Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.10 No.2, 2021, pp.6-13

DOI: https://doi.org/10.51983/ajcst-2021.10.2.2837

Beyond the Hashtag: Social Media and the Challenges to Cyber Security

S. O. Maitanmi[1], A. M. Davies[2], R. O. Oladapo[3], A. Omotunde[4] and A. O. Awoleke[5]
[1]Department of Software Engineering, [2]Department of Law and Security
[3&5]Department of Nursing, [4]Department of Public & Allied Health,
Babcock University, Ilisan Remo, Ogun State, Nigeria
E-mail: maitanmio@babcock.edu.ng, abimbolajohnsondavies@gmail.com, waleoladpo@gmail.com,
omotundeilesanmi07@gmail.com, adeolaawoleke@gmail.com
(Received 6 May 2021; Revised 28 May 2021; Accepted 30 June 2021; Available online 10 July 2021)

Abstract - **Social media may be seen as the new oil that makes the world go round providing access to all manner of information about the users. With the challenges to cyber security, social media users now require a level of awareness of the impact of their actions. This study focuses on the awareness level of social media users to the threats and risks of using the platforms and the extent to which the users are prepared to take responsibility. The study adopted a quantitative descriptive cross-sectional survey research over WhatsApp with 95 respondents selected from two institutions using random selection. Data collected were analyzed using IBM SPSS version 21 to generate summaries of descriptive statistics. All (100%) the respondents are within working class ages although most were aged 31-40 years (45.3%). All users were always on social media (SM) (100%), post daily on social media even though not all (21%) of them read terms and conditions associated with the different social media platforms. Also (55%) of the respondents agree that social media influences their thinking. However, majority of the users are unbothered about the aftermath of their posts as few respondents (32%) disagree that the thoughts of other users about their post is not their problem but that of the other users while (87%) of the respondents believe they can defend their posts. Few respondents (27%) believe that it is possible for litigation to arise as a result of their post on social media and (26%) believe that the application stores their records, which encourages litigation. Despite high level of awareness of the impact of acts of users on cyber security, users are more interested in their protection than that of other users. Whilst regulation would go a long way to manage identified threats, regulation should seek to regulate the coding of social media platforms while social media users garner the requisite emotional intelligence required as a defense mechanism for cyber security.**
Keywords: **Hashtag, Social media, Cyber Security, Facebook, YouTube**

I. INTRODUCTION

Human activities have over time, been influenced by technological advancements which in turn have forced notable changes on the society. As predicted by [1] over 15 years ago, technology will bring about dematerialization, omnipresence and malleability such that information would migrate largely from the physical world to the electronic world and would literarily be everywhere at the same time. This easily depicts the characteristics of social media, which is any technology that allows for social networking, sharing of information, ideas or thoughts online. Cambridge Dictionary [2] expresses social media to be websites and computer programs that allow people communicate and share information on the internet using a computer or mobile phone. According to [3], social media allows for exchange of user-generated content and makes knowledge sharing possible. These features allow tacit knowledge to be captured, reused and rebroadcasted amongst users with online presence as further elucidated by [4].

Social media therefore evidences the movement of physical communication, social interaction and now commercial transactions to various online media forums. The impact of social media as noted by [5] has gone beyond entertainment to a full-fledged part of everyday life. The proportion and share social media occupies in the technological advancement is easily captured by records of few social media platforms. [6] For instance, identified that Facebook had over 2.7 billion monthly active users as at second quarter of 2020 and a whopping 3.14 billion combination of users for Facebook, Instagram and WhatsApp. With the rise in the use of social media and the consequent migration of interaction to the virtual world, [7] notes the concern of social media reducing opportunities for real interactions with people.

With the increased adoption of social media platforms, human interaction, and in some parts, the majority of their interests and lives are being migrated to the virtual world. This portends significant benefits for a wide range of users with benefits including new relationships, ease of reach and opportunities for trade and e-commerce. The challenge is the increasing insecurity of the cyberspace, which the widespread use of social media can exacerbate. According to the Federal Bureau of Investigation Internet Crime Complaint Center of United States of America, between 2016 and 2020, the center received a total of 2,211,396 complaints and total loss reported amounted to approximately $13.3 billion. The cybercrimes reported were mostly phishing messages, personal and corporate data breaches, extortions, non-payment/non delivery, identity theft, and cyber fraud. The increased use of social media

also exposes the user to all forms of possible cyber risk including the risk to a breach of privacy, as explained by [8]. These concerns extend to the problems of cyber-attacks, cyber terrorism, cybercrime, cyber stalking, cyber squatting, cyber bulling, identity theft, credit card fraud, spread of computer viruses or spam, intellectual property theft, hate speech, intercepting communication amongst others. Some of these concerns manifested in the recent examples leading to the conviction of Obiwanne Okeke, otherwise known as Invictus for cyber fraud of $11m as reported by [9], the new trend of cyber protests evidenced by #This Flag, in Zimbabwe as critiqued by [10], #EndSARS in Nigeria evaluated by [11] and the spread of fake news.

There may also be some indirect costs to the society resulting from the use of social media including the unintended influence of social media messages and interactions on other users.

The risks of social media are not limited to individuals alone as societies can be affected as well. For instance, social media is credited at least in part for the successes of not one but two election victories in the United States, first for Obama and then for Trump [12, 13, 7] Its ability to destabilize societies was also brought to the fore with the Arab Spring explained by [14], and recently, the End SARS protests in Nigeria expounded by [15] and [11]. Given the threats associated with the social media, governments across the globe continue to respond with more regulation, some of which have been argued to interfere with the rights of citizens [16]. This is in addition to security requirements put in place by the different owners of the social media platforms.

It is important that users and other interested parties are protected not only from the risk of loss of data but also from unwanted threats, after all security as defined by [17] is the freedom from risk and threat of change for the worse. On the other hand, awareness of these social media risks is key.

Not only should users be aware of threats from other users, in today's world, they must also be aware of exposure of their personal data that can accrue on account of the administrators of the social media platforms who are alleged to be constantly developing means of profiling and collecting information about users to pursue their own agenda as seen in the case of Facebook and Cambridge Analytica.

This threat of profiling as reported by [18] as well as [19] was exposed in the wake of the discovery that Facebook gave out personal data of over 87 million unsuspecting users to Cambridge Analytica in a bid to influence the US elections in 2016. Constitutionally, the duty to protect the security of citizens, whether physically or online is placed on governments. In Nigeria, this is affirmed by Section 14(1) (b) of the Constitution of the Federal Republic of Nigeria [20] and other countries will have similar responsibilities.

Perhaps it is in recognition of these responsibilities that the United Nations Institute of Training and Development, called for more security of the cyberspace citing the increasing incidences of credit card fraud, intellectual property and identity theft, need to combat terrorism and promote e-commerce as expounded by [20].

While there is significant literature on the benefits and risks of social media in different fields of endeavor, there is a need to further assess the awareness level of the users to the existing risk and the preparedness of users to dutifully consider and accept the risks associated with the social media. There is also the need to assess the willingness of users to accept even more regulation of the social media space. Based on these, this study evaluates the average user's attitude to the current security threats presented by the increased use of social media while the specific objectives are to:

1. Identify whether users are aware of the threats and risks of using social media platforms;
2. Identify the areas of social media security for which the average user is prepared to take responsibility;
3. Assess the awareness of users to the existence of regulations on cyber security.

II. LITERATURE REVIEW

A. Social Media Risks and Threats

Sufficient literature establishes the existence of risks and threats of using social media. Some of them include the work of [21], [22], [23] and more recently the work of [24]. The work of [24] identified a range of social media related issues which include the possibility of violent behaviour, availability of offensive content such as pornography, hate speech, exposure to addiction etc. The array of social media risks is not limited to the aforementioned. Social media also features the existence of online predators (sexual and non-sexual), cyber bullying and a huge risk to children and young adults [24]. However, the age of the user does not necessarily mitigate the risk of using social media. This is so because the extent of risk has been established to be associated with the extent of self-disclosure by the user as explained by [24]. Explained that adults with huge online disclosure are equally exposed to criminal exploitation such as identity theft and fraud, all forms of stalking and cyber stalking, employment scams, commercial exploitation and interestingly government surveillance. Most users also employ social media sites from the convenience of their homes or offices. This creates a deceptive feeling of anonymity while unwittingly posting pictures or videos of criminal acts which they had committed.

Interestingly, [25] explained that cyber threats, a form of social media risk, are cheaper than physical attacks and this further displays the possibility of more risk for social media users. Social media threats do not have territorial limitation. Experiences of users cut cross several jurisdictions. In May

2021, the news of death of a young graduate [26] who tweeted her dire need of employment was reported by [26].Following her tweet, she was contacted for an interview which she obliged. Events that unfolded thereafter indicated that the said lady was raped, killed and buried in a shallow grave in Akwa Ibom, Nigeria when she attended the interview. Unknown to her, the alleged interview was all a set up. This reawakens the question of 'what type of disclosure' should be available on social media and what should be the extent of disclosure. In any case, the social media risks are largely visible but are social media users aware?

B. Social Media Risk Awareness

In a study conducted by [27], it was revealed that majority of high school students were ignorant of the risk associated with electronic forms of communication as the respondents largely believed that their predators could not contact them online on the basis of information they posted. This occasions a need to confirm whether the age of the user informs the level of awareness of the risk involved in using social media. [27] Attributed the unawareness to the lack of parental involvement in the internet activities of the respondents. Naturally, this presents the impression that the level of awareness of risk in the use of social media should be higher with age. The need for awareness is not limited to the risk solely but equally to the need for accountability on the part of the users. Put, differently, are the users aware of the implication of their conduct on social media on other users or are users generally unbothered?) [28] in an attempt to study unprofessional behavior on social media by medical students revealed that the respondents posted contents related to intoxication, illegal drug use, patients information etc. On one part, the contents posted on social media may not be regulated or self-regulated by the operators but the content itself may have far reaching consequences on the user whose actions may be regulated by other bodies for instance, medical association and on the victim who may be affected by the content.

The level of awareness is expected to improve the level of responsibility of users of social media. Hence in mitigating social media risks, more research is required to establish the level of awareness of users and their preparedness to take responsibility.

C. Regulation of Social Media versus Personal Responsibility

The issue of whether to regulate social media or not has been a continuous conversation. Would regulation mitigate the risks or should users simply take personal responsibility. In Nigeria, for instance, attempts to regulate social media have been made through the sponsoring of few bills and regulations some of which include 'The Independent National Commission for Prohibition of Hate Speech Bill, the Protection from Internet Falsehood and Manipulations and Other Related Matters Bill, The Nigerian Data Protection Regulation among others. Unfortunately, some of the bills were greeted with major concerns, which include an allegation that the proposed bills were attempts to shut down social media and interfere with the right to freedom of speech [29]. In a more radical approach, the operations of social media giant 'Twitter' was banned in Nigeria while the Nigerian Broadcasting Corporation released the list of requirements for operations within the country and since the ban, a number of reactions have followed including but not limited to an order by the Economic Community of West African States "ECOWAS" Court to the government of Nigeria to lift the said ban [30]. The essence of regulation is to control the use of social media but over regulation may also stifle the media and eliminate the whole range of benefits of using social media. An interesting approach as recommended by [31], is to regulate the code as opposed to the technology. According to [31], the law will better regulate the technology if it regulates the code that developed the technology. Hence, owners and developers of social media platforms have placed on them the huge responsibility of developing platforms with code that cannot permit profile hijacking and can monitor and/or report unauthorized social activities by users. Equally, some measure of personal responsibility is required in the use of social media but such personal responsibility is dependent on the awareness of the implications of actions of users of social media on themselves and other users.

III. RESEARCH METHOD

The use of social media, awareness of risks and degree of responsibility assumed by its users were ascertained by a survey that was carried out between two universities representing the South Western part of Nigeria. The questionnaire was randomly distributed via WhatsApp groups created for the students of these universities. Ninety-five respondents returned the questionnaire out of the 250 respondents who were sampled using the G power formula. Given the mode of distribution of the questionnaire, it is expected that only those who have used any of the social media were included, while those who have not used any of the social media were excluded in the research.

A. Instrumentation

A research instrument was adopted with four constructs namely, demographic variables, information about threats and risks of using social media platforms, scope of the terms and conditions, and level of comprehension of social media regulations.

1. The section B is the second construct apart from the social demographic variables, which was titled "information about threats and risks of using social media platform", and is measured with either Yes/No since this is testing for the knowledge of users. Yes was assigned a value of 1 and No, a value of 0 for coding in the Statistical Package for Social Sciences (SPSS).

2. In addition, the third construct was titled "scope of the terms and conditions" This was measured using Likert scale of five variables which were strongly agree (5), agree (4), undecided (3), disagree (2), and strongly disagree (1).
3. The forth construct was titled "level of comprehension of social media regulations" these questions had dropped down answers where respondents had the privilege of picking more than one answer at a time.

The questionnaire and the skill rating scale were carefully developed to ensure that it covered the constructs and contents areas needed in order to assess the social media and the challenges to cyber security. The researchers and other experts in the fields of computing, information science, law and security scrutinized the instruments. Corrections were made to reflect the face and content validity of the instrument. The reliability of the instrument was achieved by administering the questionnaire to fifteen (15) university students of Ibadan, Oyo state Nigeria in order to establish the reliability of the instrument. The data collected was used to estimate the reliability of the instrument using Cronbach Alpha (R) in order to bring out internal consistency and construct validity of the instrument. It was found to be 0.89 for information about threats and risks of using social media platform, and 0.80 for scope of the terms and conditions. The questionnaire was administrated randomly and ninety five (95) respondents were captured. The questionnaire was screened for outliers and missing values. This was further coded and analysed using the Statistical Package for Social Sciences (SPSS) version 21. Descriptive statistics was used to determine the mean, median, and mode of the information about threats and risks of using social media platform.

B. Description of Sample

From table 1, more of the respondents to the questionnaire were males than females with the demography showing 48(51%) as against the 47(50%) attributed to female users. With the insignificant difference in the gender ratio, it can be said that gender was evenly distributed and the results of the survey should not reflect any gender bias. Again, 84.2% of the respondents are married whilst 15.8% are single. This particularly is more likely a function of the age group of the active participants on social media. The age of respondents can influence the awareness level of social media exhibited by the respondents as. 100% of them are within the working class ages as defined with a significant portion (i.e. 43.5%) aged between 31-40 years More important, is the confirmation that the participants were well educated up to the higher institution level and therefore considered to be aware and understand the implications of their acts and experiences on social media. The sample of respondents is considered apt or the research work as it represents a caliber of people who are highly educated, are accustomed to taking responsibility for themselves and for others and also have good opportunity for active social media engagement.

IV. RESULTS AND DISCUSSION

TABLE I DEMOGRAPHIC VARIABLES AND SOCIAL MEDIA AWARENESS

Demography and Social Media Awareness			
Items	**Description**	**Frequency**	**Percentage**
Gender	Male	48	50.5
	Female	47	49.5
	Total	95	100
Education	Higher Education	95	100
	Total	95	100
Age	20-30	14	14.7
	31-40	43	45.3
	41-50	22	23.2
	51-60	15	15.8
	61-70	1	1.1
	Total	95	100
Active on Social Media	Yes	95	100
Post on Social Media	Yes	95	100
Share Joy and happiness on social media	Yes	95	100
Access Social Media once daily	Yes	94	98.9
	No	1	1.1
	Total	95	100
Aware of Terms and Conditions	Yes	82	86.3
	No	13	13.7
	Total	95	100
Read Terms and Conditions	Yes	21	77.9
	No	74	22.1
	Total	95	100
Social Media Rules does not affect me	Yes	48	50.5
	No	47	49.5
	Total	95	100
Responsible for Post on Social Media	Yes	66	69.5
	No	29	30.5
	Total	95	100

On the awareness level, most users were always on the social media, post daily on social media (SM) even though not all of them read terms and conditions associated with the different social media platforms which is a big challenge to all users.

As expected based on the quality of the sample, about 100% of the respondents are quite active on social media. Their activities include posting frequently on social media and these posts are sometimes about the occurrences in their lives that gave them happiness, joy or sadness. This

corroborates the trend described in Section 2 that users post details of their private lives on social media and confirms the work of Brake (2014) that there is an increase in personal disclosures while using social media. The results indicate that similar trend applies in Nigeria as well. However, it is interesting to note that despite the high quality education of the respondents, over 22% of them do not bother to read the terms and conditions of the social media platforms they subscribe to. For those that did not read the terms and conditions, it appears their awareness of the terms did not matter since only about 14% indicated that they were not aware of them, meaning at least 8% of the respondents did not bother with the terms and conditions even though they were aware of same. It is therefore debatable whether the requirement for users to accept the terms and conditions of use is really of any relevance in protecting the users of the social media platform or are they solely to protect the providers of the platform from liability. This is even more dangerous when the users are not aware of the liabilities they have consented to accept or waive. What is even more intriguing is the finding that out of a population of people who take responsibility for themselves and others, over 50% of them would assert that social media rules do not apply to them and over 30% do not expect to be held responsible for their views on social media. This may be reflective of an attitude that one can get away with anything done on the social media; an attitude that reinforces the need for regulations that at least make users aware of the impact of their actions and of likely consequences. The responses also call to question the reliance that can be placed on users to on their own exercise good judgment in their use of the social media platforms.

TABLE II EFFECT OF SOCIAL MEDIA CONTENTS ON USERS

Social Media Security			
Particulars	**Description**	**Frequency**	**Percentage**
Social Media influences my thinking	Strongly Agree/Agree	52	54.7
	Undecided	11	11.6
	Strongly Disagree/Disagree	32	33.7
	Total	95	100
My opinion and Messages affect others	Strongly Agree/Agree	64	67.4
	Undecided	20	21.1
	Strongly Disagree/Disagree	11	11.6
	Total	95	100
What others think about my opinion and message is their problems and not mine	Strongly Agree/Agree	63	66.3
	Undecided	14	14.7
	Strongly Disagree/Disagree	18	31.5
	Total	95	100
I can defend my post on social media	Strongly Agree/Agree	83	87.4
	Undecided	9	9.5
	Strongly Disagree/Disagree	3	3.2
	Total	95	100

Table II shows the effect of social media security contents on users. It was observed that majority of the respondents believe that social media contents affect frequent users. As shown, a simple majority of 55 (55%) of the respondents agree/strongly agree that social media influences their thinking. Similarly, majority of the respondents (67%) strongly agree/agree that their opinions affect others while 20 (21%) of them think otherwise. This reiterates the level of awareness of respondents of the implications of their acts and conducts on social media and emphasizes the moral hazard users. More than 12% of the respondents were unsure of the truth of their posts on social media. At least 3% admitted users are exposed to as they refuse to accept responsibility for their posts on the social media platforms even when they expect that their posts will impact other people. Invariably, large portions of social media users are aware that their unwitting post of criminal acts or even their progresses/ successes has the capacity to influence other users. However, majority of the users are unbothered about the aftermath of their posts as only a few respondents set at 18 (32%) disagree/strongly disagree that the thoughts of other users about their post is not their problem but that of the other clearly that they could not defend their posts creating the possibility that at least 3% of social media content in

Nigeria cannot be substantiated. In a world of heavy social media interactions and the recorded impacts of false information and fake news, this is indeed a worrisome trend that requires some attention.

TABLE III AWARENESS OF REGULATIONS AND CYBER SECURITY

Awareness of regulation and cyber security			
Particulars	**Description**	**Frequency**	**Percentage**
Social Media Activities are under Regulation	I can be traced	44	46.3
	Litigations may arise from my post	26	27.4
	The apps have my data	25	26.3
	Total	95	100.0
Prevention of litigation from Social Media Use	Be well informed	37	38.9
	Avoid inciting posts	10	10.5
	Avoid unnecessary likes or comments	48	50.5
	Total	95	100.0
Fake news is dangerous	Avoid at all cost	90	94.7
	Can ignite violence	5	5.3
	Total	95	100.0
Social Media Circle	Family	87	91.6
	Business	3	3.2
	Political	2	2.1
	Education	3	3.2
	Total	95	100.0
Profile open to the public	Only when I am online	26	27.4
	Not open to the public	21	22.1
	Always open to everyone	48	50.5
	Total	95	100.0
Social media terms and condition protects users	Yes	31	32.6
	No	33	34.7
	I don't know	31	32.6
	Total	95	100.0
Social Media Account Protection Type	Single password	9	9.5
	Two steps verification	86	90.5
	Total	95	100.0
User's social media account that has been hacked	Facebook	82	86.3
	Twitter	13	13.7
	Total	95	100.0

Table III shows the awareness of regulations and cyber security. It is no longer news that social media activities are under regulations and this should naturally encourage users to be careful of all activities carried out on social media. This research shows that majority of the respondents believe that their identities can ultimately be uncovered regarding their activities on social media. It was observed that 44(46%) of the respondents think they can be traced, 26 (27%) believe that it is possible for litigation to arise as a result of their post on social media while 25(26%) believe that the application stores their records, which encourages litigation. For the prevention of litigation, most respondents believe that the best method is to avoid unnecessary likes or comments as evidenced by the 48(51%) response in support while about 39% expect that more user education can reduce the risk of litigation. It was interesting that only about 11% of respondents will suggest that users avoid making inciting posts in the first instance but would rather place more responsibility on users to exercise judgment on whether to like or comment. This is even more so when virtually all respondents suggest that fake news can be dangerous.

Most respondents, specifically 87 (92%) are on the social media circle with their family relations while others go on social media for business reasons, political and educational purposes as seen in their 3(3%), 2(2%), and 3(3%) results respectively. This shows that most social media users engage with their close contacts via the social media and confirms that social media interactions are now intertwined with everyday living for most people. This also shows the range of people that can potentially be impacted by the irresponsible behavior or compromise of one social media account. Those impacted will include close family and friends as well as business and political associates who could then go on to impact other people in their networks as well. The question of respondents consciousness of when their profile is open to the public was answered in three ways: majority of the respondents believed that it is always opened to everyone with 48(51%), 26 respondents (27%) believe that their profiles are only opened to the public when online while a third set of users representing 22% claim that their profiles are not open to the public.

'Table III shows the respondents' perception of the protection level afforded by the terms and conditions of social media platforms. Regarding the belief as to whether or not social media users are protected by the terms and conditions, the respondents are torn between a positive response at 34% as against 33% which believe either the terms or conditions do not protect or simply have no idea. This indicates a lack of faith in the social media platforms to actively protect the users or a lack of understanding of the protections offered despite about 78% of respondents taking the time to read the said terms and conditions (see Table I).

The vulnerability in software is on the rise and as a result, the security of users needs to be prioritised. With this development, knowledgeable users are expected to protect their mobile devices. Majority of the respondents that is, 86 (91%) chose the two steps verification password to protect their social media accounts while about 9.1% adopt single password. In addition, respondents were asked if their social media has ever been hacked and majority of the respondents to the tune of 82 (86%) indicated that their Facebook account had been hacked at one time or the other while only few respondents representing 13(13.1%) indicated that their Twitter handle were hacked. This goes to corroborate the possibility of an identity theft through the frequent use of social media. The need for enhanced security becomes even more important when one considers the wider spread of people likely to be impacted by a security breach on one person's account.

V. RECOMMENDATIONS AND CONCLUSION

In this study, the level of awareness of social media users to cyber security issues was examined and the findings showed an impressive awareness level of the possible impacts of the acts and conducts of the users on others as well as the risks to cyber security. Unfortunately, the social media accounts of many of the respondents had been hacked or hijacked in the past which should give the respondents some sort of firsthand experience. This translated to majority of the users adopting two-stage verification on their mobile devices. Nonetheless, only a few respondents demonstrated understanding or concern for the impact of their actions on social media on the security of others. While the common thinking is that psychology and emotional intelligence is now required in using social media platforms, there is significant evidence that users are looking to avoid responsibility for the impact of their social media interactions on others and rather expect other people to worry about how they manage such impact. Whilst there may be views opposing the regulation of social media, the moral hazard created by the lack of responsibility for posts and actions on social media must be recognized. The results of this research supports that some form of regulation of social media may be necessary to ensure that users are at least mindful of the consequences on their actions on the various platforms. Such regulations could potentially include valid identification etc. although this must be moderated to ensure it is not abused as another means to obstruct freedom of expression and other constitutionally guaranteed freedoms. There is also the need for social media platforms to emphasize the security of their users and not merely be focused on their own private objectives and such efforts needs to be better communicated to users through the terms and conditions section as well as through other relevant means.

REFERENCES

[1] R. Widdison, "Electronic Law Practice: An Exercise in Legal Futurology," *The Modern Law Review*, Vol. 60, No. 2, pp. 143-163, 1997.

[2] Cambridge Dictionary, 'Social Media' Cambridge Dictionary, Retrieved from https://dictionary.cambridge.org/dictionary/ english/social-media 2021.

[3] Kaplan, and M. Haenlein, "Users of the world, unite! The challenges and opportunities of social media," *Business Horizons*, Vol. 53, No 1, pp. 59-68, 2010. [Online]. Available: https://dx.doi.org/10.1016/j. bushor.2009.09.003, 2010.

[4] D. Leary, "Knowledge Management and Enterprise Social Networking: Content Versus Collaboration," *Social Science Research* Network, [Online]. Available: http://dx.doi.org/10.2139/ssrn.2773273, 2016.

[5] J. Wharton, "The Impact of Social Media: Is it Irreplaceable," Knowledge@Wharton, [Online]. Available: https://knowledge. wharton.upenn.edu/article/impact-of-social-media/ 2019.

[6] H. Tankovska, "Facebook: Number of monthly active users worldwide 2008-2020. Statista', [Online]. Available: https://www.statista.com/ statistics/264810/number-of-monthly-activefacebookusersworldwide/#:~:text=With%20over%202.7%20billion%20monthly,network%20e ver%20to%20do%20so, 2021.

[7] G.Tiso, [Online]. Available: https://newhumanist.org.uk/articles/ 5358/ time-to-log-off 2018.

[8] H. Kim, "Online Social Media Networking and Assessing Its Risks," *International Journal of Security and Its Applications*, Vol. 6, No 3, pp. 11-18, 2012.

[9] British Broadcasting Corporation (BBC), "Obinwanne Okeke: Nigerian email fraudster jailed for 10 years in US. BBC News," [Online]. Available: https://www.bbc.com/news/world-africa-56085217, 2021.

[10] M. Shepherd, and M. Admire, "#ThisFlag: Social Media and Cyber-Protests in Zimbabwe," *Social Media and Elections in Africa*. [Online]. Available: https://dx.doi.org/ 10.1007/978-3-030-32682-1_9, 2021.

[11] O. Abimbade, O. Philip, and D. Herro, "Millennial Activism within Nigerian Twitterscape: From Mobilization to Social Action of #ENDSARS Protest," *Social Science Research Network*, [Online]. Available: http://dx.doi.org/10.2139/ssrn.3760973, 2021.

[12] C. Dewey, "Facebook Fake-News Writer: I Think Donald Trump is in the White House because of Me. Washington Post," [Online]. Available: https://www.washingtonpost.com/news/theintersect/wp/2016/11/17/facebook-fake-news-writer-i-think-donald-trump-is-in-the-white-house-because-of-me/, 2016.

[13] J. Parkinson, "Click and Elect: How Fake News Helped Donald Trump Win a Real Election," Guardian [Online]. Available: https://www.theguardian.com/commentisfree/2016/nov/14/fake-news-donald-trump-election-alt-right-social-media-tech-companies, 2016.

[14] H. Brown, E. Guskin, and A. Mitchell, "The Role of Social Media in the Arab Uprisings," *Pew Research Centre Journalism and Media*, [Online]. Available: https://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/, 2012.

[15] C. Ekoh, and E. George, "The Role of Digital Technology in the End Sars Protest in Nigeria, 2021.

[16] E. Kambellari, "Online Impersonation: I have a right to be left alone. You can't mandate how I use my privacy toolbox," Timely Tech @ University of Illinois. pp. 112, 2017.

[17] Cambridge Dictionary, "Security' Cambridge Dictionary" [Online]. Available: https://dictionary.cambridge.org/dictionary/english/security, 2021.

[18] British Broadcasting Corporation (BBC), "Facebook Data: How it was used by Cambridge Analytica," BBC News, [Online]. Available: https://www.bbc.com/news/av/technology-43674480, 2018.

[19] M. Hanna, and J. Isaak, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer*, Vol. 51, No. 8, pp. 56-5, Retrieved from https://doi.org/ 10.1109/MC.2018.3191268, 2018.

[20] A. Kamal, "The Law of Cyber-space – an invitation to the table of negotiations," United Nations Institute of Training and Research, [Online]. Available: https://www.un.int/kamal/sites/www.un.int/files/The-Ambassador's-Club-at-the-United-Nations/the_law_of_cyber-space.pdf, 2005.

[21] Hargrave, and S. Livingstone, "Harm and Offence in Media Content: A review of Evidence," 2nd Revised Edn Intellect, Bristol UK, 2009.

[22] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the internet: The perspective of European children," Full Findings, LSE, London: EU Kids Online, 2011.

[23] Livingstone, Brake, "On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications," *Children & Society*, Vol. 24, No. 1, pp. 1-9, 2009.

[24] D. Brake, "Sharing Our Lives Online: Risks and Exposure in Social Media," Palgrave Macmilian, DOI: 10.1057/9781137312716, 2014.

[25] J. Jang-Jaccard, and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, Vol. 80, No. 5, pp. 973-993,2014.

[26] C. Ukpong, "Missing Akwa Ibom Woman raped, killed by man who promised her job," Premium Times, [Online]. Available: https://www.premiumtimesng.com/news/headlines/459002-missing-akwa-ibom-woman-raped-killed-by-man-who-promised-her-job-police.html, accessed 18 July 2021.

[27] S Kite, and R. Gable, "Cyber threats: a study of what middle and high school student know about threatening behaviours and internet safety," *International Journal Social Media and Interactive Learning Environment*, Vol. 1 No. 3, pp. 240-254, 2013.

[28] C. Barlow, J. Morrison, S. Stephens, H. Jenkins, E. Bailey, and M. Pilcher, "Unprofessional behaviour on social media by medical students," *The Medical Journal of Australia*, Vol. 203, No. II.

[29] Amnesty International, "Nigeria: Bills on hate speech and social media are dangerous attacks on freedom of expression," [Online]. Available: https://www.amnesty.org/en/latest/news/2019/ 12/nigeria-bills-on-hate-speech-and-social-media-are-dangerous-attacks-on-freedom-of-expression/, 2019.

[30] British Broadcasting Corporation (BBC), "Ecowas court order Nigeria to lift ban on Twitter," [Online]. Available: https://www.bbc.com/pidgin/world-57572699> accessed 18 July 2021.

[31] L. Lessig, *Code Version 2.0*, Perseus Books Group New York, 2006.