International Journal of Management, Social Sciences, Peace and Conflict Studies (IJMSSPCS), Vol.5 No.3 September, 2022; p.g. 367- 376; ISSN: 2682-6135

SOCIAL MEDIA NETWORKING AND PRIVACY CONCERNS

OLUWATOSIN E. KOMOLAFE
Department of Mass Communication
Redeemer's University, Ede, Osun State
komolafee@run.edu.ng

&
BERNICE O. SANUSI (PhD)
Department of Mass Communication
Redeemer's University, Ede, Osun State
sanusib@run.edu.ng

Abstract

It comes as no secret that social media has become an integral part of our everyday lives. The things we post, like, search, and even the people we interact with can reveal certain attributes about ourselves that we did not know existed. Social media might seem like a safe place to interact and share all manners of information, however strong passwords and other security measures do not secure our data. Unknown to many social media users, these platforms have the ability to collect, store, and share users' data with third parties. More often than not, privacy policies are not read through before granting these platforms access to personal information consequently leaving users to carelessly utilize social media by revealing more than they should. Numerous data breaches across social media platforms over the years have incited a growing concern with online privacy and how these social media companies use their data. Despite these concerns, users' are still compelled to make use of social media in order to meet specific needs, which is why the uses and gratifications theory was employed in this conceptual study. This paper touched on issues with privacy policies, and privacy concerns regarding online social media networking.

Keywords: Privacy Policy, Social Media, Social Media Networks, Data Users.

Introduction

As of July 18, 2021, Global Social Media Stats reported that there are 4.48 billion social media users worldwide, equating to almost 57 percent of the total global population. Social media platforms have provided several benefits to human existence and one of the most prominent effects is the dependency on these platforms. Whether it is to reach out/keep in touch with people, promote a brand, start a business, and whatever reason one can think of, there are thousands of social media platforms, each with a significant purpose to meet the needs of its users. These social media platforms have become an extension of the human body and have made it very difficult to perform even the simplest tasks without them. Marshall McLuhan knew what he was saying when he argued that man has integrated technology so much in his life that it has become an extension of his body. Being cut off from or denied access to social media is like rendering one handicapped and disabled. In that moment life almost becomes meaningless when one have no access to the platform that caters to your basic needs, wants,

and desires. Man has become so dependent on these platforms that he is willing to overlook certain shortcomings and concerns such as privacy. Alexandra (2019), confirmed this when she stated that;

> Most Internet users are least bothered about their online privacy and are unaware of the plausible risks associated with it. Not only your privacy but your safety is also endangered, especially when you are using the Internet to carry out important and secretive tasks like online banking and sharing crucial business files (Alexander, 2019, para. 2).

Privacy on social media is put in place to protect users' personal information and create boundaries to restrict or block external interference and influence. When privacy on social media is compromised, it can lead to several implications such as identity theft, location tracking, spying and snooping; stealing of personal information, and data usage.

As important and useful as social media is, it can pose multiple threats to users, which is why privacy is very essential to not only ensuring safety but also allowing for anonymity to a great extent. Although personal information is needed to create profiles on these platforms, it is quite contradictory to imply anonymity is guaranteed. It is the responsibility of the social media platform to keep the users' personal information un-linkable to their identities. They assure users of this but is that the case? This seminar paper will be exploring online social media networking and privacy concerns on popular social media platforms which include; *WhatsApp, Instagram, Facebook, Snapchat,* and *TikTok*.

Statement of the Problem

The Internet is a world of its own and like reality that requires protection against all manner of physical threats; online presence equally requires protection against dangers to user's personal information and data. Although privacy is a qualified fundamental human right in most countries, it is almost non-existent in the digital atmosphere since every data put out by the users are collected, stored, and shared to third parties by websites and social media companies. Users have allowed this for too long because of their lack of knowledge of how their data is used. Although social media companies inform users of how they use their information in the privacy policy, this is often overlooked by users who do not have the patience to read nor understand these policies and just accept whatever the company requires in a bid to gain access to the platform.

There are a number of consequences attached to these companies having a great deal of control over users information, one of them being how they share data with and allow very powerful institutions such as the government and other corporations, continuously interfere with users privacy.

Since this has become the reality of online social media networking, finding solutions to how it can be contained so that our online presence does not negatively affect our everyday lives is the real challenge.

Definition of Terms

Privacy: This is the freedom from interference or intrusion. It is the barrier that protects one from external harm and allows one to manage their boundaries.

Privacy Policy: A document or online manuscript that informs readers of how their personal information will be collected, used, and processed if granted access to products or services, whether online or offline.

Social Media: Websites and applications that permit users to create and share content or participate in social networking.

Social Networking: This is the use of websites and applications to interact with other users, or to find people with similar interests to one's own.

Mobile App: Initially known as mobile application or simply an app, this is a computer program or software application designed to run on a mobile device.

Data: A collection of facts or information which can be numerical and /or non-numerical.

Review of Literature

The Evolution of Social Media

It is hard to imagine a world without social media. In today's society, we use social media for just about any reason you can think of, because numerous platforms serve specific purposes whether it is business-related, education-oriented, or probably just for entertainment purposes. Whatever the reason may be, social media has changed the way we communicate, conduct business, and even tackle some of the world's biggest challenges amongst other things. The evolution of social media dates as far back as 1997. Before society was flooded with countless social media websites and applications, Andrew Weinreich was ahead of his time and what was to come when he invented 'Six Degrees', the world's first social media network. This media platform was a free web-based networking service that allowed users to sign up using their email address, and then create individual profiles to locate people around the world to their network. This platform was aimed at building and improving users' networking to make their lives more efficient. The site was quite popular with about 3.5 million users before it was shut down in 2002 after being sold for $125 million to Youth Stream Media Networks. Although its reign was short-lived, Six Degrees made a significant and lasting impression which created a path for other new and improved social media platforms such as Friendster, Linkedin, Myspace, and the very popular and prominent social media providers we have today.

Privacy Concerns and Online Social Media Networking

When a company, website, or mobile app creates a privacy policy, it is primarily to shield them from lawsuits. For the users, on the other hand, privacy policies do not protect them from anything; instead, it is the company's way of informing users of what they do with their data. Therefore, it is up to the users to decide whether to agree to these policies or not. Privacy policies can only grant users' protection if companies and institutions assert that they will do so.

Social media platforms and their users have significant roles to play in protecting and ensuring privacy. Although the privacy policy only makes promises that are not always kept, users' can take control of their social media privacy by adjusting their privacy settings within the social media network, turning off location features, and limiting the amount of information they share. Abuse of personal information can expose users' to the likes of cyber-stalking, stalking and harassment, identity theft, and many other risks.

In the case of social media platforms that ensure confidentiality, there is still cause for concern on possible breaches of the policies.

Data collection, data storage, what is done with the data, who it is shared with, and most importantly if the social media platforms can prevent data from leaking, are the main privacy concerns when using social media.

Auxier et al (2019) conducted a study on Americans' attitudes and experiences with privacy policy and findings revealed that 79% of Americans recruited for the research have little to no confidence in a company's ability to protect them. Only 3% indicated that they are very confident, while 18% are somewhat confident that companies will protect them and take responsibility when personal data is misused or compromised. The study also drew attention to privacy concerns among the general public about how companies and the government are using their data. 79% of adults said they were at least somewhat concerned about how company's use the data it collects about them, including 36% who stated that they are very concerned about this issue. At the same time, 64% of Americans reported that they feel very or somewhat concerned about how the government is using the data it collects about them.

Correspondingly, in Adelola's (2015) investigation on Nigerians' perceptions of personal data protection and privacy, respondents were asked if they trusted the government to fully handle data protection and privacy issues. The results translated a general lack of trust in the government on these issues with fewer than one in 6 (16%) agreeing that the government could be trusted. 0% of the respondents strongly agreed that the government can generally be trusted to look after privacy interests, whereas 31% disagreed and 17% strongly disagreed. 36% of the respondents, however, neither agreed nor disagreed with this.

Although Auxier's and Adelola's research areas do not focus strictly on social media platforms, instead online privacy as a whole and privacy on online shopping sites respectively, their work is relevant in this study because of the privacy policy background and how Internet users perceive and behave towards it, as well as their trust or lack of it in the government, is drawn attention to.

A lot of time, energy, and money are dedicated to social media. Statista, puts forward that as of 2019 and 2020, the average daily social media usage of the Internet worldwide amounted to 145 minutes per day, up from 142 minutes in the previous year. People have become so absorbed in social media that their online presence holds greater significance than their actual lives without these platforms. Totka (2015) believes that if we're making connections and doing business in the "real world," the same rules should apply on the web.

As interesting and engaging as social media is, it is not all it is cut out to be behind the scenes. What happens on the other side of the Internet? The real question, however, is who controls and monitors information and Internet activity? Ilozue (2017), made a good effort at answering this question by stating:

> The Internet is not in one country or run by one company. Quora monitors Quora with our help and *Facebook* does the same with *Facebook*. When something is an independent site, the search engines usually monitor it. When something is criminal, we report it to the FBI or whatever our local government investigative agency is. (Iluzue, 2017, p.1)

Google for instance specifies in their privacy policy that they do not share users' personal information with companies, organizations, or individuals outside of *Google* without the user's consent. College (2012) begged to differ and argued that *Google* stores every single search and claim it is to improve its engine, when what they really do is store data for specific reasons, one of them being to provide any user information or activity to federal governments and police organizations all over the world if they require them.

When users are online, any form of interaction, whether it is sharing a picture, making a random comment, or even liking a post, creates digital footprints which can be tracked and stored in the platform's database. These footprints left behind by users' can either be passive or active. A passive footprint is made when information like the IP address is collected from the user without their knowledge. An active digital footprint on the other hand is where the user has deliberately shared information about themselves such as, emails, social media posts, and so on, either by using social media sites or by using websites. Eriksen (2018) adds that;

Every email, post, photo and click you make online leaves a trail. Even by reading this article, you're adding to your ever-growing string of breadcrumbs online. It's permanent, it follows you for life and it's not going anywhere—it's your digital footprint. (Eriksen, 2018, para.1).
Specific examples of digital footprints As mentioned byMedia Literacy Council are:

1. Your search history.
2. Text messages, including deleted messages.
3. Photos and videos, including deleted ones.
4. Tagged photos, even those you never wanted online.
5. Likes/loves on sites like *Facebook* and *Instagram*.
6. Browsing history even when you are on incognito (disguise/anonymous) mode.

Digital footprints are important because it determines users' digital reputation, which is also as vital as their offline reputation as employers check a potential employee's digital footprints before hiring. If people are not trying to know more about you from your social media profile, and what you post, they can go the extra mile by turning to the many sites that are committed to gathering as much public information about people as possible. Even a simple *Google* search may just give outsiders what they are looking for.

Asides from digital footprints, there are tracking technologies in browsers and mobile apps that can reveal much more about people. These tracking technologies include cookies, web

beacons, tags and scripts, Software Development Kits (SDKs), and so on. These technologies can track users' IP address, location, operating system, browser, browser language, device identifiers, advertising identifiers, and other usage information.

The presence of these footprints and tracking technologies have made it difficult to remove oneself from the digital atmosphere, although it provides benefits like detecting fraud and adding value to Internet usage, it can pose a threat to privacy and expose users' to risks.

Users Attitudes towards Privacy Policies

Privacy policies do always contain a lot of text, and a great deal of the time this is ignored by users who have no patience to read the fine print and what it entails. The privacy policy many overlook usually notifies users of how their personal information is collected, processed, and stored. Guynn (2020) asserted that what you do not know can hurt you and by signing away all kinds of rights concerning your data without making an effort to find out how applications and websites make use of it, who they share it with, as well as how long they keep it can put one at grave risk.

For instance, in 2010, it was reported that 7,500 online shoppers unknowingly sold their souls when they ignored the terms of conditions put in place by Game Station, a chain of retail shops in the United Kingdom that deals with new and used video games. The game site included an "immortal soul clause" to their terms and conditions, meaning that customers grant the company the right to claim their souls. As reported by Fox News, it read as thus:

> By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant us a non transferable option to claim, for now and forever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions.

The terms of service were updated on April fool's day as a gag, but the retailer did so to make a very important point which was that no one reads the online terms and conditions of shopping, and companies are free to insert whatever language they want into the documents. Obar & Oeldorf-Hirsch (2016) conducted an empirical investigation of privacy policy and terms of service policy reading behaviour to find out the extent to which individuals ignore both policies when joining a fictitious social networking site. The dummy site which they called Name Drop, contained the privacy policy and the terms of service policy which had a total of 7,977 and 4,316 words respectively. The study highlighted that an average adult reading speed is approximately 250-280 words per minute. This suggests that it should take 29-32 minutes to read the site's privacy policy and 15-17 minutes to read through the terms of service policy.

This piece of information is very important because As mentioned by Banner (2021), the average reader only has an attention span of about eight seconds when reading online. Therefore, the possibility of an average individual with such a low attention span will most likely not sit through even three minutes of reading any policy.

Using the words-to-time website (www.wordstotime.com), the number of words from the privacy policies of *Facebook, WhatsApp, Instagram, Snapchat, Twitter* and *TikTok* were automatically counted and converted to how many minutes it will take to read. Computation of these policies indicated that *Facebook's* privacy policy will take an individual with an average reading speed 32 minutes to read. *WhatsApp* takes 29.9 minutes, *Instagram*, 32.2 minutes, *Snapchat*, 31 minutes, *Twitter*, 29.5 minutes and *TikTok*, 28.6 minutes. The information overload of the privacy policies of these social media platforms poses a challenge to users as it will discourage them from reading the detailed wordings of the privacy policy.

Auxier et al (2019) researched Americans' attitudes and experiences with privacy policies and laws. They analysed the thoroughness users apply when reading privacy policies and found out that amongst the adults who say they read privacy policies before agreeing to it, only 22% say they read it all the way through before giving consent. Merely 13% however, indicated that they typically understand what they read. "Online privacy policies are difficult to understand. Most privacy policies require a college reading level and an ability to decode legalistic, confusing, or jargon-laden phrases" (McDonald et al., 2008, p.1). Litman-Narvano (2019) was not in favour of this and claimed that a vast majority of privacy policies exceed the college reading level. He went on to quote Jen King, the director of consumer privacy at the Center for Internet and Society, who stated that privacy policies are created by lawyers for lawyers and were never created as a customer tool.

Bailey et al (2018) asked college and law school students in India to review the privacy policies of five popular websites (*Uber, WhatsApp, Google, Flipkart,* and *PayTM*) and then tested them on their comprehension. Despite being well-educated, most students could not correctly answer difficult questions about the policies, and 20-40% of the "easy" questions were answered incorrectly.

Other factors that intimidate users from reading the privacy policy are the font size, which is usually too small, the lack of clarity, and also the complex use of words.

Conclusion

With the continuous growth of social media platforms, its users, along with the changing nature of social networking, tons of data is shared daily, and maintaining privacy online has become somewhat impossible or rather difficult to control. Whether or not we reject the policies and conditions put forward by these social media companies, access to the internet alone along with the presence of tracking technologies and digital footprints monitor our social networking habits and stores the data of everything we click, type, and upload. It should be kept in mind that there will always be interferences where privacy is concerned, regardless; users should be cautious about the type of information they share and take extra precautions to do what they can to at least enjoy what is left of their privacy.

Recommendations

For Users

Users' should:

1. Educate themselves on privacy literacy meaning they should gain knowledge about the technical aspects of online data protection, and also about the laws and directives as well as institutional practices.
2. Learn how to read privacy policies by knowing what to search for. Important keywords like monitor, access, such as, exchange, share, store…etc.
3. Limit the personal information shared on social media.
4. Adjust their privacy settings within the social media network, i.e. turning off location.
5. Not use public computers to log into your social media accounts.

For Social Media Platforms

1. Privacy policies should be reader friendly. It should avoid the use of legal and technical jargons.
2. It should be short in order not to overwhelm readers. Privacy policies need to be specific and provide meaningful information that should be as brief as possible.
3. Before a user is given access to an app, they should be given a compulsory survey asking about their privacy preferences and should also be given options to what they want the app to have access to and how they want their data used.

References

Adelola, T., & Dawson, R., & Batmaz, F. (2015). Nigerians' Perceptions of Personal Data Protection and Privacy. Retrieved From: https://www.researchgate.net/publication/275968129_Nigerians'_Perceptions_of_Personal_Data_Protection_and_Privacy

Alexander, S. (2019). 3 Major Internet Privacy Issues and How to Avoid Them. Retrieved From: https://securitytoday.com/articles/2019/09/03/3-major-Internet-privacy-issues-and-how-to-avoid-them.aspx

Auxier, B., Rainie, l., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans' attitudes and experiences with privacy policies and laws. Retrieved From: https://www.pewresearch.org/Internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

Bailey, R., Parsheera, S., Rahman, F., & Sane, R. (2018). Disclosures in privacy policies: Does "notice and consent" work? *National Institute of Public Finance and Policy (NIPFP), New Delhi.* Retrieved From: https://macrofinance.nipfp.org.in/PDF/BPRR2018_Disclosures-in-privacy-policies.pdf

Banner, M. (2021). How to Capture and Keep Your Readers' Attention. Retrieved From: https://vwo.com/blog/keep-your-readers-attention/

Carson, B. (2014). The rise of Snapchat from a sexting app by Stanford frat bros to a $3 billion IPO. Retrieved From: https://www.businessinsider.com/the-rise-of-snapchat-from-a-stanford-frat-house-to-a-3-billion-ipo-2017-1?r=US&IR=T#it-wasnt-until-spiegels-junior-year-that-the-idea-for-snapchat-was-born-i-wish-these-photos-i-am-sending-this-girl-would-disappear-brown-told-spiegel-in-april-2011-his-friend-immediately-got-excited-about-the-concept-of-disappearing-photos-and-told-brown-that-this-was-a-million-dollar-idea-five-years-later-that-idea-would-now-be-worth-billions-3

College, O. (2012). Who monitors the Internet? Retrieved From: https://www.quora.com/who-monitors-the-Internet?top_ans=88704866 Date Retrieved:

Debatin, B., Lovejoy, J.P., Horn, A., & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication.* DOI: 10.1111/j.1083-6101.2009.01494.x Downloaded From: https://academic.oup.com/jcmc/article/15/1/83/4064812

Eriksen, K. (2018). Your Digital Footprint: What Is It and How Can You Manage It? Retrieved From: https://www.rasmussen.edu/student-experience/college-life/what-is-digital-footprint/

Fox News (2010). 7,500 Online Shoppers Unknowingly Sold Their Souls. Retrieved From: https://www.google.com/amp/s/www.foxnews.com/tech/7500-online-shoppers-unknowingly-sold-their-souls.amp

Global Social Media Stats. Retrieved From: https://datareportal.com/social-media-users

Guynn, J. (2020). What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy. Retrieved From: https://www.google.com/amp/s/amp.usatoday.com/amp/4565274002

Ilozue, C. (2017). Who monitors the Internet? Retrieved From: https://www.quora.com/Who-monitors-the-Internet

Jones, C. (2014). Snapchat hack affects 4.6 million users. Retrieved From: https://www.bbc.com/news/av/business-25582763

Kane, J. (2015). Uses and gratification theory – social media. Retrieved from: https://newhousesocialmedia.syr.edu/uses-gratification-theory-social-media/

Litman-Narvano, K. (2019). We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. Retrieved From: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

Mapping Awareness Campaign (2018). Privacy and Social Media. Retrieved From: https://youtu.be/sMLVkBxke20

McDonald, A. M. & Cranor, L. F. (2008). "The Cost of Reading Privacy Policies," I/S: A *Journal of Law and Policy for the Information Society* Retrieved From: http://cups.cs.cmu.edu

Nakashima, E., Lerman, R., & Whalen, J. (2020). Trump says he plans to bar TikTok from operating in the U.S. Retrieved From: https://www.washingtonpost.com/technology/2020/07/31/tiktok-trump-divestiture/

Nas, C. (2020). How To Stop Instagram From Tracking Everything You Do. Received From: https://www.wired.com/story/how-to-stop-instagram-from-tracking-everything-you-do/

Obar, J. &Oeldof-Hirsch (2016). The biggest lie on the on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. Retrieved From:https://www.ftc.gov/system/files/documents/public_comments/2016/10/00067-129185.pdf

Phillips, S. (2007). A brief history of Facebook. Retrieved From: https://www.theguardian.com/technology/2007/jul/25/media.newmedia

Reiff, N. (2020). 5 Companies Owned By Facebook. Retrieved From: https://www.investopedia.com/articles/personal-finance/051815/top-11-companies-owned-facebook.asp

Rollason, H. (2021). What Countries are the Biggest WhatsApp Users? Retrieved From: https://www.conversocial.com/blog/what-countries-are-the-biggest-whatsapp-users

Selfkey. (2020). Facebook's data breaches – A timeline. Retrieved From: https://selfkey.org/facebooks-data-breaches-a-timeline/

Statista. Daily time spent on social networking by Internet users worldwide from 2012 to 2020. Retrieved from: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/

Thompson, R. (2017). For better or worse, Snapchat changed sexting forever. A double edged sword. Retrieved From: https://mashable.com/article/snapchat-sexting-revolution

Totka, M. (2015). Is Social Media a Waste of Time? Retrieved From: https://www.wired.com/insights/2015/02/is-social-media-a-waste-of-time/

Wamsley, L. (2020). Your Technology Is Tracking You. Take These Steps for Better Online Privacy. Retried From: https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy

Warzel, C. & Mac, R. (2018). These Confidential Charts Show Why Facebook Bought WhatsApp. Retrieved From: https://www.buzzfeednews.com/article/charliewarzel/why-facebook-bought-whatsapp

WhatsApp. Security and Privacy. Retrieved From: https://faq.whatsapp.com/general/security-and-privacy/how-we-work-with-the-facebook-companies?eea=1