harassed on different networks.

Looking at the statistical result of the students were bullied by the National Center for Education Statistics (NCES) of the Philippines over 1 in 5 students (21%) reported being bullied during the school year, that is considered over 5 million youth annually for the record [13]. It was also stated that youth who are bullied are at chances of risk for depression, lower academic records, anxiety, sleep difficulties, and dropped out of schools.

3. Research Questions:

This research study aims to assess the personal information that is shared on their Facebook account; the researcher main question is as follows:

1. How many FB users account be described in terms of:
 - a. Personal characteristics; and,
 - b. Personal information shared?
2. How many users with FB accounts are aware of privacy settings?
3. What are the FB user’s experiences related to Privacy Violation?
4. What are the FB user's coping strategies after having encountered an issue?

3. METHODS

A descriptive research design, particularly, a survey, will be utilized in collecting information from FB users’ personal information shared in their FB accounts.

3.1 Sample and Setting

The study focuses on the privacy characteristics of the social networking site Facebook, with limitless audience on every social media network but the content is always permanent. Participants of the study are coming from a private university school in central Luzon. Employees and/or students can post a photo, upload files, change profile pictures or get tagged in another and delete it quickly, but someone still be able to archive the page or make a copy and this could threaten their career and job. The social networking site Facebook will use because of its popularity among other social networking and easy access among users. In particular, Quota sampling will be considered a non-probable sampling technique, in selecting the sample. The respondents are divided into three (3) groups: the non-teaching personnel (NTP), faculty, and the students, targeting at least 100 for each. Quota sampling methods are commonly used nowadays because they are fairly easy to implement and can be easily performed. Additionally, the researcher can easily group the respondents with similar characteristics in proportion to their population size by using a quota sampling technique [12].

3.2 Survey Instrument

The researcher used the online form, which are the google forms for easy access to allow respondents easy to reach and use. Prior to distribution of the questionnaire the researcher send a copy via email to check the content by two (2) IT Specialists on their field of expertise in data security and privacy network. The researchers seek advice to the expert to verify the content in relation trying to answer the purpose of the study. Also, the questionnaire was validated by a research expert/statistician by profession to check for potential risks including psychological and emotional risks. The online survey consists of 35 questions and divided into two parts, demographics and question appertaining to the most common information FB users are comfortable in sharing based on FB’s account settings prompt [7].

3.3 Data Collection

Permission shall be sought from the University President, through Human Resource Management Office, to be allowed to float the instrument to the prospect sample. A survey questionnaire uploaded on an online base platform for ease in distribution. A google form is a web-based app used to create forms for data collection the data to be gathered is typically stored in a spreadsheet. The advantages of an online survey that it is easier can be self-administered and can reach anyone and everyone [3].

3.4 Data Analysis

A descriptive statistical tool is used to analyze the data: frequency and percent for categorical data and mean, standard deviation, median, interquartile range, minimum and maximum values for quantitative data. The actual sample is divided into subgroups that are: non-teachers, faculty, and students. The online survey was available within 30 thirty (30) days.

4. Results And Discussion

The survey respondents were mostly female (*f* 155; 51.67%) with an average age of users of 31, ranging from 18 to 60 of age. Half of the respondents were over 20 and a graduate of a college or higher with (*f* 179; 59.67%) in [Table 1] reveal.

Table 1. Personal Characteristics/Information of the Study Participants (n=300)

| Item | <i>f</i> (%) |
|---------------------------------------|--------------|
| Gender | |
| Male | 145 (48.33) |
| Female | 155 (51.67) |
| Age | |
| <i>Mean</i> | 31.32 (31) |
| <i>Median</i> | 30 |
| <i>Mode</i> | 20 |
| <i>Standard Deviation (SD)</i> | 10.93 |
| <i>IQR</i> | 18 |
| <i>Variance</i> | 119.37 |
| <i>Range</i> | [18, 60] |
| <i>Minimum</i> | 18 |
| <i>Maximum</i> | 63 |
| Category (Department) | |
| Faculty | 100 (33.33) |
| Non-Teaching (NTP) | 100 (33.33) |
| Students | 100 (33.33) |
| Highest Educational Attainment | |
| Associate Degree | 3 (1) |
| College graduate or higher | 179 (59.67) |
| College undergraduate | 59 (19.66) |
| Elementary graduate | 1 (0.33) |
| High school | 9 (3) |
| undergraduate | 9 (3) |
| | 40 (13.33) |

Junior high school 0
graduate
Senior high school
graduate
Vocational / Technical
Courses

Table 2, reveals that with a total of 278 respondents, the majority of those respondents own their account for 3 years or more among those are students. However, few of the respondents have one or less than two years of their account.

Table 2. Years/months Facebook was created

| Category (Department) | 1 year to less than 2 years | 2 years to less than 3 years | 3 years or more | 6 months to less than 1 year | Less than 6 months | Total |
|-----------------------|-----------------------------|------------------------------|-----------------|------------------------------|--------------------|-------|
| Faculty | 2 | 2 | 93 | 1 | 0 | 98 |
| Non-Teaching (NTP) | 3 | 7 | 88 | 1 | 1 | 100 |
| Student | 2 | 0 | 97 | 0 | 0 | 99 |
| Total | 7 | 9 | 278 | 2 | 1 | 297 |

In factors of knowing the times while checking their Facebook account indicate in table 3 that the majority of respondents 162 total visit their FB page more than five times a day and are mainly students with 61 respondents and half of them are the faculty and non-faculty.

Table 3. Times checking Facebook account

| Category (Department) | 1 to 3 times per month only | 2 to 3 times a day | 4 to 5 times a day | at least 4 times a month but not daily | at least once a day | more than 5 times a day | Total |
|-----------------------|-----------------------------|--------------------|--------------------|--|---------------------|-------------------------|-------|
| Faculty | 0 | 19 | 16 | 3 | 11 | 51 | 100 |
| Non-Teaching(NTP) | 2 | 20 | 13 | 0 | 14 | 50 | 99 |
| Student | 2 | 5 | 16 | 8 | 8 | 61 | 100 |
| Total | 4 | 44 | 45 | 11 | 33 | 162 | 299 |

Approximately 95 respondents in total answered that over 1 hour of their time spent on FB page amazingly, most of them are faculty and few of the respondents said they visit their account for about 11 to 15 minutes illustrated in table 4.

Table 4. Time spent each visit

| Category (Department) | 11 to 15 minutes | 16 to 30 minutes | 31 minutes to 1 hour | 5 minutes or less | 6 to 10 minutes | more than 1 hour | Total |
|-----------------------|------------------|------------------|----------------------|-------------------|-----------------|------------------|-------|
| Faculty | 11 | 13 | 21 | 7 | 5 | 43 | 100 |
| Non-Teaching (NTP) | 11 | 24 | 18 | 13 | 10 | 24 | 100 |

Assessment of Personal Information Shared by Facebook Users

| | | | | | | | |
|---------|----|----|----|----|----|----|-----|
| Student | 14 | 17 | 20 | 7 | 12 | 28 | 98 |
| Total | 36 | 54 | 59 | 27 | 27 | 95 | 298 |

It shows in the presentation of the data in table 5 that the most frequently reported personal information in the FB account of the respondents were gender (240) mainly the students, birthdate (185) and hometown (176) half of the number said yes for each category, personal interest (177) each group almost coordinately said yes, and similarly to educational history (204). Nevertheless, respondents do not disclose their relationship status (154), which will support in disclosing of their interest to men, or women (225) and their political views (242) with nearly same results for each category, religious views (191) predominantly said no by the faculty and few of them are NTPs, email address (213) nearly same result by faculty and NTP likewise with phone numbers (241), and home address (221).

Table 5. Types of Personal Information Revealed in the FB Profile (n=300)

| Category (Department) | Gender | | Relationship | | Interest Men/Women | |
|--------------------------|-----------|------------|--------------|------------|-----------------------|-----------|
| | No | Yes | No | Yes | No | Yes |
| Faculty | 32 | 68 | 47 | 53 | 77 | 23 |
| Non-Teaching (NTP) | 21 | 79 | 38 | 62 | 69 | 31 |
| Student | 7 | 93 | 69 | 31 | 79 | 21 |
| Total | 60 | 240 | 154 | 146 | 225 | 75 |

| Category (Department) | Birthdate | | Hometown | | Political Views | |
|--------------------------|------------|------------|------------|------------|--------------------|-----------|
| | No | Yes | No | Yes | No | Yes |
| Faculty | 44 | 56 | 50 | 50 | 79 | 21 |
| Non-Teaching (NTP) | 37 | 63 | 30 | 70 | 80 | 20 |
| Student | 34 | 66 | 44 | 56 | 83 | 17 |
| Total | 115 | 185 | 124 | 176 | 242 | 58 |

| Category (Department) | Religious Views | | Email address | | Phone Number | |
|--------------------------|--------------------|------------|---------------|-----------|--------------|-----------|
| | No | Yes | No | Yes | No | Yes |
| Faculty | 70 | 30 | 75 | 24 | 85 | 15 |
| Non-Teaching (NTP) | 58 | 42 | 72 | 28 | 81 | 19 |
| Student | 63 | 37 | 66 | 34 | 75 | 25 |
| Total | 191 | 109 | 213 | 86 | 241 | 59 |

| Category (Department) | Home Address | | Personal Interest | | Educational History | | Work Information | |
|--------------------------|-----------------|-----------|----------------------|------------|------------------------|------------|---------------------|------------|
| | No | Yes | No | Yes | No | Yes | No | Yes |
| Faculty | 82 | 17 | 50 | 50 | 39 | 61 | 43 | 57 |
| Non-Teaching (NTP) | 68 | 32 | 39 | 61 | 36 | 64 | 41 | 59 |
| Student | 71 | 29 | 34 | 66 | 21 | 79 | 71 | 29 |
| Total | 221 | 78 | 123 | 177 | 96 | 204 | 155 | 145 |

It was found that the respondents signed up to FB using their real full name with a total of 184 and frequently is students. Followed by using their nicknames with the same number to 21 responses from faculty and NTP. In addition, few replied that they only use their first name shown in table 6.

Table 6. Signed-up name

| Category (Department) | First Name only | Made- up Name | Nickn ame | Real Full Name | Total |
|--------------------------|-----------------------|---------------------|--------------|----------------------|-------|
| Faculty | 9 | 11 | 21 | 59 | 100 |
| Non-Teaching (NTP) | 9 | 10 | 21 | 60 | 100 |

| | | | | | |
|---------|----|----|----|-----|-----|
| Student | 18 | 0 | 17 | 65 | 100 |
| Total | 36 | 21 | 59 | 184 | 300 |

Table 7, 278 of the respondents said yes to the uploading feature for the profile picture by posting a photo of themselves or with friends with almost the same amount coming from the NTP and the students.

Table 7. Uploaded picture of self or with others

| Category (Department) | No | Yes | Total |
|-----------------------|----|-----|-------|
| Faculty | 13 | 87 | 100 |
| Non-Teaching (NTP) | 2 | 96 | 98 |
| Student | 5 | 95 | 100 |
| Total | 20 | 278 | 298 |

Concerning FB privacy practices, Table 8 shows that most respondents (252) said they were aware of the privacy setting on the FB page on the data below, showing the same number of response among group.

Table 8. Familiarity with Facebook privacy settings

| Category (Department) | No | Yes | Total |
|-----------------------|----|-----|-------|
| Faculty | 18 | 82 | 100 |
| Non-Teaching (NTP) | 17 | 83 | 100 |
| Student | 13 | 87 | 100 |
| Total | 48 | 252 | 300 |

As shown in Table 9, most respondents (235) made their privacy change on their FB page these are the students and faculty while the NTP (63) responses that they protect and adjust their privacy settings.

Table 9. Protection of profile/privacy adjustment

| Category (Department) | No | Yes | Total |
|-----------------------|----|-----|-------|
| Faculty | 14 | 86 | 100 |
| Non-Teaching (NTP) | 37 | 63 | 100 |
| Student | 14 | 86 | 100 |
| Total | 65 | 235 | 300 |

Presentation in Table 10 indicates the privacy setting practices on their FB account. To protect their personal profile more than half (164) make their profile only visible to friends and (136) apply various settings. Only (105) respondents said their FB privacy settings were changed immediately upon their account creation, while (194) learned how to change the privacy settings when they found out how to do it. Nearly half (155) of the respondents said they made the change as they were just vigilant while the rest changed their FB privacy settings because they heard distressing stories.

Table 10. Data privacy practices at FB

| Category (Department) | Way to protect personal profile | | Since when the privacy setting was adjusted | | |
|-----------------------|---------------------------------------|---------------------------------|---|---|----------------------------|
| | Different settings for my FB profile. | Profile visible only to friends | When created my FB account | When figured out how to adjust the settings | Generally a careful person |
| Faculty | 43 | 57 | 38 | 62 | 50 |
| Non-Teaching (NTP) | 38 | 62 | 38 | 61 | 51 |
| Student | 55 | 45 | 29 | 71 | 54 |
| Total | 136 | 164 | 105 | 194 | 155 |

| Category (Department) | Reasons to adjust privacy settings |
|-----------------------|--|
| | Heard alarming stories about FB which do not have private settings |
| Faculty | 48 |
| Non-Teaching (NTP) | 48 |
| Student | 46 |
| Total | 142 |

Some experiences related to privacy violations who have personally experienced problems on stalking or harassment and unwanted advances in FB majority answered no 169 while knowledge of other persons encountered problems in the profile is 218 Also, respondents who personally experienced gossip or rumors on profile majority said no is 183 while knowing other people that their data have stolen is 236 as shown in table 11.

Table 11. Experiences leading to data violations

| Category (Department) | Personally encountered problems in profile | | Knowledge of other person encountered problems in profile | |
|-----------------------|--|-----|---|-----|
| | No | Yes | No | Yes |
| Faculty | 44 | 53 | 22 | 78 |
| Non-Teaching (NTP) | 73 | 24 | 41 | 59 |
| Student | 52 | 48 | 19 | 81 |
| Total | 169 | 125 | 82 | 218 |

| Category (Department) | Personally experienced gossip or rumors on profile | | Knowledge of another person that their data is stolen | |
|-----------------------|--|-----|---|-----|
| | No | Yes | No | Yes |
| Faculty | 57 | 43 | 16 | 84 |
| Non-Teaching (NTP) | 71 | 29 | 29 | 71 |
| Student | 55 | 45 | 17 | 81 |
| Total | 183 | 117 | 62 | 236 |

Lastly, table 12 represent the respondents' most common approach to cope with FB privacy breaches is to limit their profile 231. Few numbers from respondents 23 would fix the issue by canceling their FB account while 46 would do nothing to address the issue.

Table 12. Possible actions of there are problems encountered in Facebook profile

| Category (Department) | I cancelled my Facebook account | I didn't change anything | I restricted my profile and privacy settings | Total |
|-----------------------|---------------------------------|--------------------------|--|-------|
| Faculty | 19 | 7 | 74 | 100 |
| Non-Teaching (Office) | 10 | 12 | 78 | 100 |

| | | | | |
|---------|----|----|-----|-----|
| Staff) | | | | |
| Student | 17 | 4 | 79 | 100 |
| Total | 46 | 23 | 231 | 300 |

This research aimed to establish the privacy behaviors of the users, knowledge of privacy concerns, and coping approaches and experiences relevant to privacy issues faced by the respondents on Facebook. It revealed that most respondents have had their accounts for over three years and normally spend more than an hour each time they visit their accounts. Furthermore, it is found that the respondents typically include their basic information such as gender, birthdate, hometown, personal interest, educational history, use their real name for their accounts, and uploading their photo for their profile image. The same was pointed out by Debatin [7] that this is natural, user's show they want to maintain a tenuous and intimate relationship with other people they have met in their lives. However, the results revealed that the respondents usually protected their accounts by different measures such as including only friends they know and have heard of personally because they are wary of their security.

In terms of awareness on privacy issues, the study found that most respondents said they were aware of the privacy settings of Facebook. A small number of respondents suggested they were protecting their Facebook profiles or changing their privacy settings. Nearly half of the respondents used various ways to secure their accounts in adding different settings, and more than half making their profile available only to friends. It also supports the ideas on the Ibrahim, Blanford & Berthouze [11] study, that Facebook's privacy settings give users value to protecting their personal details.

The study shows that most respondents did not experience any negative experiences such as unwanted bullying advances, threats, gossips and rumors, and identity theft. Nevertheless, there are still many who have had such unpleasant experiences. According to the Debatin [7] report, respondents typically learned about these adverse encounters, which could have frightened them and altered their actions towards protecting their privacy. Some of the respondents also limit their profile and privacy settings to deal with Facebook privacy breaches, but a small number of respondents have decided to do nothing or cancel their Facebook account.

Lastly, the research has found that the majority of users do not seem to understand that limiting access to their personal information does not sufficiently resolve the threat resulting from the amount of data they provide. After all, restricting the exposure of profiles to friends simply means restricting it to the visible portion of your group. In addition, based on the research findings, privacy awareness, and coping technique in dealing with data breach using Facebook most of the respondents would be more vigilant about their own privacy protection after being alarmed by hearing stories about privacy settings.

5. Conclusion

In this study, it can be concluded that students are more exposed to Facebook rather than those who work as faculty and non-teaching personnel. However, despite that student are more frequently visiting their Facebook account, the results showed that those who are working as a faculty spends more time every time they visit their Facebook account. Students also are more revealed on their gender, birthday, educational information, and their interests. Surprisingly, some of the respondents, which include students, teachers, and non-teaching personnel -- which most of them -- revealed their home address knowing that it could be seen by strangers. Most of the non-teaching personnel are revealing their work information also. In the past two months, there are a lot of Facebook dummy accounts that have been noticed by the public and it has the same names as the other people too. In terms of names revealed on the Facebook account, most of the respondents revealed the real full name in their account, especially students. Almost all of the respondents are aware of the Facebook privacy settings, however, there are still some people who do not even familiar with it, which is more of them are working as a faculty. An alarming finding also is that more of the students and faculty have experienced unwanted advances in their account. Restriction of personal account is the most picked choice by the respondents in terms they experienced any problem with their privacy in their account.

References

[1] Abdul Wahid Khan, M. I. (2012, May). *A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing*. Retrieved from https://www.researchgate.net/publication/235769884_A_Literature_Survey_on_Data_Privacy_Protection_Issues_and_Challenges_in_Cloud_Computing

- [2] Ali Padyab, A. S. (2016). Facebook Users Attitudes towards Secondary. *Thirty Seventh International Conference on Information Systems*.
- [3] Bhat, A. (2019). *questionpro*. Retrieved April 29, 2019, from questionpro.com: <https://www.questionpro.com/blog/data-collection/>
- [4] Brutas, K. (2015, October 30). Social Media and Privacy: The Philippine Experience. 1.
- [5] Celina Rebello, E. T. (February 18, 2018). Big Data Privacy Context: Literature Effects On Secure Informational Assets. *Big Data Privacy Context: Literature Effects On Secure Informational Assets*.
- [6] Ching, M. D., Fabito, B. S., & Celis, N. J. (2018). Data Privacy Act f 2012: A Case Study Approach to Philippine Government Agencies Compliance. 1.
- [7] Debatin, B. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Facebook and online privacy: Attitudes, behaviors, and unintended consequences*.
- [8] Deng, L., & Tavares, N. J. (2013). Moodle to Facebook: Exploring students motivation and experiences in online communities. *elsevier.com*.
- [9] Dollarhide, M. (May 2019). Social Media Definition. *Social Media Definition*, 1.
- [10] Facebook Data Privacy Issues: Facebook Shared Your Private Messages With Its Partners. (2019, January 3). *Facebook Data Privacy Issues: Facebook Shared Your Private Messages With Its Partners*. Retrieved from <https://usa.inquirer.net/17723/facebook-data-privacy-issues-facebook-shared-your-private-messages-with-its-partners>
- [11] Ibrahim, S., Blanford, A., & Berthouze, N. B. (2012). Privacy Settings on Facebook: Their Roles and Importance. *The 2012 IEEE International Conference on Green Computing and Communications*.
- [12] Mathstopia. (2020). Quota Sampling.
- [13] Meier, M. (2019, November). *Bullying, Cyberbullying & Suicide Statistics*. Retrieved from meganmeierfoundation.org: https://meganmeierfoundation.org/statistics/?gclid=EAIaIQobChMI843Lq-fc5gIVEA4rCh3YNQhOEAAAYASAAEgKpGvD_BwE
- [14] (n.d.). Retrieved from <https://cnnphilippines.com/news/2019/12/30/Holiday-greeting-Facebook-Messenger.html?fbclid=IwAR3SpjnnAqQH65yAkC3JhurQPFkil28YDsOwzFgEiMFbObg0Gut7PHTjyo8?fbclid>
- [15] [NapoleonCat. (2019, January). *stats*. Retrieved from napoleoncat.com: <https://napoleoncat.com/stats/facebook-users-in-philippines/2019/01>
- [16] Nations, D. (March 29, 2019). What is Facebook? *Learn why so many people can't stay away from Facebook*, 1.
- [17] NortonLifeLock, W. for (Ed.). (n.d.). What Is Data Privacy and Why Is it Important? Retrieved December 30, 2019, from <https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html>
- [18] Nyoni, P. (2014). AN EMPIRICAL INVESTIGATION ON STUDENTS' ONLINE PRIVACY. *AN EMPIRICAL INVESTIGATION ON STUDENTS' ONLINE PRIVACY*.
- [19] Pappas, S. (2015, June 23). *social-media-cyber-bullying-linked-to-teen-depression*. Retrieved from scientificamerican.com: <https://www.scientificamerican.com/article/social-media-cyber-bullying-linked-to-teen-depression/>
- [20] *Personal Data Loss - A Guide to Identity Theft*. (2019, January 2). Retrieved from securedatarecovery: <https://www.securedatarecovery.com/resources/personal-data-loss-a-guide-to-identity-theft>
- [21] Protalinski, E. (2012). Facebook admits it needs to fight scams more efficiently.
- [22] Rodriguez, S. (2018, October 12). Facebook Says Hackers Were Able to Access Millions of Phone Numbers and Email Addresses. Retrieved from <https://www.cnn.com/2018/10/12/facebook-security-breach-details.html>

- [23] Rouse, M. (2019, November). *TechTarget*. Retrieved from search.techtarget.com: <https://searchcio.techtarget.com/definition/data-privacy-information-privacy>
- [24] Samat, M. F. (November 2018). A REVIEW ON SOCIAL MEDIA USAGE AMONG STUDENTS. *KONVENSYEN KEBANGSAAN PEMIMPIN PELAJAR, At UNIVERSITI TEKNOLOGI MARA CAWANGAN KELANTAN*.
- [25] Statista2020. (2016). *Facebook: most popular user activities 2016*. Statista Research Department.
- [26] Telangana Man Allegedly Hacked Woman's Facebook, Asked Friends For Money. (2019, November 4). *Telangana-News*. Retrieved from <https://www.ndtv.com/telangana-news/telangana-man-allegedly-hacked-womans-facebook-asked-friends-for-money-2127057>
- [27] Veltsos, D. C., Veltsos, D. J., & Wells, D. M. (2012). An Exploratory Study of a User's Facebook Security and Privacy Settings