CRAWFORD JOURNAL OF BUSINESS & SOCIAL SCIENCES (CJBASS)
VOL. X NO.1, SEPTEMBER 2020:
ISSN 2141-9094; website: www.cjbasscru.org

Privacy Concerns Of Facebook Applications Users: Perception Of Babcock University Undergraduates

By

Mofoluke Ibidunni Akoja[1]
Mass Communication Department, Babcock University
Ilishan-Remo, Ogun State
akojam@babcock.edu.ng, 08038313899

Eyitemi Adrian Doyle[2]
Mass Communication Department, Babcock University
Ilishan-Remo, Ogun State

Mobolude Abolarin[3]
Information Resources Department, Babcock University
Ilishan-Remo, Ogun State

Abstract

The use of Facebook applications, especially among young people, has continued to increase on a daily basis. Among other things, the issue of privacy of users in terms of amount of information requested from users, as well as the safety of such information, has continued to generate a lot of concerns among communication stakeholders. One of the major reasons why these concerns are raised is the issue of lack of awareness and insufficient concern of the privacy issues which these applications expose users to. The study therefore looked at the extent to which Babcock University undergraduates are aware and concerned about their online privacy while using the services of Facebook. Two theories provided theoretical justification for this study including privacy calculus theory and communication privacy management theory. The quantitative survey research method was adopted. From a population of 9,180 Babcock University undergraduates, a sample size of 368 was determined with the Cochran formula while the respondents were selected through the simple random sampling technique and fishbowl method. Using questionnaire as the data collection instrument, data were collected from the 359 copies of the questionnaire that were properly filled and analysed with descriptive statistical tools such as simple percentage calculation as well as frequency counts. Findings showed that in spite of the intense use of Facebook applications among the undergraduates, they do not take active steps to safeguard their privacy online, although they are aware of some of the privacy issues. For example, only 37% agreed that they were actually concerned about their privacy while using these Facebook applications. The study recommends that users take the proper steps to safeguard their privacy on Facebook applications by being cautious of the kind of information they reveal online or share with friends especially on the Facebook applications while also avoiding the installation of third-party applications from Facebook applications.

Key words*: Facebook applications, privacy, concerns, privacy calculus theory, perception*

1. Introduction

Social media have been integrated into the lives of people and business organisations so much so that they appear to have evolved almost into a cultural phenomenon. Facebook has had many more acquisitions than others making it a powerhouse amongst social networking sites with over 2 billion users (Reiff, 2020). As a result of its numerous acquisitions and market expansion drives, the company has had a significant amount of privacy issues levied against it, given its large user base (Newcomb, 2018). The fact is that threats from insufficient online security are diverse and affects everyone irrespective of their background. Most of the time people associate these threats with the government (government surveillance and spying) and it is then disregarded because they say to themselves that they have nothing they are trying to hide (Tytyk, 2018).

1.2 Statement of the Problem

Over 2 billion people worldwide utilize Facebook services and this is not just the *Facebook* app but Facebook messenger, Instagram which as of June 2018 succeeded in having over 1 billion active users including WhatsApp with over 1.5 billion active users (Newcomb, 2018). Since its launch, Facebook has had a plethora of privacy issues one of which happened over ten years ago. Everything a user does on Facebook applications or any web site that is affiliated with Facebook and has a Facebook 'like' button shares a user's information with Facebook (Nield, 2017). Facebook monitors both users and non-users and use their private information often times without permission for profit by selling it to advertisers under the guise of creating an intuitive user experience (Yurieff, 2018). In 2018, Facebook revealed that the profiles of almost 2 billion users may have already been breached by hackers taking advantage of the company's lax data sharing policies (Isaac & Frenkel, 2018).

Even if a user is not on Facebook or have never created an account, a user would be using at least one of its other social media like *WhatsApp* or *Instagram*. Unfortunately, people often do not think twice about divulging their personal information on these social networking sites. Facebook, being so involved in people's lives, has even been accused of moulding opinions of people when it launched its infamous newsfeed which was seen as biased and manipulative. Although the founder Mark Zuckerberg had made efforts to reassure users of the fact that it does not sell users information to advertisers indiscriminately, the sincerity of this position is quite subjective given the fact that a large portion of Facebook's profit comes from advertising (Yurieff, 2018). Due to these reasons, this study examined the level of awareness of privacy issues on Facebook applications and extent to which Facebook company users among Babcock University undergraduates are concerned.

1.3 Objective of the Study

The study investigated the:

1. level of awareness of privacy issues on Facebook applications among Babcock University Undergraduate users.
2. extent of concerns of Babcock University undergraduate users on the privacy of Facebook applications

2. Literature Review

2.1 Facebook Company: An Overview

Facebook Company is a social network owned by Mark Zuckerberg; an American media magnate. Zukerberg founded Facebook from his dormitory room in Harvard University in 2004

at the young age of 19. The site was designed to allow users connect and share with family and friends online. Facebook remains one of the five largest American tech companies with over 2 billion active users that keep expanding as recent data shows that during the coronavirus pandemic lockdown, the company has become a go-to communications tool (Forbes, 2020; BBC.com, 2020).

Facebook company within this context refers to not just the *Facebook* application but also *WhatsApp (*a free messenger application for smartphones that uses the internet to send messages, audio, video, calling and video chatting), *Instagram* (a photo and video sharing social networking service which also includes messaging) and *Facebook Messenger* (formerly Facebook Chat but in the last quarter of 2018 was made a standalone messaging app that was free to download for iOS and Android) which are also owned by Facebook.

Ever since its inception, *Facebook* has constantly had to deal with issues of privacy. Newcomb (2018) provides a timeline of these privacy issues. Recalling that on September 5, 2006 *Facebook* launched newsfeed which was a centralised area within the application where users could browse through to see the updates and activities of their friends. Over 1 million users joined "Facebook News Feed protest groups", complaining that it was too intrusive, but the protests died down and *Facebook* still has its newsfeed. In December 2007, companies were able to track the purchases of *Facebook* users and notify their *Facebook* friends of what had been purchased, without the user's consent. In November 2011, Facebook agreed to undergo an independent privacy evaluation for the next 20 years. Regulators stated that *Facebook* falsely claimed that third party apps only accessed the data that they needed to operate but in reality, these apps could access nearly all of a user's personal information. By June 2013, a bug was discovered by a White Hat hacker revealing emails and phone numbers of over 6 million Facebook to anyone who only had a piece of their contact information. Facebook quickly removed that feature offline claiming that it had fixed it.

July 2014, Facebook conducted a mood-manipulation experiment on more than half a million randomly selected users. This was done by altering their news feeds to show more positive or negative posts to show how emotions could spread online. Facebook issued an apology and the experiment was taken offline. February 2018, a Belgian court told Facebook to stop tracking people across the entire internet. This was done through the use of online cookies to track Belgians illegally, even tracking non-Facebook users that might have gone on a Facebook site. The court asked Facebook to comply or risk being fined 100 million euros.

From the foregoing, there appears to be more than an assumption of the privacy issues associated with the use of Facebook, there are evidences that there are concerns which users need to take more seriously.

i. Privacy

Aptly defined, privacy is the right to "being let alone". Guided by this, it may be said that privacy is something that one has as long as people, organisations or institutions do not have undue access to one's private life. However, this notion, inspired mainly by the idea of physical boundaries, sees itself confronted with insuperable difficulties in an age where the debates' focus lies squarely on information privacy (Hauser, 2015).

Privacy transcends just a physical right of an individual because in contemporary times there is another realm of privacy and that is online. In this study, privacy specifically refers to the safeguarding of a person's information online. This is where information privacy becomes very vital because internet users want to be involved with the internet and its many attractions. No

one wants to be left behind in the social realm. Information privacy is a right by a person to have a degree of control over how his personal information is collected and used (IAPP, 2019). According to Belyh (2015), computers are everywhere and there is no aspect of our lives that remain untouched by them. Privacy of information is very vital in the current digital age with the interconnectedness of every facet of life. It has therefore become a necessity to safeguard any personal information that may be gathered by an organisation from being accessed by third parties. Privacy is not about whether or not you have something to hide but rather it is a right that one has to keep anything one deems private out of the sight of others and also prevent the unlawful access, sharing and or viewing of your information no matter its form or nature.

Islam and Jahan (2015) further state that an important aspect of privacy is the ability to exclude others from the premises. The right to be free from intrusion or interference is a key element of privacy. According to Techopedia (2020), internet privacy is the level of security and personal data that is sent through the internet. It is a general term that refers to a variety of factors that are used to protect sensitive data.

ii Privacy Invasion in the Online Space

Lindsey (2017) states that every time a person visits a website, there is a great possibility that a corporation is tracking you, seeing what pages you visit and where you head next. According to BullGuard (2020) there are several ways user's privacy can be invaded online. Data scraping is one method which entails harvesting and tracking people's conversations on social media, job websites and online forums. This is carried out by research companies that in turn sell this information to other companies, who in turn use the data gathered to create targeted advertisements for their products. An argument one might raise is that people willingly share their personal information on social media and by extension it is free to use but data harvesters do not ask for people's permissions or consent and this is a serious privacy issue.

Equally of great importance in terms of privacy invasion is the concern that Facebook Company reveals personal data of users. It was once reported that Facebook Company leaked personal information of users to advertising and internet tracking companies without the users' knowledge. This is carried out during the apps installation process and the user is shown certain terms that require you to "allow" and as soon as a user clicks it, the Facebook application receives an "access token". Facebook then proceeds to give these tokens to advertisers, granting them access to user's personal information which includes chat logs and photos. This is done without a disclaimer or notification to the user stating that their data is being sent to third parties (Newcomb, 2018).

Online social tracking on Facebook apps such as *Instagram* allows users to use the "like" buttons which is a tracking tool for social media sites working with online cookies, which are small files stored on a device that enable tracking online. These cookies are placed in browsers so that when a user logs in or creates an account, it is known. These browsers can also track interest and online shopping habits. Surveillance is the business model of the internet. Internet users seem more relaxed about giving up fundamental aspects of their privacy for the benefit of using their phones and computers and have accepted that being monitored is just another aspect of life (Berkeman & Belfer in Mineo, 2017). According to Schneier (in Mineo, 2017), "if people were told that they had to inform the police when they made a new friend, they would never do that but instead they inform Facebook*"*.

iii. The Privacy Paradox

Norman, Guta and Flicker (2009) describes privacy paradox as a competing demand to use Information Technologies such as social technology and social software, and having an on-line persona while simultaneously having to guard against potential threats to personal safety and privacy resulting from the misuse of available information. Hart (2019) added that consumers consistently say that they want more privacy, but they do not do much about it. 92% of consumers say that they should be able to control the amount of information about them on the internet and 71% say that they would stop doing business with a company that gives away their private data without permission according to a report from PricewaterhouseCoopers, but most consumers do not actually take active steps to protect their privacy. Barnes (2006) stated that students want to keep their information private but do not realise that Facebook is a public space. Sharing their personal information on social networking sites is not only sharing with online friends. This is an inconsistency between the concerns of people regarding their privacy and their actual behaviour (Burkardt, 2018). Facebook despite its privacy scandals that a lot of people are aware of still has massive growth and its overall revenue shot up to 30.4% in the last quarter of 2018. The multitude of privacy scandals that some users are aware of, has not affected the way they use the application or their behaviour (Naughton, 2019).

Research has shown that people put a value of 25 euros for sensitive information and only 10 euros for browsing information, so services provided by big companies like *Facebook* seem worthwhile in comparison. Even if users actually care about their privacy, they often do not have the expertise needed to protect their privacy nor do they understand the consequences of it being violated (Glance, 2018).

2.2 Theoretical Review

Two theories formed the theoretical basis for this study. The first is the privacy calculus theory proposed by Culnan and Armstrong in 1990. The theorists posit that an individual's intention to disclose personal information is based on risk-benefit analysis. In other words, the individuals compare perceived risks with the anticipated benefits. This theory established that online self-disclosures are based on a cost-benefit trade-off, this means that people will disclose personal information when the perceived benefits outweigh the potential costs. In privacy calculus, the use of social networking sites is measured by the perceived privacy risks or privacy concerns. Bringing it into the study context, the more Facebook users benefit (interaction, connectivity, entertainment) from using *Facebook*, the more they will be willing to disclose personal information about themselves (Dienlin & Metzger, 2016).

The second is the Communication Privacy Management theory (CPM) propounded by Sandra Petronio in 2002. The theory makes three assumptions about humans, which includes the fact that humans are choice makers, humans are rule makers and rule followers and humans' choices and rules are based on consideration of others as well as self. CPM reinforces the fact that people negotiate processes when it comes to disclosing private information or concealing it. This theory reveals that users determine their boundaries in disclosing private information, making conscious decisions about how they perceive and set boundaries for their individual privacy while examining the negotiation process in which private information is shared. CPM suggests that people understand that when others are told or given access to a person's private information, they become co-owners of that information. When co-owners of private information do not effectively negotiate and follow jointly held privacy rules, there would be a disruption in the boundaries that the owner of the private information had set prior to co-ownership and thus destroys the trust between them. The theory illustrates the relationship that exists between every Facebook company app users while emphasising that there are rules

which both parties must adhere to in order to manage the communication process (Petronio & Durham, 2015; Petronio & Hernandez, 2019).

2.3 Review Of Previous Related Studies

i. Awareness of privacy issues by users of Facebook Applications

Acquisti and Gross (2006) examined the awareness, information sharing and privacy on Facebook to compare members' attitudes with actual behaviours concerning privacy in a survey. The findings of the study showed that individuals who actually cared about their privacy were still revealing large amounts of personal details about themselves. In addition, there were evidences of misconceptions about the actual size of the online community and the visibility of users' profiles.

A study on 210 Facebook users to examine users' privacy awareness and how information is disclosed revealed that the users that are the most active actually disclose a large amount of privacy information and that Facebook privacy policy are not known or understood (Pitkanen & Tuunaimen, 2012).

A study of the factors influencing privacy awareness of Bangladeshi undergraduate university students by Rahaman and Ullah (2013) revealed that employers do comb through the social media accounts of prospective workers and it was found that a large number of students actually care about their privacy and they do make regular changes to their settings.

Young and Haase (2009) carried out a study on information revelation and internet privacy concerns using Facebook as a case study. A survey of undergraduate communication studies students in English Canada and 77 respondents revealed that 99.35% use their full name on their profile, two-third indicated their sexual orientation, interests, school and relationship status and 7.9% even disclosed their physical home address.

Ibrahim and Masrom (2015) carried out an explorative study of the perceived benefits, privacy risks and the use of privacy strategies on Facebook to know which privacy settings and features on Facebook are utilised by users. An online survey was used and the data revealed that privacy strategies on Facebook were mostly used for managing profile visibility, networking boundaries and privacy awareness.

Schofield, Reips, Stieger, Joinson and Buchanan (2007) in an article titled: I*nternet user's perception of privacy concerns and privacy actions*", examined the internet user's privacy concerns, and any actions they take to guard against these concerns. The researchers made use of a Dynamic Interviewing Programme (DIP) to survey users automatically and 530 participants were analysed. 56% stated that they were concerned about their privacy online, 73% take actions to protect their privacy online. However, the survey did not consider the non-English speakers and as a result one cannot be sure that they fully understood the term privacy.

A study carried out by Hoadley, Xu, Lee and Rosson (2009) analysed the case of the Facebook news feed privacy outcry. A survey of 172 current Facebook users was carried out and they found out that people who use Facebook have an illusionary control over the private information on the newsfeed and this was the major reason for the public outcry while the information on the news feed being used to judge people in a professional context.

A study carried out by Child and Starcher (2016) about mediated lurking, vague-booking and Facebook privacy management, utilised the communication privacy management theory. 383

participants completed an online survey and mediated lurking was related more to Facebook privacy management while men engaged more in strategic ambiguity to protect their privacy on Facebook and enacted less privacy management than women. Users, despite their concerns for privacy, still disclose personal information about themselves.

Although previous studies have attempted to highlight some of the privacy issues arising from user's experience as well as user's attitude to these concerns, not much of these works focused particularly on Nigeria with a teeming youthful population coupled with the increasing use of social media among this population. This study attempts to harvest as many of these privacy issues which previous studies may not have discussed exhaustively.

3. Methodology

This study utilised the survey research method. The study population were all undergraduates of Babcock University, Ilishan-Remo, Ogun State with a total population of 9,180 according to the University Registry (2019/2020 academic session). The sample size of 368 was determined using the Cochran (1997) formula. Simple random sampling method was used for the selection of respondents from two male and two female halls of residence. The fish bowl method was used in drawing two female and male hostels from the nine male and female hostels available. The name of each hall was written on tiny strips of papers which were squeezed and placed in two different bowls representing male and female hostels. After shaking the baskets one after the other, one paper was drawn randomly in two consecutive turns. . At the end of the selection, Bethel Splendor and Samuel Akande halls (with 500 student capacity each) were chosen for the male respondents while respondents from Havilah Gold (750 capacity) and White hall (500 capacity) represented the female students. To get the total number of respondents from each hall, proportional distribution was used to get a number proportional to its capacity. 82 copies of the questionnaire were administered at Samuel Akande, Bethel Splendor and White Halls respectively while 122 copies were administered at Havilah Gold purposively based on the condition that they use the three Facebook Applications (Facebook Messenger, Instagram and WhatsApp) which this study focused on due to their popularity among the youth. Quantitative data were derived from a validated questionnaire tested for reliability with a pilot test which yielded a Cronbach Alpha score of 0.721. Data were analysed and presented using descriptive statistical tools such as percentage calculation and frequency counts of variables measured.

4. Answers to Research Questions

Research Question 1: What is the level of awareness of privacy issues on Facebook applications amongst Babcock undergraduates?

Table 1: Respondents' Awareness of Facebook Applications privacy issues

S/N	Response Variables		NA	SA	SA	MA	VA	EA	Total
1.	I am aware that Facebook applications (Facebook, WhatsApp and Instagram,) track my location	Freq	61	34	29	157	48	30	359
		%	17.0	9.5	8.1	43.7	13.4	8.4	100.0
2.	I am aware that Facebook applications can access my contact list and the people I text and call.	Freq	17	30	39	68	165	40	359
		%	4.7	8.4	10.9	18.9	46.0	11.1	100.0

3.	I am aware that Facebook applications have profiles on users who have never created an account before.	Freq	189	22	38	16	9	85	359
		%	52.6	6.1	10.6	4.5	2.5	23.7	100.0
5.	I am aware that Facebook applications track my online purchases	Freq	190	96	15	26	20	12	359
		%	52.9	26.7	4.2	7.2	5.6	3.3	100.0
8.	I am aware that Facebook applications sell my information to companies for profit	Freq	200	61	30	33	22	13	359
		%	55.7	17.0	8.4	9.2	6.1	3.6	100.0

Key: NA=Not Aware, SA= Slightly Aware, SA= Somewhat Aware MA= Moderately Aware, VA = Very Aware, EA= Extremely Aware
Source: Field Survey 2020

To establish the level of awareness of privacy issues on Facebook applications amongst Babcock undergraduates, table 1 shows that most of them are (43.7%) moderately aware that Facebook applications track their location, 46.0% are very aware that Facebook applications can access their contact list and the people they text and call, 52.6% are not aware that Facebook applications have profiles on users who have never created an account before. 52.9% are not aware that Facebook applications track their online purchases, Also, 55.7% are not aware that Facebook applications sell users information to companies for profit. The findings showed that respondents are largely unaware of how the information they had submitted to Facebook Applications are being used to monitor their activities and that of their friends without their permission. The implication is that the privacy of these respondents have been largely violated as most of these users may have disclosed these information without fully comprehending how they will be used subsequently. In an earlier study, Barnes (2006) had noted that as much as students want to keep their information private, they do not realise that *Facebook* is a public space. They do not realise that sharing their personal information on social networking sites is not only sharing with online friends but sharing with strangers. They may also be unaware of the actual size of the online community and how visible their profiles are. These are issues of great concern that many of these youths are yet to come to terms with in relation to the potential dangers as well as the extent of violation of their privacy. Based on the argument of the communication privacy management theory, both Facebook Applications and their users have become co-owners of information once disclosed or shared. Going by the prediction of these theorists, a disruption in the boundaries that the owner of the private information had set prior to co-ownership is what is being experienced, thus the trust between Facebook App and users may be on the decline. As much as the theory illustrates the relationship that exists between every Facebook company app users, it equally emphasises the fact that there are rules which both parties must adhere to in order to manage the communication process (Petronio & Durham, 2015). .

Research Question 2: To what extent are Babcock undergraduates concerned about their privacy on the Facebook applications?

Table 2: Privacy concerns of Respondents to Facebook applications

S/N	Response Variables		SD	D	A	SA	T	M.V
1.	I am concerned when I see online advertisements on Facebook applications that are of interest to me when I did not search for it	Freq	34	71	162	92	359	4.28
		%	9.5	19.8	45.1	25.6	100.0	

2.	I am concerned that Facebook applications have access to my internal storage on my device and can see files on it as well as modify it	Freq	31	97	119	112	359	4.14
		%	8.6	27	33.1	31.2	100.0	
3.	I am concerned that Facebook screens through my personal messages in order to sell it to interested third parties	Freq	25	88	93	153	359	4.41
		%	7.0	24.5	25.9	42.6	100.0	
4.	I am concerned that even if I have a private profile some people can still search for my profile and view some of my posts	Freq	34	101	126	98	359	4.04
		%	9.5	28.1	35.1	27.3	100.0	
5.	I am concerned that Facebook applications knows some of the websites I visit online	Freq	47	77	102	133	359	4.18
		%	13.1	21.4	28.5	37.0	100.0	
6.	I am concerned about how well Facebook applications protect my data	Freq	42	87	97	133	359	4.17
		%	11.7	24.2	27	37.0	100.0	

Keys**: SD= Strongly Disagree D= Disagree, A= Agree, SA= Strongly Agree**

Source: Field Survey 2020

Table 2 shows that respondents generally agree that they have privacy concerns in relation to their usage of the Facebook Apps. 45.1% are concerned when they see online advertisements on Facebook Apps that are of interest to them when they have not searched for such; 33.1% are concerned that Facebook Apps have access to the internal storage of their devices; 42.6% strongly agree that they are concerned that Facebook Apps screens through their personal messages in order to sell to third parties; 35.1% agree that they are concerned that even if they have a private profile, some people can still search for their posts; 37% strongly agree to be concerned that Facebook Apps know some of the websites they visit likewise, 37% strongly agree to be concerned about how well Facebook Apps protect their data. From the findings, there is no doubt that respondents have different concerns regarding how the information they have disclosed on Facebook Apps are being used.

Several studies have provided evidences that these concerns are genuine. Lindsey (2017) had noted there is a great possibility that a corporation is tracking a consumer every time they visit a website. In the opinion of BullGuard (2020), Unfortunately, Hart (2019) citing the PricewaterhouseCoopers report revealed that most consumers do not actually take active steps to protect their privacy and consumers are unwilling to stop doing business with a company that gives away their private data without permission. The fact that these respondents have these concerns and are still active on these applications brings to fore the issue of the privacy paradox – a situation where consumers consistently say that they want more privacy, but they do not do much about it. Theoretically, the privacy calculus theory revealed another reason why users engage in online self-disclosures which is when they think that the perceived benefits outweigh the potential costs. In privacy calculus, the use of social networking sites is measured by the perceived privacy risks or privacy concerns. In other words, the more Facebook users benefit (interaction, connectivity, entertainment) from using *Facebook*, the more they will be

willing to disclose personal information about themselves (Dienlin and Metzger 2016) regardless of the risks involved.

5. Conclusion and Recommendations

This study investigated the level of awareness and privacy concerns of Babcock University undergraduate users of Facebook company applications such as *Facebook*, *WhatsApp, Instagram* and *Facebook messenger* as regards the privacy issues associated with signing up. It showed that most of the users are not aware of the privacy issues associated with the use of the Facebook Apps while some are only moderately aware that they have granted Facebook Applications certain access to their privacy. In addition, respondents are largely concerned about what Facebook Applications do with all the data they have submitted and the fact that their online and offline activities can be monitored and even transferred without their permission. This reinforces the fact that there is concern amongst the students on the privacy issues of Facebook applications but then there is not a sufficient response on the part of students to mitigate this concern. This can be due to the benefits that they derive from using these applications despite the apparent issues.

5.2 Recommendations

Following the conclusions stated, the following recommendations are made;

1. There is a need for more sensitisation among communication bodies in Nigeria especially directed at youths who are the major users of social networking sites to be more aware and cautious of the kind of information they reveal online and what they share with friends especially on the Facebook applications.
2. Users need to take specific actions in protecting their privacy such as avoiding the installation of third party applications from Facebook applications this is because installing these applications allows them to gain access to your personal data, including your name, gender, usernames and profile picture, location and more.
3. Users need to turn on the extra security settings on Facebook applications so that they are notified immediately if Facebook sees a log in from a device that do not normally use and also make use of two factor authentication.
4. The study equally highlights the issue of media and information literacy among users of the new media as the study shows that most users of social media are not knowledgeable enough to understand how to manage their information and online activities. There is therefore a need for more user education especially of social media applications such as Facebook Applications in order not to jeopardise their safety and security.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: awareness, information sharing, and privacy on the facebook. *Privacy Enhancing Workshops, 4258*.

Barnes, S. B. (2006). A privacy paradox: social. *First Monday, 11*(9). http://firstmonday.org/issues/issue11_9/barnes/index.html

BBC.COM (2020) https://www.bbc.com/news/business-53689645

Belyh, A. (2015). Privacy. Retrieved from cleverism.com: https://www.cleverism.com/lexicon/data-privacy/

BullGuard. (2020). *BullGuard*. Retrieved from bullguard.com: https://www.bullguard.com/bullguard-security-center/internet-security/social-media-dangers/privacy-violations-in-social-media.aspx

Burkhardt, K. (2018). *Internet Citizen*. Retrieved from mozilla.org: https://www.axios.com/consumer-data-privacy-protection-personal-adeba01c-fce2-43ad-890a-222bdbbb7f4a.html

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behaviour*.

Dienlin, T. & Metzger, M.J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, 21(5), 368–383,

Forbes (2020) #3 Mark Zuckerberg: Real Time Net Worth. https://www.forbes.com/profile/mark-zuckerberg/

Glance, D. (2018). How Facebook uses the 'privacy paradox' to keep users sharing. *The Conversation*. Retrieved from theconversation.com: https://theconversation.com/how-facebook-uses-the-privacy-paradox-to-keep-users-sharing-94779

Hart, K. (2019) The privacy paradox. Axios survey Poll. https://www.axios.com/consumer-data-privacy-protection-personal-adeba01c-fce2-43ad-890a-222bdbbb7f4a.html

Hauser, J. (2015). The evolution of the concept of privacy. European Digital Rights (*EDRi*) https://edri.org/evolution-concept-privacy/

Hoadlry, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2009). Privacy as information access and illusory control: The case of Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications* *9*(1), 50-60. https://doi.org/10.1016/j.elerap.2009.05.001

IAPP. (2019). *IAPP*. What is privacy? https://iapp.org/about/what-is-privacy/

Ibrahim, S. Z., & Masrom, M. (2015). Perceived benefits, privacy risks and the use of privacy strategies on Facebook: An explorative Study. *ARPN Journal of Engineering and Applied Sciences*.

Isaac, M. and Frenkel, S. (2018) *The New York Times*. Facebook Security Breach Exposes Accounts of 50 Million Users. https://www.nytimes.com/2018/09/28/technology.

Islam, M.Z. and Jahan, A. (2015) Right to privacy: is it a fundamental right in Bangladesh constitution? *Journal of Asian and African Social Science and Humanities*, Vol. 1, No1, pp. 1-7Lindsey, N. (2017). Invasion of Privacy: Tracking Your Online Behavior Across the Web. *CPO Magazine*. https://www.cpomagazine.com/data-privacy/invasion-of-privacy-tracking-online-behavior-across-web/

Mineo, L. (2017). On Internet privacy, be very afraid. *The Havard Gazette*. https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/

Naughton, J. (2019). The privacy paradox: why do people keep using tech firms that abuse their data? *The Guardian*. Retrieved from theguardian.com:

https://www.theguardian.com/commentisfree/2019/may/05/privacy-paradox-why-do-people-keep-using-tech-firms-data-facebook-scandal

Newcomb, A. (2018). A timeline of Facebook's privacy issues and its responses. *nbcnews*. Retrieved from nbcnews.com: https://www.nbcnews.com/tech/social-media/mediatimeline-facebook-s-privacy-issues-its-responses-n859651

Nield, D. (2017). You probably don't know all the ways Facbeook tracks you. *Gizmodo*. Retrieved from gizmodo.com: https://gizmodo.com/all-the-ways-facebook-tracks-you-that-you-might-not-kno-1795604150

Norman, C. Guta, A. and Flicker, S. (2009) Engaging youth in health promotion using multimedia technologies: Reflecting on 10 years of TeenNet Research Ethic and Practice. *Handbook of Research on Technoethics*. IGI Global.

Petronio, S. and Durham, W.T. (2015) Communication Privacy Management Theory: Significance for Interpersonal Communication. https://us.sagepub.com/sites/default/files

Petronio, S. and Hernandez, R. (2019) Communication Theory, Health and Risk Communication, Interpersonal Communication. *Oxford Research Encyclopediashttps://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-373*.

Pitkanen, O., & Tuunainen, V. K. (2012). Disclosing Personal Data Socially- An Empirical Study on Facebook Users' Privacy Awareness. *Journal of Information Privacy & Security, 8*(1).

Rahaman, A., & Ullah, S. (2013). Exploration of Influencing Factors that Effecting Facebook Privacy Awareness on Bangledeshi Undergraduate University Students. *International Journal of Scientific and Technology Research , 2*(6), 163-171.Reiff, N. (2020) 5 Companies Owned By Facebook: Photo and video-sharing, virtual reality, and messenger services. https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp

Schofield, P.C., Reips, U, Stieger, S., Joinson, A.N., & Buchanan, T. (2007). Internet users' pereption of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536.

Techopedia. (n.d.). *Techopedia*. Retrieved from techopedia.com: https://www.techopedia.com/definition/24954/internet-privacy

Tytyk, K. (2018, February 4). Retrieved from stopad.io: https://stopad.io/blog/why-online-privacy-matters

Young, A. L., & Quan-Hasse, A. (2009). Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook.

Yurieff, K. (2018) Your Facebook data scandal questions answered. *CNN Business*. https://money.cnn.com/2018/04/11/technology/facebook-questions-data-privacy/index.html.