Sub-Sahara African Academic Research Publications
September, 2020 Editions

JHSS
Journal of Humanities and Social Science.
Vol.16, No.6, ISSN:2316-7989

PRIVACY ON FACEBOOK; AWARENESS, CONCERN AND ONLINE BEHAVIOUR

***BASHIRU USMAN; AND **ABUBAKAR TUKUR LIMAN**

**Department of Mass Communication, Adamawa State Polytechnic, Yola, Adamawa State, Nigeria **Department of English Education, Adamawa State Polytechnic, Yola, Adamawa State, Nigeria*

ABSTRACT

It is an indisputable fact that social networking sites have redefined communication and penetrated virtually every sphere of human endeavours, connecting the world in an unimaginable manner. In a spur of a moment the technology gained popularity across continent and countries faming the world with surreal communication experiences. However, shrouded in the shines of the digital interaction is a multidimensional security and privacy issues that can subject the social media users to stinking consequences. Facebook being one of the social networking sites, and the most popular platforms for that matter, has its peculiar and general challenges. Therefore, this paper explores the general security/privacy issues on social networking sites with more emphasis on Facebook. The researcher applied qualitative approach to review the content of extant studies conducted in the area to determine the social media users' awareness and concern about the challenges with view to gauge the extent of the concern vis-à-vis the prevalent security and privacy challenges to ascertain users' readiness to quit Facebook. The essay concludes that, though the users value their privacy and wary of security threat there on, they prefer available precautionary to completely quitting the social networking sites. Finally, the paper recommends ameliorative steps at individuals, apps developers and states levels to mitigate threats and ensure safety and fair play on the platform.

Keywords: *Social media, Facebook, Privacy, Awareness, Concern, Online Behaviour*

INTRODUCTION

Advancement in the internet and internet of things technologies in a couple of decades has transformed information creation, dissemination and consumption to a most flexible, eased and interesting experiences. Social media as a key player in the modern communication succeeded in reducing the world to a village that can be explored by "clicking" on a palm size device. The sites are so pervasiveness that they penetrate virtually every home, organization, institution and sector knitting social, business, educational and religious domains. Sudden growth of the social media come with both benefits and losses as it becomes a prime target of cybercriminals, corporate bodies and the platforms' developers who work tirelessly strategizing ways of tapping users personal information for various criminal, commercial and surveillance activities. Winseck as summarized in Lyon, (2003) laments that valuable private information are generated in form of user profile, customer details or enrolment data while some of the systems are quite aware of weakness of their data protection mechanisms. This situation is obtainable in virtually all the social platforms.

Facebook being the most popular and widely used social networks succeeded in penetrating most countries and continents (Pempek et al., 2009). It was launched in February 2004 by Mark Zuckerberg as "Thefacebook", chiefly to connect students of Harvard University and enable them share opinions, experiences, information and amusements. It was also for them to know their classmates, school mates and events transpired in the school (Lee, 2007) open access was given to all students with Harvard university e-mail, and subsequently to all interested cybernauts. Facebook is a free social networking site which allows members to upload and share photos; post and publish information, opinion or ideas; get the latest news feed from friends; post videos on their profiles; tag friends at will; and send and receive text messages among others. Although in its novelty days it was cascaded into School, corporate and regional networks, the division were removed in 2009 to make it a seamless network (Zuckerberg, 2010). The sudden proliferation of the platform was largely aided by the introduction of smart phones coupled with internet service provision by GSM service providers. Signing up Facebook account requires much personal information including active e-mail address name, surname, Date of birth, address, phone number, educational status, marital status and gender pictures, events, location and city of

residence to mention just a few. In view of sensitive nature of the information provided, the social networking site providers devised mechanisms to protect such information against unauthorized use by potential cyber criminals and intruders. The privacy settings enable users restrict access to their personal information on the platform (Aldhafferi et al., 2013). Although, this measure is a good step, it left to be desired as user private data still face intrusion inform of data mining by institutions, governments, companies, organizations, bankers, and enterprises resulting to risk of identity theft, hacking, stalking, eavesdropping and commodification. Worse still, complexity of the cyber cloud, flexibility of the internet and pervasiveness of social media contribute to the spread of security threat and privacy violation (Steijn & Vedder, 2015). Thus, privacy and security protection on Facebook has over the years been the major concern of its users.

Consciousness of rampant privacy right violations and data misuse triggered concern about online data privacy due to complexity and porosity of the cyber-cloud which seemingly defy safety and control mechanism (Külcü & Henkoğlu, 2014). These are shady third party deals, surveillance, privacy right dispossession and cybercrimes like, phishing, stalking, hacking, spamming, identity theft and cyber harassment among other harmful activities (Aldhafferi et al., 2013). This is evident in Cambridge Analytica saga and revelations of Edward Snowden and Mr. Tim Clemente that NSA and FBI illegally intercept and harvest all digital communications. This study therefore examined the privacy/security issues on Facebook to gauge users' awareness, concern and online disclosure.

Privacy

Privacy is a difficult term to define. It attracts different interpretations which make it impossible for the concept to assume a particular definition that is accepted by all. Hence, it is often defined contextually. Although, privacy is a universal phenomenon playing a significant role in proper functioning of humans and maintaining decorum among members of various societies (Kasper, 2016) its understanding is dependent on cultural norms and values which vary from place to place (A. D. Moore, 2003). Therefore, what privacy entails in one community, society, or group might not be obtainable to the others. Moore, (2008) observes that bashing into a room without knocking is a serious privacy violation in some cultures and yet permitted in others.

Privacy is seen as a control over access to self; determining who accesses private information; and preventing unauthorized exposure and usage (Cavusoglu et al., 2013). Privacy is also seen as the freedom from intrusion disturbance and interference in one's personal affairs (Blizard & Turner, 2011). Solove, (2002) & Holvast, (2007) unanimously argue that there are six traits of privacy rooted in many recurrent definitions, these are: (1) right to be let alone; (2) limited access to the self; (3) right to keeping one's information secret; (4) control over personal information; (5) protection of one's personality and dignity; and (6) right to determine who, when and how to grant or deny access to one's personal affairs. Privacy is a control over access to personal details, location and domicile as well as protection of body, reputation and personality against violent access or utilization. Warren and Brandeis view privacy as "the right to be let alone". Privacy does not mean an absolute confidentiality in which nobody has access to information *per se*, rather it is an ability of an individual to allow selective release of personal information about them to whoever they feel comfortable sharing with (Shullich, 2011). Privacy is a tort that protects user from invasions of privacy characterised by intrusion upon seclusion, public disclosure of private facts, false light or publicity and appropriation (A. Moore, 2008). This torts formed part of American jurisprudence though, technological advancement necessitated review of the torts to address the current situation. In whatever way one may define it, privacy has common attributes cutting across all boundaries. These are: right to have control over one's information; power to determine access; and freedom from any form of intrusion.

In view of its relevance, privacy is valued in virtually all societies. For centuries it has been recognized and protected by both primitive and modern laws. In America for example, privacy protection law was strengthened in the third and fourth amendments to limit boundaries to be crossed by security agents and census officials. It was meant to address the prevalent issues of invading people's houses and rooms during war period in guise of keeping security (Holvast, 2007). The fourth amendment categorically states that:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"*(Fourth Amendment, 1791).

Thenceforth, many privacy protection measures in the phase of law were taken with a view to protecting people's privacy. Warren & Brandeis, (1890) observes that

> *Privacy of the Body which protects Americans against physical privacy violation was established in response to privacy violation by media which then characterized sensationalism, yellow journalism, gossips and defamation .Similarly, Privacy is enshrined in the Universal Declaration of Human Rights (UDHR), 1948, as a distinct human right. Article 12 reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (UNESCO, 2012).*

In 1960s and 1970s, the fourth amendment was revolutionized by laws such as: New Limits on Government Surveillance; The Constitutional Right to Privacy; and Responses to the Rise of the Computer, Financial Privacy 1970. More so, in 1980s and 1990s advancement in computer technologies, spread of the internet and emergence of World Wide Web warranted reshuffle and enactment of many laws to contain the emerging Changes. These include: Article 11 of American Convention on Human Rights (ACHR): "*(2) No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation. (3) Everyone has the right to the protection of the law against such interference or attacks"*(UNESCO, 2012). Similar privacy protection laws are also found in Article 8, of European Convention on Human Rights (ECHR); Directive 95/46 of EU Data Protection Directive; Directive 2002/58 concerning the protection of privacy in electronic communications (e-Privacy Directive); Directive 2006/24 on the retention of data (Data Retention Directive); African Charter on Human and Peoples' Rights; Article 40 of Chinese Constitution; Article 21 of Indian Constitution; Articles 226-1 to 7 of France Penal Code (Solove, 2006). Aldhafferi et al, (2013) opines that privacy has to do with allowing personal information access to restricted entities in order to protect their information against misuse by mischievous persons. In many countries, right to privacy is given not only cultural backing but legal as

well. In the United States for example, the privacy right is a personal and fundamental human right. The emerging technologies particularly the internet and 'internet of things' reshaped and redefined privacy (UNESCO, 2012). This prompted debates on attributes that constitute privacy. Powell, (2011) observes that, these days it is quite difficult to define privacy outside the purview of huge amount of individuals' private data online. Thus, Finn et al, (2013) state that there are seven types of privacy which include "privacy of the person; privacy of behaviour and action; privacy of personal communication; privacy of data and image; privacy of thoughts and feelings; privacy of location and space; and privacy of association. Virtually all forms of privacy mentioned in the previous particular those of behaviour, action, personal communication, data, image, and location are threatened by prevalent of the internet and internet of things.

Social Media Privacy

The social media has become part people's lives that it draws attention to concern about the fate of users' privacy in the vulnerable cyber-cloud (Buccafurri et al., 2015). Risk of privacy leakage is the biggest problem as many users fail to understand the implication of revealing their personal information (Asif & Khan, 2012). It is designed in such a way that users are stimulated to release their personal information. Perhaps because of the business motive the designer has on the information (Buccafurri et al., 2015). Mostly, information posted and shared on the social networking sites are of two types: Profile information including photos, name, e-mail address, home address, phone numbers, location, date of birth, educational status, marital status, spouse's name and interest; and non-profile information including: news feed, status updates, tags, friends list and timeline messages etc (Tsikerdekis & Zeadally, 2014). Consequently, people become concerned about their privacy on the social media. Steijin et al, (2015) observes that recent debates among privacy experts mostly focused on privacy risk on social media like sharing information on the internet in general and on SNSs in particular. Much attention has been drawn towards the privacy risks associated with profiling on the basis of data mining. It is very vital to efficiently protect users' privacy in social media. Certainly, the social media came with many benefits of making communication much easier and cheaper connecting and reconnecting with new people and old friends. However,

personal data provided on the SNS are so sensitive enough to expose users to various forms of Privacy risks (Finn et al., 2013). Golbeck & Mauriello, (2016) learns that, the social media providers commoditize users' data for financial gains which is inimical to the safety of users' privacy. Social media rely on advertising hence personal data of user is the key commodity. The sites therefore, obtain and sell the data to enable them remain profitable and afloat (UNESCO, 2012). Similarly Schwartz, (2016) laments that social media consumers are often not conversant with the increasingly complex methods devised to collect information about them, let alone evaluation mechanisms. Unfortunately, social media platforms earn huge amount money in share users' sensitive information with corporate bodies, organizations, institutions and companies that often fail to preserve the information either because of their commercial interests or weak access control (Wirtz et al., 2007). Social Networking sites make billions from manipulating users' personal data (Fuchs, 2011). These activities violate and expose people to serious privacy risk (Shullich, 2011).

Facebook

Facebook appears to be the most popular social media whose coverage cut across virtually all forms of barriers. The platform created a community with all sort of members (Croom et al., 2016). In fact Facebook is the most heterogeneous community on the earth with over 2 billion people from diverse cultural, geographical, racial, religious, financial and educational backgrounds. The Facebook community members are united by a culture of sharing and interacting with friends, family members, business partners and colleagues online. Indeed, Facebook enjoys fast growth within just a decade of its establishment to the extent that many believe that its population outnumbers that of Chinese. The platform keeps developing and strategizing ways of attracting more users through providing user friendly and captivating features. Facebook asserts it gives users the power to share as part of its mission to make the world more open and connected seamlessly across diverse communities (Facebook, 2016). The platform is one of the widely used social media whose privacy settings drew attention of privacy concern individuals and organizations since the social network was made public in 2006 (Hauff et al., 2015). It has indeed succeeded in gaining popularity and acceptance which leads its geometrical growth. The users are comfortably

sharing astonishing amount of data including personal information (Kirkpatrick, 2010).

Privacy and Security Issues on Facebook

Despite the role of Facebook in transforming communication, it exposes users' personal information which results to risk of gross privacy abuse. The platforms demands a lot of information about user, but fails to protect such information (Chen et al., 2017) thus, allowing it open to the access everyone thereby violating privacy rights. Hence the hacking that exposes accounts of 50 million Facebook users (Isaac & Frenkel, 2018). The platform lacks a cogent mechanism for enlightening users about the state of their default setting and its implication on their privacy, an action that encourage information sharing and facilitate potential privacy violation (Stutzman et al., 2012, Stern & Salb, 2015). Aquisti and Gross (2006) lament that default profiles of Facebook user clearly shows contact information like personal addresses, email address and cell phone numbers, pictures and location among other sensitive information. The privacy settings are not often used, which leads to privacy risks for the Facebook users. Steijn & Vedder, (2015) observe that young people who constitute the larger percentage of Facebook users are enthusiastically sharing huge amounts of personal information on social media. But unfortunately they scarcely customize their privacy settings (Nyoni & Velempini, 2018) due to inadequate knowledge of the risk involved. Taneja et al., (2014) learn that, controlling access to privacy is determined by user's confidence in its strength to prevent risk of harm. Although, several security measures have been provided to safeguard Facebook users' data, the irony is that some shady activities of the Facebook tilted towards revenue generation seem to undermine safety of users' privacy.

Selling users information; sharing with third parties; exploitative attitudes; as well as weak access control mechanism are some of the factors widening chances of privacy abuse on the platform (Gross et al., 2005). The social media platform focuses much attention on exploiting users' privacy for commercial favours at expense of users' privacy rights (Van Eecke & Truyens, 2010). Sharing users' information with third party, placing cookies to monitor users' activities and selling users' information favour Facebook economically at the expense users' privacy right. Zlatolas et al., (2015) lament that users are mostly ignorant of the nature of data Facebook gathers about them, and what

it does with the data. This presents dangers such as identity theft, hacking, blackmail, spamming, pharming and phishing (Mohamed et al., 2015). Wua et al., (2014) observe that users provide their information for easy recognition and identification by friends end up in wrong hands. The way Facebook collects and manipulates users' personal data for financial favours confirmed the statement attributed the Zuckerberg the CEO of the Facebook that "privacy is dead"(Richard, 2010). Facebook believes that, sharing is a "new social norm", which has overshadowed privacy value (Hoanca, 2016). Wu, (2015) observe three main factors that bedevilling the security of Facebook users' privacy. These are: (a). Facebook profile open and thoroughly descriptive in such a way that users are easy recognized or identified. (b). Facebook proprietors floundered to care and protect the users' privacy. (c). There are other parties hunting for users data through Facebook. These subject users to crimes including hacking, security number theft, identity theft, attack and surveillance. This is an online crime whose victims are mostly social media users. It involves stealing users profile details and uses it in a malicious way.

(1) Facebook commercially motivated comprise (adware, spamming, third parties,):

- **Adware:** The data users provide in their profiles are the primary data Facebook gathers; these include Names, e-mails, photos, interests, likes, dislikes and educational backgrounds amongst others information for commercial purposes. It devises multiple strategies to track users, analyse their interests and behaviours for profiling and advert placement based on individual user's interests. In a complex way, the platform records audio calls, video clips and mines photos, all contacts and text messages on the host devices. Other data include posts, comments and lot more information (Jin, 2018). Facebook also gets information from its partners like advertisers, app developers, and publishers through Facebook pixel and Business Tools including social plug-ins, like buttons, Facebook Login, APIs and SDKs. These partners provide information about users activities off Facebook—including information about their devices, websites they visit, purchases they make and the ads they see (Jin, 2018). Facebook collects even data about what people are shopping for and looking at on the web to easily analyse the aggregated user behaviour (Neld, 2020). The tools are

used for mining data of even those without Facebook account (Privacy International, 2018). An example is the travel search and price comparison app "KAYAK", which sends people's flight searches and itinerary details to Facebook, including: departure city, departure airport, departure date, arrival city, arrival airport, arrival date and ticket numbers of various classes (Privacy International, 2018). Thus, site owners are able to build up a profile of pages visitors (Neld, 2020).

- **SPAMMING:** Facebook mines e-mail addresses and phone numbers on host devices for corporate promotional spams irrespective of the interests of the consumers. It also harvests addresses of even users of its partners who have no Facebook accounts. Moreover, cybercriminals sometimes hack such information in order to send fraudulent mails and messages sometimes inform of wall post, newsfeed adverts or hyperlinks that lead to stinking consequences (Chewae et al., 2015).

- **Third party:** Facebook as an application does not operate in isolation, it relates symbiotically with partner applications and developers for commercial purposes. It usually shares data with third parties like online games and other applications as a means of generating revenue (Okesola & Marthie, 2014). Mahmood, (2013) observes that Facebook charges thirty percent of third party applications' revenue for giving access to its ecosystem. It is worrisome as neither the Facebook nor its users have control over the data shared with a third party, hence the data is prone to misuse (Stutzman et al., 2012) evident in unethical behaviour exposed by Cambridge Analytica scandal. Calbalhin, (2019) laments that such a third party can use the information shared with it to gain access to more information for its benefit without users consent. Worst still, some of these third parties sell users information to malicious applications who can unleash serious online terror on users (Mahmood, 2013). More so, Facebook also gets information from other apps, developers, SDKs and other partners. Privacy International, (2018) found that, Facebook gathers even information about users who haven't signed in or have Facebook account in manner that often bypass its data policy. For example Privacy International (2019) reveals that the Apps that share information with Facebook include Calorie Counter - MyFitnessPal, Duolingo: Learn Languages Free,

Family Locator - GPS Tracker, Indeed Job Search, Instant Heart Rate: HR Monitor & Pulse Checker, KAYAK Flights, Hotels & Cars, King James Bible (KJV) Free, Muslim Pro - Prayer Times, Azan, Quran & Qibla, My Talking Tom / My Talking Hank, Period Tracker Clue: Period & Ovulation Calculator, Qibla Connect® Find Direction- Prayer, Azan, Quran, Shazam, Skyscanner - Cheap Flights, Hotels and Car Rental (Ad Personalisation = Off), Skyscanner - Cheap Flights, Hotels and Car Rental (Ad Personalisation = On), Spotify Music, Super-Bright LED Flashlight, The Weather Channel: Local Forecast & Weather Maps, TripAdvisor Hotels Flights Restaurants Attractions, VK (vkontakte), Yelp and صلاتك Salatuk (Prayer time). Facebook also apply cookies to monitor online activities like sites visited, links followed, posts and comments etcetera, to profile users' interests and relevant adverts placement (Privacy International, 2019).

- ✓ **AI (Artificial Intelligence)** is applied in analysing the information scooped through the cookies and other algorithms. Facebook uses Artificial Intelligence usually helps in building a virtual profile of individual users and groups in order to target them for the adverts and automated activities. Privacy International, (2018) found that AI applications have the following features:

i. **Re-identification and de-anonymisation:** AI applications can be used to identify and thereby track individuals across different devices, in their homes, at work, and in public spaces. For example, while personal data is routinely (pseudo-) anonymized within datasets, AI can be used to de-anonymise this data. Facial recognition can also be used tracked and identify individuals, which has the potential to transform expectations of anonymity in public space.

ii. **Discrimination, unfairness, and inaccuracies, bias:** AI-driven identification, profiling, and automated decision-making may also lead to unfair, discriminatory, or biased outcomes. People are prone to misclassification, misidentification, or misjudgement, and such an error may disproportionately affect certain groups of people.

iii. **Opacity and secrecy of profiling:** Some of the AI applications can be opaque to individuals, regulators, or even the system designers,

making its outcomes difficult to challenge or questioned. Although, there are technical solutions to some systems interpretations and audit by different stakeholders, where it impossible the challenge impacts significantly on people's lives.

iv. **Data exploitation:** People often find it difficult to understand the nature and magnitude of data their devices, networks, and platforms generate, process, or share? Frequent use of the internet and internet of things in public places, private spaces and even wearables, bolster up AI profiling, tracking and identification of netizens across devices (Privacy International, 2018).

(2) Fraudulent Attack/identity theft include: Holvast, (2007) Holvast learns that identity theft is one of the most fastest growing online fraud challenging social networking sites. It involves using another person's identity tapped through social media including the person's name, date of birth, address, social security number, credit card numbers, account information and other sensitive information. The identity theft is of various forms viz:

i. **Cloning:** criminals use profile data to create another fake account using the same information and send friendship request to friends of the victim. Thus, anyone who accepts the request has his personal data accessed by the cloner. Another way is stealing users' information on a social media account and creates an account on another social media using the information and send friendship requests to the victim's friends. For example, stealing profile information on twitter and use it to create Facebook account and send request to the victim's friends viewed on twitter. This is quite tricky as users usually accept requests from people they know thus, they easily fall victims of this type of identity theft (Gunatilaka, 2011).

ii. **Social phishing:** Usually phishers target financial information to defraud victims. The phisher creates a website exactly like a bank authentic site to convince potential victims provide their sensitive data like financial information, password or identification number to the pseudo site. The phishers scoop data from social media like Facebook, to accomplish their mission. The attackers often send phishing sites using the potential victims' friends' name. They use profiles to extract account details which can be used to inflict financial harm (Kumar et

al., 2013). Hashed out, 2020 reports that phishing activities constitute 32% of the world's cybercrime.

iii. **Fake product Advert:** Attackers sometimes study Facebook users' interests and target them with fake product advert offering attractive discounts. If a user clicks on the product their information automatically goes to the fraudster (Kumar et al., 2013).

Koobface:

It is a type of worm that infects computers and other internet of things through social media platforms to gathers sensitive information of users. The worm infiltrates devices by clicking on malicious links, apps, pop ups, spam emails, raunchy videos and adverts (Thomas & Nicol, 2020). The perpetrators also spread the worm through messages sent between friends on the social media (Rajesh et al., 2017). When a user clicks to follow a link or apps update suggestion, it can take control of the internet traffic to steal sensitive information for use and further infect all devices connected to the server. (Gunatilaka 2011, Chewae et al. 2015, Ackerman & Schutte, 2015). The forms of Koobface popular on Facebook are clickjacking and likejacking, the hackers usually presents a video similar to YouTube, captivating picture, link a clicks on which leads to compromise of the data of both user their friends. Unwary Facebook users are usually are at risk of such an attack (Kumar et al., 2013). A study identified fraudulent and compromised social network accounts used to spread malicious links to over 213,000 social network users which generated over 157,000 clicks (Thomas & Nicol, 2020). Virtually all sensitive information on social networking sites or its third party partners make hacking. For example, an online security consultant Ron Bowles in 2010 hacked and posted personal data of 100 million users online(Das & Sahoo, 2011, Paullet & Pinchot, 2012).

(3) Specific target attack/surveillance involving stalking, spyware:

Cyberstalking: This one of the most popular and overlapping type of online personal harassment. It uses electronic communication channels to subject victims to various online torture including harassment, bullying and intimidation. Begotti & Maran, (2019) laments that the anonymous perpetrator harasses victims, impersonates others and encourages third parties to take part in the Cyberstalking behavior. Lowry et al., (2014) learn that, the motives of the cyberpunk include satisfying curiosity, intimidating or

taking control of the victim, retaliating against or punishing the victim and catching fun. The criminals use emails, social networking sites, online websites, online gaming, and message forums to accomplish their malice (Canadian Internet Policy and Public Interest Clinic, 2008). Victims of stalking usually experience psychological trauma, physical disturbance and paranoia resulting to cyber-phobia and forceful change of online habits. Lowry et al., (2014) classify stalking into Secret, indirect and direct.

- **Secret Cyberstalking:** It involves monitoring, tracing and tracking the victim, though it doesn't involves direct communication of any form, the cyberstalker usually tracks data of the victim secretly without the notice of the victim. The cyberstalker though, processes the information privately, no infliction of harm or malicious intention attached.
- **Indirect Cyberstalking:** has to do with subjecting victims to cyberbullying, embarrassment, defamation, information eavesdropping, impersonation and blackmail. The behaviors usually cultivate long-term harm obliviously.
- **Direct Cyberstalking:** Unlike others, direct stalker communicates with the victim through instant messages, emails, online comments and feedback in manner that both parties are aware of the interactions. The cyberstalker's behaviors usually inflict physical, financial, career, psychological, or emotional harm. It also involves mailing offensive or raunchy texts, photos and videos, horrific threats, extortion, virus transmission, and damaging data or its equipment.

Surveillance is one of the major problems affecting online privacy. Although, surveillance is milder in terms of harmfulness than other crimes like identity theft and spamming, it infringes people's right to private life. Usually, such surveillances are done by governments, security agencies, organisations and corporate bodies through data bases managed by various social media platforms and other internet sources. The snoops inter alia monitor victims' digital communications including mails, chats, voice messages and text messages. Although, surveillance is culture traceable from world wars among rival countries, it was reignited by the controversial 9/11 2001 attack on world trade centre, in New York and pentagon. Countries came up with online spy, pry and espionage strategies to forestall and cushion terrorism even at

the expense of privacy rights (Holvast, 2007). Consequently, U.S Promulgated an act "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA Patriot Act) Act of 2001 to empower government and its security agencies like FBI and CIA to secretly penetrate all sort of databases and extract digital information and discussions, chats and any other forms of communication without obtaining a search warrant or other sanction from a due court law (Gordon-Lickey, 2015). The new surveillance strategies do not eschew even citizens as it is claimed to be necessary for forestalling internal and external terrorism. America appeared to be a leading country in terms of violating privacy rights. This is evident in revelation made by an NSA former staff Edward Snowmen's who felt uncomfortable with highest level of human right violation and decided to expose the atrocities (Bernal & Bernal, 2016). The whistle blower exposed how the agency collect exposed how the agency collect social media users' personal information through various programs it designed like prism and bullrum to subject people to surveillance (Mahmoud & Zeki, 2016). Facebook is among the social media platforms whose data is tapped directly by NSA and FBI for surveillance and other activities not intended by the users (Gellman & Polyras, 2013).

Facebook Privacy Awareness and Information Disclosure

Facebook the most popular social networking site in Nigeria with 27.46 users in 2020, and the number is expected to reach 43.53 million by 2025 (Statista, 2020). A study by Onifade et al., (2018) suggest that Nigerian though concern about their data privacy and safety, are not conversant with the safety measures which lead default privacy settings. Online privacy awareness can be defined as having factual and procedural knowledge of online privacy settings, policies, technicalities, laws, institutional data practices and ability to apply same for the purpose of data protection (Trepte et al., 2015). It is a state of acquaintance with the technics of controlling and restricting access to online information. This is because, information disclosure on social media is linked with the trust a consumer have for the platform used. Aïmeur et al., (2016) Argue that willingness to share personal information is dependent on the extent of their satisfaction with the mechanisms designed to preserve user personal data. Awareness of privacy issues on Facebook helps users control access to their personal information (Bartsch & Dienlin, 2016). Thierer,

(2013) observes that many social networking sites are taking steps to raise awareness among their users about how they can better protect their privacy and security. Nyoni & Velempini, (2018) found that many Facebook users still lack privacy awareness (Calbalhin, 2019) of strategies of user data mining, the nature of the data, how it is shared and for what purpose? A study on self-disclosure on Facebook reveals that majority of subscribers publish sensitive data like phone numbers, their relationship status, location, email address, residential address and birthday to an average of 300 friends (Mohamed et al., 2015). Social response theory suggests that an individual develop habit of self-disclosure on social media platforms is stimulated by a similar self-disclosure from online friends (Li, 2012). Similarly, Li, (2012) suggests that low perceived benefits, low coping appraisal and high risk appraisal results to reluctance to disclose personal data. Information disclosure specifically involves exposing certain information about oneself. However, the other side of the unrestricted sharing on Facebook is privacy risks capable of causing serious psychological, social, physical and financial damages (Wuest, 2010). Livingstone, (2008) found that defective interface and internet illiteracy makes it quite difficult for students to handle social networks' privacy settings. Some of these also paved ways for users to share personal information among themselves (Boyd M. Danah & Ellison, 2007). Hence, incautious online behaviour triggers fear of theft and abuse prompted a need for privacy control. However, the burden of controlling access to privacy lies with the user. The Facebook access control mechanism changes in manner that invalidates some privacy settings without notifying users. Hoy & Milne, (2010) learn that users' awareness of Facebook practices heightened privacy concerns.

Facebook Privacy Concern and Behaviour

Information privacy concern is seen as a discomfort about the way personal information are tapped and used by organizations, institutions and corporate bodies (Hauff et al., 2015). Openness of the Internet and social networking sites allows personal information to be easily collected, stockpiled, stored, processed, and used by multiple parties, both within and outside a specific economic exchange, thereby making information privacy concerns a major issue in the information age (Pavlou, 2011). Asif & Khan, (2012) observe that, Privacy leakage is the major problem of social networking sites as many users

fail to understand the implication and dangers involved in revealing personal information online. Golbeck & Mauriello, (2016) found that Facebook apps users do not know the type and magnitude of data those apps could access and how it could be shared, hence the less concern about privacy. Although, both Facebook and other social media platforms provide "terms and Condition one can accept, before proceeding to create account, the vague and blurring language used in designing the terms conceal the actual policy and create obtuse mindedness among the users. O'Bien & Torres, (2012) observe that though Facebook's lapses in privacy policies earns it low levels of trust, though, its membership continues to rise which suggests that users prefer pushing trust issues aside to achieve social interaction. While the way users data are manipulated and retained is not clearly stated (Liu et al., 2011). Ali et al., (2019) found that privacy concern triggers users to embrace cautious online behaviour to limit the possibility of attacks and check vulnerabilities. A study by Steijn & Vedder, (2015)reveals that people are concerned about their informational privacy and the concern is chiefly caused the deteriorating state of privacy characterized by gathering of personal data online by companies or governmental organizations such as Facebook and the NSA. A similar study indicated a relationship between social networking sites user's culture, the level of privacy concern and pattern of the social media use (Rashidi & Camp, 2016). In many societies, privacy is culturally rooted, hence the high regard some individuals have for the privacy particularly at this technology age that reduced private information of billions to a mere article of commercial value with or without their consent. Fogel & Nehmad, (2009) found that women are more concerned about their privacy and more secretive in terms of disclosing identity information than men. A reveals that online privacy concerns could lead the social subscribers to deliberately use inaccurate personal information for online registration, exploit privacy settings, and wary of visiting suspicious website (Chen et al., 2017).

Steijn & Vedder, (2015) found that, adolescents are less concerned about their privacy, freedom and security than young adults. O'Bien & Torres, (2012) Argue that rise in privacy concerns affect trust levels, which in turn will limit interactions and exchanges between entities and vice versa. Ikhsan et al., (2013) in a study found that majority of students are concerned about data protection on Facebook, hence frequent change of privacy setting in their profile. A study of 553 students of a German University shows that Facebook

users resorted to designing a suitable self-disclosure strategies to manage and protect their privacy in manner that satiates their scepticism and privacy concern (Krasnova & Kift, 2012). Finally, Social Networking sites pay more attention to making billions out of users' personal information. This is through exploiting the users through violating their rights without any compensation. Wu, (2015) suggests that Facebook should be paying its users. Usually they prioritize advert chances and exchange of users' private data regardless of inconveniences it may cause them.

CONCLUSION

Social Networking sites have become a part our daily life with billions of people navigating within and across social media platforms exploiting the multifaceted communication options championed by technology advancement. Facebook is appears to be the most populous platform with over 2.5 billion users worldwide out of whom over 2.7 million are Nigerian. However, the sites like another application are not without challenges owing to the porosity and complexity of the cyberspace coupled with interests of the apps developers, governmental and non-governmental agencies and cybercriminals occasioned multidimensional ills ranging from cyber security threat to privacy issues. These realties sparked concern among users of the various platforms designed for socio-communication purposes, the irony is the fact that studies conducted in the field suggest that users are so obsessed with the sites that most of the studies in the area proved no relationship between the worry about security and privacy challenges and readiness to quit. Hence, they prefer to privacy control settings and cautious online behaviour as precautionary measures, though, these can only mitigate vulnerability to a certain extent as most complicated intrusions defies simple encryption and preferences. Worst still, inadequate awareness of the sites' data policies and security setting mechanisms particularly in the developing countries expose users to grave criminal attacks and privacy violations at a time when such platforms innovate features supportive to learning, businesses, organisational communications in a manner that extends their usability to all facets of human endeavours. Moreover, exploiting the platforms without the requisite enlightenment can lead to grave consequences. Although, data regulation policies and privacy laws are put in place to scrutinise data traffics and mining in order protect citizens from

cybercrimes, enforcement of the laws are becoming increasingly difficult due to the complex nature of the cybercloud, dimensions of data harvesting and usage. Moreso, inadequate awareness of the privacy and security setting among Facebook users in Nigerian bolster up stinking experiences. Onifade et al., (2018) found that Facebook users are concerned about their privacy and data security on Facebook, but they lack knowledge of restricting access to their data using security and privacy settings put in place.

RECOMMENDATIONS

Cushioning security of online data and respect for user privacy requires a concerted effort of governments, the Facebook and the users. Thus, the paper made the following recommendations:

Government has to come up with enforceable laws safety and security of data. The Activities of social media platforms should be regulated and controlled in a way that suit Nigerian society and protects citizens against cybercriminal activities. The government needs to create awareness and enlighten citizens about the various online privacy and security risks and importance of privacy setting, privacy protection mechanism and other available safety measures (Begotti & Maran, 2019).

Facebook needs to make its data policies clear short and easy to digest. It should devise a way of enlightening users on its privacy and security settings. The present lengthy, vague and elusive data policy discourages users from reading and block digestion.

Facebook users must be cautious of what they share on facebook; change their privacy settrings to control access to their data and revisit such settings frequently for necessary updates should the need be; they must be conversant with the facebook policies and boundaries; they must be wary of links and third party applications; they must limit and avoid locations disclosure; they should activate two steps authentication and single sign on ID; they must avoid apps update from unautheticated sources; they must use powerful Antivirus and strong passwords; they must be wary of friend requests from unknown persons; and finally, they must install internet security software (Rathore et al., 2017).

Bibliography

Ackerman, S., & Schutte, K. (2015). *Social Media as a Vector for Cyber Crime*. www.clarkschaefer.com

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, *58*, 368–379. https://doi.org/10.1016/j.chb.2015.11.014

Aldhafferi, N., Watson, C., & Sajeev, a S. M. (2013). Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management*, *2*(2), 1–17. https://doi.org/10.5121/ijsptm.2013.2201

Ali, A., Malik, A. K., Ahmed, M., & Raza, B. (2019). Privacy Concerns in Online Social Networks : A Users ' Perspective. *International Journal of Advanced Computer Science and Applications, 10*(7), 601–613. https://doi.org/10.14569/IJACSA.2019.0100780

Asif, Z., & Khan, M. (2012). Users ' Perceptions on Facebook ' S Privacy Policies. *ARPN Journal of Systems and Software*, *2*(3), 119–125. http://www.scientific-journals.org

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. https://doi.org/10.1016/j.chb.2015.11.022

Begotti, T., & Maran, D. A. (2019). Characteristics of Cyberstalking Behavior , Consequences , and Coping Strategies : A Cross- Sectional Study in a Sample of Italian University Students. *Future Data*, *11*(120), 1–11. https://doi.org/10.3390/fi11050120

Bernal, P., & Bernal, P. (2016). Data gathering , surveillance and human rights : recasting the debate debate. *Journal of Cyber Policy ISSN:*, *1*(2), 243–264. https://doi.org/10.1080/23738871.2016.1228990

Blizard, K., & Turner, C. (2011). Facebook, Beacon and Your Privacy. *California Polytechnic State University, San Luis Obispo (Cal Poly)*, 16. http://true-reality.net/csc300/resources/Resources/Reference/Term-Papers/termpaper_blizard.pdf

Boyd M. Danah, & Ellison, N. B. . (2007). Social Network Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 1–23.

Buccafurri, F., Lax, G., Nicolazzo, S., & Nocera, A. (2015). Comparing Twitter and Facebook user behavior: Privacy and other aspects. *Computers in Human Behavior*, *52*, 87–95. https://doi.org/10.1016/j.chb.2015.05.045

Calbalhin, J. P. (2019). Facebook User ' s Data Security and Awareness : A Literature Review. *Journal of Academic Research*, *3*(2), 0–13.

Canadian Internet Policy and Public Interest Clinic. (2008). *Online Privacy T hreats : A Review and Analysis of Current Threats*. www.cippic.ca.

Cavusoglu, H., Phan, T., & Cavusoglu, H. (2013). Do Privacy Controls Influence Content Generation and Sharing Patterns of Online Social Network Users? A Natural Experiment. *The Twelfth Workshop on the Economics of Information Security*, 1–18. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.3498&rep=rep1&type=pdf

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Computers in Human Behavior Securing online privacy : An empirical test on Internet scam victimization , online privacy concerns , and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Chewae, M., Hayikader, S., Hasan, M. H., & Ibrahim, J. (2015). *How Much Privacy We Still Have on Social Network ? 5*(1), 1–5.

Croom, C., Gross, B., Rosen, L. D., & Rosen, B. (2016). What's Her Face(book)? How many of their Facebook "friends" can college students actually identify? *Computers in Human Behavior*, *56*, 135–141. https://doi.org/10.1016/j.chb.2015.11.015

Das, B., & Sahoo, J. S. (2011). Social Networking Sites – A Critical Analysis of Its Impact on Personal and Social Life. *International Journal of Business and Social Science*, *2*(14), 222–228. http://www.ijbssnet.com/journals/Vol._2_No._14;_July_2011/25.pdf

Facebook. (2016). *Facebook, Inc.*

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. *European Data Protection: Coming of Age*, 3–32. https://doi.org/10.1007/978-94-007-5170-5_1

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Fourth Amendment Search and Seizure, Authenticated U.S. Government Information 1197 (1992). http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

Fuchs, C. (2011). An Alternative View of Privacy on Facebook. *Information*, 140–165. https://doi.org/10.3390/info2010140

Gellman, B., & Polyras, L. (2013, July 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Golbeck, J., & Mauriello, M. L. (2016). User Perception of Facebook App Data Access : A Comparison of Methods and Privacy Concerns. *Future Internet*, *8*(9), 1–14. https://doi.org/10.3390/fi8020009

Gordon-Lickey, M. (2015). Do we still want privacy in the information age? Marvin. *Journal of Thermal Analysis and Calorimetry*, *119*(1), 1–13. https://doi.org/10.1007/s10973-014-4098-3

Gross, R., Acquisti, A., & Iii, H. J. H. (2005). Information Revelation and Privacy in Online Social Networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80. http://dl.acm.org/citation.cfm?id=1102199.1102214

Gunatilaka, D. (2011). *A Survey of Privacy and Security Issues in Social Networks http://www.cse.wustl.edu/~jai*. 1–12. n/cse571-11/ftp/social/index.html

Hauff, S., Veit, D., & Virpi, T. (2015). Towards a Taxonomy of Perceived Consequences of Privacy-invasive Practices. *ECIS 2015 Proceedings*, 1–15. http://aisel.aisnet.org/ecis2015_cr/74

Hoanca, B. (2016). If Privacy is Dead , What Can We Do Instead ? *IEEE Technology and Society Magazine*, 29–37. https://doi.org/10.1109/MTS.2016.2518255

Holvast, J. (2007). History of privacy. *The History of Information Security*, 737–769. https://doi.org/10.1016/B978-044451608-4/50028-6

Hoy, M., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. https://doi.org/10.1080/15252019.2010.10722168

Ikhsan, M., Hisham, I., & Saadiah, Y. (2013). Think Privacy : The Awareness of UiTM Pahang Students as Facebook Users. *Th International Science, Social Science, Engineering and Energy Conference 2012*, 147–153. t www.iseec2012.com I-SEEC

Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Account of 50 Million Users. *The New York Times*. Retreaved from www.nytimes.com/2018/technology/facebook-hack-data-breach.amp.html on 15/06/2020

Jin, G. Z. (2018). *Artificial Intelligence and Consumer Privacy* (No. 24253; NBER WORKING PAPER SERIES).

Kasper, D. V. . S. . (2016). Privacy as a Social Good. *Social Thought & Research*, *28*, 165–189.

Kirkpatrick, M. (2010, January 10). Facebook's Zuckerberg Says The Age of Privacy is Over. *New York Times*. Retreaved from www.nytimes.com/external/readwriteweb/2010/01/10/readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html

Krasnova, H., & Kift, P. (2012). Online Privacy Concerns and Legal Assurance : A User Perspective. *Journal on Internet Regulation*, *2*(1), 1–23. https://doi.org/10.14763/2013.1.107

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management*, *34*(6), 761–769. https://doi.org/http://dx.doi.org/10.1016/j.ijinfomgt.2014.07.006

Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. *International Journal of Scientific and Research Publications*, *3*(4), 1–5.

Lee, B. (2007). *Privacy and Awareness on Facebook.com Brian Lee May 14, 2007*.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: user expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. ACM*, 61–70. https://doi.org/10.1145/2068816.2068823

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*, 393–411. http://dx.doi.org/10.1177/1461444808089415

Lowry, P. B., Zhang, J., Wang, C., & Wu, T. (2014). Understanding and predicting cyberstalking in social media : Integrating theoretical perspectives on shame , neutralization , self-control , rational choice , and social learning. *International Conference on System Sciences*, *December 2013*. https://doi.org/10.13140/2.1.3361.2480

Lyon, D. (2003). Surveillance as social sorting: computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, risk, and digital discrimination* (pp. 1–282). Routledge.

Mahmood, S. (2013). Online Social Networks: Privacy Threats and Defenses. In R. Chbeir & B. Al Bouna (Eds.), *Security and Privacy Preserving in Social Networks* (Lecture No, pp. 47–71). Springer-Verlag Wien. https://doi.org/10.1007/978-3-7091-0894-9

Mahmoud, F. Z. M., & Zeki, A. M. (2016). Edward snowden disclosures turn the fears of surveillance into reality: The impact and transformation in information security. *Journal of Theoretical and Applied Information Technology*, *83*(2), 173–179.

Mohamed, A. A., Ibrahim, O., & Nilashi, M. (2015). Journal of Soft Computing and Decision Support Systems The Security Awareness Framework for Social Network Sites Facebook : Case Study in Universiti Teknologi Malaysia. *Journal of Soft Computing and Decision Support Systems*, *2*(3), 1–8. http://www.jscdss.com

Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy*, *39*(3), 411–428.

Moore, A. D. (2003). Privacy: its Meaning and Value. *American Philosophical Quarterly*, *40*(3), 215–227. http://www.jstor.org/stable/20010117 .

Neld, D. (2020). *All the Ways Facebook Tracks You-and How to Limit it*. WIRED. Retreaved from www.wired.com

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook Social media : Facebook. *South African Journal of Science*, *114*(5), 1–5. http://www.sajs.co.za

O'Bien, D., & Torres, A. (2012). Social Networking and Online Privacy: Facebook Users' Perceptions. *Irish Journal of Management*, *31*(2), 63–98. http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=1649248X&AN=74485990&h=lyJ9O7uv8maj+F2o8oViDme8szr8lq1R2+Jg+D876F6E2f8kt41GkRokxkQhSN7fvFtqb1nrCU1rSmTAdRg61Q==&crl=c

Okesola, J. O., & Marthie, G. (2014). *Measuring the impact of information security awareness on social networks through password cracking*. University of South Africa.

Onifade, O., Olomu, M., Ajao, B. F., Atoyebi, M., & Ilevbare, O. (2018). SOCIAL MEDIA USERS PERCEPTION ON PRIVACY ISSUES IN A NIGERIAN Social Media Users Perception on Privacy Issues in a Nigerian University. *Journal of Digital Innovations & Contemp Res.*, *6*(2), 35–46. https://doi.org/10.22624

Paullet, K., & Pinchot, J. (2012). Cybercrime: The Unintentional Effects of Oversharing Information on Facebook. *Proceedings of the Conference on Information Systems Applied Research*, 1–7. http://proc.conisar.org/2012/pdf/2231.pdf

Pavlou, P. a. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, *35*(4), 977–988.

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, *30*(3), 227–238. https://doi.org/10.1016/j.appdev.2008.12.010

Powell, C. D. (2011). "You already have zero privacy. Get over it!" Would Warren and Brandeis Argue for Privacy for Social Networking? *Pace Law Review*, *31*(1), 146–181. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=60797300&site=ehost-live

Privacy International. (2018). *How Apps on Android Share Data with Facebook* (Issue December).

Privacy International. (2019). *Investigating Apps interactions with Facebook on Android*. https://privacyinternational.org

Rajesh, B., Yadav, P. P., & Chakradhar, C. V. (2017). Malicious Computer Worms and Viruses : A Survey. *National Conference on Recent Innovations in Engineering and Technology*, 16–25. www.ijtrd.com

Rashidi, Y., & Camp, L. J. (2016). Understanding Saudis' privacy concerns when using WhatsApp. *USEC (NDSS Workshop)*.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017). Social Network Security : Issues , Challenges , Threats , and Solutions. *Information Science*, *421*, 43–69.

Richard, W. (2010). Facebook's Mark Zuckerberg says privacy is dead. So why does he want to keeps this picture hidden? *Times Newspaper Ltd*. http://erasingdavid.com/categories/issues-in-the-news/facebook%25E2%2580%2599s-mark-zuckerberg-says-privacy-is-dead-so-why-does-he-want-to-keeps-this-picture-hidden/

Schwartz, P. M. (2016). Property , Privacy , and Personal Data. *Harvard Law Review*, *117*(7), 2056–2128. http://www.jstor.org/stable/4093335

Shullich, R. (2011). *Risk Assessment of Social Media Risk Assessment of Social Media*.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.1145/1929609.1929610

Solove, D. J. (2006). A Brief History of Information Privacy Law. *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, 1–46. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271

Statista. (2020). *Nigeria: number of Facebook users 2017-2025*. https://www.statista.com/statistics/972927/number-of-facebook-users-nigeria/ Retrieved on 11/8/2020 @ 5:15 pm

Steijn, W., & Vedder, A. (2015). Privacy concerns, dead or misunderstood? The perceptions of privacy amongst the young and old. *Information Polity*, *20*(4), 299–311. https://doi.org/10.3233/IP-150374

Stern, T., & Salb, D. (2015). Examining Online Social Network Use and Its Effect on the Use of Privacy Settings and Profile Disclosure. *Bulletin of Science, Technology & Society*, *35*(1–2). https://doi.org/10.1177/0270467615596890

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41. http://repository.cmu.edu/jpc/vol4/iss2/2/

Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior*, *38*, 159–173. https://doi.org/10.1016/j.chb.2014.05.027

Thierer, A. (2013). The pursuit of privacy in a world where information control is failing. *Harvard Journal of Law and Public Policy*, *36*(2), 409–455. https://doi.org/10.1525/sp.2007.54.1.23.

Thomas, K., & Nicol, D. M. (2020). The Koobface botnet and the rise of social malware. *IEEE Fifth International Conference on Malicious and Unwanted Software*, 1–9. https://doi.org/10.1109/MALWARE.2010.5665793

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., & Hennh€ofer, A. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). *Springer.*, 333–365. http://dx.doi.org/10.1007/978-94-017-9385-8.

Tsikerdekis, M., & Zeadally, S. (2014). Online Deception in Social Media. *Communications of the ACM*, *57*(9), 72–80. https://doi.org/10.1145/2629612

UNESCO. (2012). Global Survey on Internet Privacy and Freedom of Expression. In *UNESCO series on Internet freedom*. https://doi.org/ISBN: 978-92-3-104241-6

Van Eecke, P., & Truyens, M. (2010). Privacy and social networks. *Computer Law and Security Review: The International Journal of Technology and Practice*, *26*(5), 535–546. https://doi.org/10.1016/j.clsr.2010.07.006

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. http://www.jstor.org/stable/1321160

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, *18*(4), 326–348. https://doi.org/10.1108/09564230710778128

Wu, T. (2015). Facebook Should Pay All of US. In J. Stubbs (Ed.), *New Communication Media Technologies, Course Reader* (Fall Semes). Lecture Materials.

Wua, Y.-C. J., Chang, W.-H., & Yuan, C.-H. (2014). Do Facebook profile pictures reflect user's personality? *Computers in Human Behavior*, *51*, 880–889. https://doi.org/10.1016/j.chb.2014.11.014

Wuest, C. (2010). The Risks of Social Networking. In *Symantec Security Response*. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

Zlatolas, L. N., Welzer, T. H., Marjan, & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, *45*, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

Zuckerberg, M. (2010). *Making Controls Simple*. Facebook Blog. http://blog.facebook.com/blog.php?post=391922327130, accessed 3 May 2016.