ASSOCIATION OF COMMUNICATION SCHOLARS & PROFESSIONALS OF NIGERIA BOOK SERIES

CANADA UNIVERSITY PRESS

PRIVACY, CONFIDENTIALITY AND THE USES AND MISUSES OF SOCIAL MEDIA

Nosa ***OWENS-IBIE***
Department of Mass Communication,
Caleb University, ImotaLagos
nosowens@gmail.com,

To cite this article:
Nosa Owens-Ibie (2019). Privacy, Confidentiality and the Uses and Misuses of Social Media in Fake News and Hate Speech; *Narratives of Political Instability,* ACSPN Book Series 2, pp. 5 — 25
Retrieved from http://www.acspn.com.ng

(Institutional or Subscribed access may be required)

Please note that this is an electronic, pre-print version of this article published by the Canada University Press, Concord Ontario, Canada for Association ofCommunication Scholars & Professionals of Nigeria (ACSPN).

The ACSPN Book Series is exclusive to the Association of Communication Scholars & Professionals of Nigeria.

ISBN: 978-1-989271-05-6

Layout/Design: Ashroph De Grafico

CHAPTER TWO

PRIVACY, CONFIDENTIALITY AND THE USES AND MISUSES OF SOCIAL MEDIA

*Nosa **OWENS-IBIE***

Introduction

In their work exploring the diminishing role of facts and analysis in American public life, Kavanagh and Rich (2018: xi) described the questions of reliability and rejection of factual information in contemporary society as indicators of 'truth decay'. Three of the four trends they identified in this 'decay' are manifest in technology-moderated engagements:
(1) a blurring of the line between opinion and facts
(2) increasing relative volume, and resulting influence, of opinion and personal experience over fact, and
(3) declining trust in formerly respected sources of factual information.

These trends have been influenced majorly by the interface between human (with sensibilities) and technology (without sensibilities). Berger (2018: 8) acknowledged that (today) disinformation and misinformation have spread largely through the empowerment of (technological platforms of) social networks and social messaging, opining that the development 'begs the question of the extent of regulation and self-regulation of companies providing these services.' Although Ireton and Posetti (2018:15) described fake news and disinformation ***as "an old story" they agreed that it is 'fuelled by new technology", and also emphasised the fact that*** **"**the 21st century has seen the weaponisation of information on an unprecedented scale" based on technological innovations. According to the authors,

> *Powerful new technology makes the manipulation and fabrication of content simple, and social networks dramatically amplify falsehoods peddled by states, populist politicians, and dishonest corporate entities, as they are shared by uncritical publics. The platforms have become fertile ground for computational propaganda 'trolling' and 'troll armies'; 'sock-puppet' networks', and 'spoofers'.*

Schoeman (1984b: 2f) distinguished between definitions of privacy as claim, entitlement, right; the measure of control of an individual over personal information, intimacy, and visibility; and

state or condition of limited access to an individual. Gormley (1992: 1337f) identified four types of privacy definitions: privacy as an expression of one's personhood and personality; privacy as autonomy; privacy as citizens' ability to regulate information about themselves; and multidimensional notions of privacy. Solove (2008) outlined six explanations of the concept as: the right to be left alone; limited access to the self; secrecy; control over personal information; personhood; and intimacy. In 2004, Solove had sought clear distinction between conceptions as they relate to privacy: privacy as protection from Big Brother; privacy as secrecy; privacy as non-invasion; and privacy as control over information use.

Problem Statement

There have been scholarly interrogations of the contexts of hate speech, fake news, privacy concerns and the social media, many of them however focusing mainly on the role and influence of Online Social Networks (OSNs) and how they serve as platforms for these. Some of such studies include the review of the privacy model of existing Online Social Networks (OSNs) by Eckles, Good, King, Naaman and Naira, (2007), Krishnamurthy and Wills, (2009), Lewis, Kuafman and Christakis, (2008), users' awareness, attitudes, and privacy concerns towards profile visibility (Acquisti and Gross, 2006), as well as new approaches to enhance content sharing privacy on OSNs (Banks and Wu, 2009, Baden, Spring, Bhattachariee and Starin, 2009, Fang and LeFevre, 2010, Stutzman and Kramer-Duffield, 2010), leakages of privacy and shadow profiles in online social networks (Garcia, 2017), and even an analysis of Facebook's privacy setting within the framework of users' expectations and reality (Liu, Gummach, Krishnamurthy and Mislove, 2011). Some others have also looked at the apparent conflict between right to privacy and freedom of expression (Nyst, 2018, https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression, accessed 30/05/29) and willingness of state organs to contain fake internet content (BBC, 2018). This paper examines the paradox inherent in the use of, and expectations from, technology-moderated interactions as evident in the growing spate of fake news and hate speech, and their negative effects on the persona of netizens. This focus becomes more pertinent with the Cambridge Analytica scandal where personal user information on Facebook was manipulated by the company to the advantage of the Trump campaign during the 2016 American general elections (Butt, n.d.).

Privacy and Privacy Policies

A distinction is made between legal and ordinary interpretations of privacy. To the individual there is an expectation that secrets entrusted to others would not be shared, while the legal focuses on the person who has the right within a professional relationship to disseminate information which is confidential (Lehavot Ben-Zeev and Neville 2012:343). Moreno, Goniu, Moreno and Diekema (2013:711) found in a Facebook study that there are risks with online data which could be used to identify individuals based on the publication of direct quotations. Such a quote entered into a search engine could lead to web link - for instance, a LinkedIn Profile. Individuals could also be identified with a combination of data connected to them. The latter is noted as evidence of inconsistency between the Privacy Policy and the sections on Rights and Responsibilities of the target audience (Moreno et al, 2013). Social networking sites have come to terms with the issue of privacy policies with periodic updating of such policies to accommodate the logics of the ever evolving terrain. There are, however, still complaints about their reliability. Mooradian, (2009: 163-164) quoting Rachels identifies privacy as a requirement for upholding the “diversity of personal relationships that people value”. Such relationships are characterised by some types of behaviour and information exchange. The expectation is that people need to be able to have control or be able to limit access to both themselves and their information in furtherance of personal relationships. Two components are

evident in Rachels' postulation. The first relate to “personal access and space privacy” and the second to personal information. Although there is an interchangeable use of the terms privacy and confidentiality, there have been efforts to focus specifically on the issue of confidentiality and how breaches occur.

The evolution of privacy policies have witnessed transitions, with obvious sensitivity to the concern of users and in recognition of the choices available to them. Boyd (2008: 13-14, 18) recounts a September 5, 2006 development when Facebook launched its “News Feeds” feature through which all activities undertaken by those on the friends list of a user were itemised on their start page. Revealed details included those on new friendships, comments by who to whom, and joiners of groups. The news feeds enhanced the visibility and accessibility of aggregated information in reversed chronological order. The reaction of users of the social networking site was swift and opposed to this feature. Efforts by Facebook's founder Mark Zuckerberg a day after the launch - to placate users, did not assuage feelings with the consequence that three days later - by September 8 - Zuckerberg though claiming that privacy was not compromised, apologised using his blog and offered “new privacy options.” His logic was that he remained committed to helping to ensure more efficient sharing of information by users and that news feeds helps give prominence to what people access.

Although the trend is to present privacy as a positive universal, but it has its shortcoming. The right to privacy admits of a personal space to which access by others is determined by individuals who are able to exercise control over the nature, extent and timing of how the exposed parts are used. Areas covered by this right include feelings, personality, secrets, body, family and household. As Karniel and Lavie-Dinur (2012: 26, 290, 300) elaborate, such a right could be lost through four possible types of exposure through personal information and data, physical (visual) representation on the Internet, disclosure of identity and sentiments and “exposure of preferences” through which data are extracted from the consumer preferences of individuals to build a profile. In each case there is a distinction between the collections of information which amount to violating privacy, and the commercial use or publication of information which themselves amount to further infringement and breach of privacy. Hessler and Freerks (2014: 48) also highlight the breaches of privacy which they declared as 'massive' in the United States. Such breaches are enabled by information technologies, especially computer matching through which various databases containing information on people can be matched to generate information on an individual's social history without their knowledge.

Privacy laws have evolved in answer to some of these challenges. The logic of privacy laws is that of protection. For instance, the Swedish Secrecy Law of 1980, defined rules which institutions storing data or conducting research must adhere to in order to assure the protection of individual privacy, while the U.S. Privacy Act of 1974 also establishes its basis as the protection of individuals from the intrusion into their privacy by federal agencies. The latter law is the legal and ethical basis of the country's various laws on privacy (Hessler and Freerks, 2014: 40, 45). In Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA) was enacted to protect the privacy of individuals in their relationships with private sector organizations and social media companies.

Social Media and Privacy

Social media symbolise development opportunities in technology use, just as it is now a veritable platform for the weaponisation of information, as evident in the spread of disinformation and misinformation (Ireton and Posetti, 2018:15). Samidh Chakrabarti, Facebook's Product Manager, Civic Engagement, as quoted by Ireton (2018:32), pointed out this duality of utility,

and its consequences, when he noted that the social media symbolises both a benefit and danger to democracy. This political ideology promotes freedom of expression, exposure and sharing of ideas and information:

> *If there's one fundamental truth about social media's impact on democracy it's that it amplifies human intent both good and bad. At its best, it allows us to express ourselves and take action. At its worst, it allows people to spread misinformation and corrode democracy.*

Thus, there is a paradox in the usefulness of, and threat from, loss of privacy to, and simultaneous demand for, computer mediated communication, aptly captured by More (1997):

> *… we are reluctant to give up the advantages of speedy and convenient computerized information. We appreciate the easy access to computerized data when making reservations, using automatic teller machines, buying new products on the web, or investigating topics in computer data bases. Our challenge is to take advantage of computing without allowing computing to take advantage of us. When information is computerized, it is greased to slide easily and quickly to many ports of call. This makes information retrieval quick and convenient. But legitimate concerns about privacy arise when this speed and convenience lead to the improper exposure of information.*

This is particularly related to social media. The evolution of social media would rank as one of the most celebrated in the history of human creativity, with epithets suggesting it is a superlative milestone in the communication process. It has variously been described as "one of the most influential innovations of the Internet" (Lehavot, Ben-Zeev and Neville 2012: 341). Bosslet and Warren (n.d: 1221-1222.) describe the growth of online social networks as "truly spectacular", dramatically changing the manner information is obtained from those we know or do not know. While acknowledging that "whatever goes on social media stays on social media", Oladipupo. (2013) describes the phenomenon as "one of the greatest things to evolve in our world". Boyd and Ellison (2007) list three features of social media network sites that differentiate them from similar online communities that support computer- based interactions. Social media sites allow individuals to "construct a public or semi-public profile within a bounded system", "articulate a list of other users with whom they share a connection", and "view and traverse their list of connections and those made by others within the system." Ito *et al* (2008: 8) have conceptualised the new media ecology as an arena where more traditional media and digital, especially interactive media, converge for social communication. Their reference to genres attempts a framework through which participants define common practices, based on socio-cultural and technological features. Such genres which speak to the diversity of engagement of new media include those that are friendship driven and those which are interest driven. Other categories include "hanging out" through which users skirt institutional and other barriers to forge relationships with peers. "Messing around" involves a keener exploration of the content and understanding of technology and media and their workings, including "gaming and digital media production". By "geeking out" participants are involved in more intense peer-driven engagement of more obscure domains of media or technology, with emphasis on seeking expertise from like-minds in distant networks (Ito *et al,* 2008: 10-29). This has contributed to the debate on how the media are serving as tools for the organisation of social movements which are moderated by the logics of global geo-politics (Funke and Wolfson, 2014:352). The clear identification of a communication process with a source encoding information and transmitting

through a medium to an audience which decodes and gives feedback to determine the effectiveness of the communication, is being fundamentally reconfigured with the audience no longer quite the consumer of information as traditionally conceived. By their configuration, social media incorporate a collection of Internet-based technological tools which enable content to be instantly available to global audiences once published, and have such interactive features that make them not exactly amenable to the controls associated with traditional media. Also referred to as Web 2.0 or Gov 2.0, they enable users to create information, foster interactivity (CIO Council, 2013: 2), with such interactivity deriving from the very nature of social media which involves using mobile and web-based technologies for such dialogue (Lambert, 2013). Individuals have a capacity to create their profiles which are accessible to those they allow (Srinivasan, n.d). Social media blur the boundaries between the public and private spheres once information gets to the public domain. Users are active in the generation and dissemination of multimedia data.

The first identifiable social media platform, SixDegrees.com was launched in 1997. Then it only enabled users to build profiles and list friends. By early 1998, it was possible to surf the list of such friends. Today, just over two decades after, through social media, you can communicate with people you know, find new people to communicate with, find people you have lost touch with, find or set up a group and keep in touch (generally) with what's going on (Laing, 2013: 18-19). Social media platforms today include Blogging (Blogger), Microblogging (Twitter), Podcasting (Blubrry), Social Networking (Facebook), Social news sharing (Reddit), Social bookmarking/social tagging (Google Reader) and Video hosting (YouTube) (*National Student*…, n.d.). Others, according to (***13 Types...*, n.d.)** include Publishing Tools (WordPress), Photo sharing sites (Instagram), Rating/Review sites (Amazon ratings), Personal broadcasting tools (Blog talk radio), Virtual worlds (Farmville), Location based services (Foursquare), Widgets (Like buttons), Group buying (Living Social). Monte (2012) also mentioned **Community Building Platforms** like Yahoo Groups which allow the creation of interactive message boards for instance for a community of customers.

The benefits of social media go beyond the individual to just about all components of society, including institutions, organisations, governments, and interest groups. Gross and Acquisti (2005) who trace the origins of the concept to the 1960s with the Plato computer-based education tool of the University of Illinois, identified the grouping by The Social Software Weblog of these social networking sites into categories, including friends, photos, face-to-face facilitation, dating, common interests, business, dating and pets. From the perspective of government benefits of social networking sites include increased access to audiences and access to communication by government, greater flexibility in managing communication, achieving cost-effectiveness in communication, improvements in the speed of inputs and feedback by targets, capacity for targeted communication with specific audience segments and a reduced dependence on traditional channels of communication (*Social Media Policy*…, 2011).

Norris (2000) has also noted that the evolution of social media has greatly encouraged new forms of activism on the global political scene in many ways. This includes reducing the barriers to civic engagements, levelling some of the financial hurdles involved in political communication, widening the opportunities for political debate, and the dissemination of information, and group interaction. Social media is also useful in advocacy, as pointed out by Scott and Maryman in their work "Using Social Media as a Tool to Complement Advocacy Efforts" (http://www.gjcpp.org/en/article.php?issue=21&article=121, accessed 22/05/19) to the effect that when social media is used to augment advocacy efforts, it bolsters outreach efforts by spreading information about a

cause, reinforcing relationships among supporters, promoting participatory dialogue between group leaders and supporters, and strengthening collective action through increased speed of collaborative communication. Unlike in the past when communication between constituents and politicians was limited to letters, phone calls, or face to face meetings social media has therefore expanded contemporary communication channels with public officials, many of whom now maintain Facebook and Twitter accounts, allowing constituents to send brief messages and share information about public concerns. Social media is also helping to deepen citizen involvement in the governance process. Rehr's (2017) position, that in the United States of America, "social media is allowing more voices than ever to exercise their First Amendment right to impact their government at all levels", was affirmed in relation to Nigeria by Dr. Bukola Saraki, former President of the Nigerian Senate, who stated that social media has helped to put Nigerian politicians on their toes thus helping to checkmate the excesses of public officials (http://allafrica.com/stories/201707240615.html, accessed 23/05/19):

> *From exchange of information, people get enlightened and platforms like yours keep those of us in top government positions on our toes. We always remember what people on discussion and news groups say about our actions, utterances and attitude. And that serves as a constant check on us. You are definitely contributing a lot to deepening our democracy and improving governance.*

Theoretical framework.

Tavani (2008) grouped theories of privacy into three "restricted access theories, control theories, and restricted access/limited control theories (RALC)". The restricted access theory recognises privacy as seeking the protection of individuals and functioning in the words of Mills (1965) as a "circle around individuals". Westin (1967) a proponent of the Control theory define privacy as acts of determining for themselves the extent, timing and method used to communicate information about individuals, groups or institutions to others. These two types of theories is condensed in the restricted access/limited control theories (RALC) which proponents like Moor (1997) and Fuch (2011) characterise as simultaneously seeking to protect individuals from "intrusion or observation" and on the other focusing on the "different zones of privacy". This paper adopts the restricted access/limited control theories (RALC) for its evaluation of the paradox involved in the exposure to technology- moderated interactions which enables the spread of fake news, and often involves the manipulation of information about individuals and hence represents within a context, an intrusion to privacy spaces. Hate speech, also exposes their targets to the loss of privacy and makes them victims of attacks online and elsewhere. The RALC encourages informed consent as much as possible, and fosters the development of practical, fine grained, and sensitive policies for protecting privacy (Moor, 1997: 32). The theory assumes that people can determine what they decide to keep private or disseminate while access to different information could be given to different people at different times (Fuchs, 2011: 222-223). Boyd (2008: 18) however, avers that "information is not private because no one knows it; it is private because the knowing is limited and controlled", noting elsewhere that there is fluidity to the interpretation of what is public and what is private with an increasing difficulty with using language, structures and social norms to deal with it (Boyd, n.d.).

Literature Review

Habermas has harped on the ultimately pseudo character of 'privacy', arguing that as a concept it is more illusory than real (see Fuchs, 2011: 229). The historical evolution of the concept would lend some credence to such conclusion, going for example by the works of Schoeman (1984b:2f,), Gormley (1992: 1337f) and Solove (2004, 2008). The basic prompting for the varied

considerations of privacy concepts would be the human desire to have, and to limit. To have, has been solved by access to the technology of communication, but to limit would require more than mere access. Indeed, to limit has become the burden of scholarship, technocrats and professionals and rights activists, leading to the creation of legal and paralegal means of curtailing undue exposure in cyberspace.

Although the concept of fake news and its violation of privacy concerns, for instance only gained prominence particularly in 2017 (Guradian, 2017 as cited by Alzamora, 2019), available literature indicates that concerns for privacy has been an age-long issue, spanning the different generations of technological development. In their article in the 1890 *Harvard Law Review*, Samuel Warren and Louis Brandeis (see Whitehouse, 2010: 311) gave a legal definition of American privacy rights which advocated legal protection through "the right to be left alone", noting that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house tops'". Whitehouse (2010), quoting Patterson and Wilkins, however noted that such advocacy for legal rights to privacy was preceded by the ethical right to privacy which is fundamental to human relationship within the community. This was much the same reflection of John Stuart Mills in his 1848 classic, *Principles of Political Economy* where he had argued:

> *That there is, or ought to be, some space in human existence thus entrenched "around", and sacred from authoritative intrusion, no one who professes the smallest regard to human dignity will call in question: the point to be determined is, where the limit should be placed; how large a province of human life this reserved territory should include* (Mill, 1965: 938).

With the recent interest in social media related spread of fake news, Allcott and Gentzkow, (2017) examined the economics of its consumption prior to the 2016 American Election. Their study brought out four major facts; two of them being the huge possibilities in the spread of fake news and its believability, based on ideological affiliation. According to the study, "of the known false news stories that appeared in the three months before the election, those favoring Trump were shared a total of 30 million times on Facebook, while those favoring Clinton were shared 8 million times and "people are much more likely to believe stories that favor their preferred candidate, especially if they have ideologically segregated social media networks". Garcia (2017) also investigated the leakage of privacy and shadow profiles in online social networks", and concluded that there is need for the creation of privacy paradigms "that take into account the fact that individual privacy decisions do not happen in isolation and are mediated by the decisions of others." In their study, Liu, Gummach, Krishnamurthy and Mislove, (2011) examined Facebook's privacy setting vis a vis what users expect as privacy opportunities and what is available in reality. The study, which surveyed 200 Facebook users recruited via Amazon Mechanical Turk found that 36% of content remains shared with the default privacy settings but that overall, privacy settings match users' expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected.'

In its survey of more than 16,000 adult intent users across 18 countries in 2017, BBC World Service (https://www.bbc.co.uk/mediacentre/latestnews/2017/bbc-world-service-poll,2017, accessed 30/05/2019) reports heightened worry among 79 percent of respondents 'about what is real and fake on the internet'. Despite this high level of concern however, a great proportion of respondents (58%) were still against state regulation. The level of anxiety about determining what is fake and online is highest in Brazil (92%), Indonesia (90 percent), Nigeria (88 percent), and Kenya (85 percent) compared with 75 to 85 percent in most countries that were part of the

survey. The country with the least worry is Germany where 51% of internet users said they not worried about uptake and spread of fake news online. The survey also considered the use of state powers to control Internet use. According to the poll, opposition to state control of internet use was greatest in Greece (84 percent), Nigeria (82 percent), Brazil (72 percent), France (71 percent), and Turkey and Kenya (each 70 percent) while in a number of Western nation, apart from Greece and France, concern about internet regulation was mixed, indeed polarised in countries like Canada, Australia, Spain, and Germany. In the UK, only 53 % of internet users support some sort of regulation but in China that number was greater (67%). The survey concluded with an insight that "the present high concern about 'fake news' may not affect people's online behaviour very much, apart from them doing more fact-checking." Brookshire (2017, https://www.sciencenews.org/ blog/scicurious/social-media-privacy-no-longer-personal-choice, accessed 06/05/19). The outcome of the study by Garcia (2017) pointed at the inevitability loss of control over privacy decisions once an individual puts out information online:

> *keeping your information private isn't just about your own choices. It's about your friends' choices, too... inhabitants of the digital age may need to stop and think about just how much they control their personal information, and where the boundaries of their privacy are.*

Garcia's study, was on how the effect that 'social interaction and data integration in the digital society can affect the control that individuals have on their privacy', a development the researcher proved using data from Friendster, a social networking site that boasted of some 115 million users before it closed down in 2015. The study indicates that social network sites collect personal information on users through their friends and other contacts in the network. The author advocated "new privacy paradigms that take into account the fact that individual privacy decisions do not happen in isolation and are mediated by the decisions of others." Determann, (2012) highlights the myths which have clear implications for privacy in social media use. These include the absence of explicit privacy rights in most international human rights treaties and national constitutions; that against social media companies, individuals do not quite have rights; individuals do not really own data about themselves and factual information are not effectively protected by copyright (protects "creative expression") and intellectual property laws; social media companies do not in themselves threaten privacy as some of them have been involved in settling lawsuits and charges linked to privacy issues; privacy laws are not necessarily better in Europe than the United States; advertisers are not a threat to privacy as what they do is to display their products and services to consumers; the exclusion of law enforcement is not a guarantor of better protection of privacy; it is not technologies that threaten privacy but the use to which they are put by people; the individual has the option of keeping information about themselves away from social media; anonymity is not guaranteed on the Internet; social networks are indeed subject to laws; employers can regulate usage of social media; and privacy is not a core concern among consumers. Moreno, Goniu, Moreno and Diekema (2013:710) in their study examined levels of consistency between the objectives of websites and their Privacy Policy identifying Twitter as the most consistent in the period of analysis. Twitter they noted explicitly stated that:

> *Our Services are primarily designed to help you share information with the world. Our default is almost always to make the information you provide public but we generally give you settings to make the information more private if you want. Your public information is broadly and instantly disseminated.*

YouTube's statement of intent which also aligns with its Privacy Policy states in relation to its public sharing of videos, that you "may control the information that is available to other users and your con?rmed friends at any time." In the case of LinkedIn which connects professionals globally, the statement of intent is also consistent as it states that:

> *The information you provide to LinkedIn may reveal, or allow others to identify, your nationality, ethnic origin, religion, gender, age, geography, or other aspects of your private life.*

Facebook's Privacy Policy, among others, states as follows:

> *When you publish content or information using the 'everyone' setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and pro?le picture)… Information set to 'everyone' is publicly available information.. Such information may, for example, be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third-party search engines and be imported, exported, distributed and re- distributed by us and others without privacy limitations…We generally limit search engines' access to our site. We may allow them to access information set to the 'everyone' setting (along with your name and pro?le picture) and your pro?le information that is visible to everyone…You can change the visibility of some of your pro?le information using the customize section of your privacy settings.*

The Rights-and-Responsibilities hyperlink clarified that,

> *If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their in- formation, and post a privacy policy explaining what information you collect and how you will use it.*

Citizen journalism, hate speech, fake news and privacy

Another dimension to social media influence on contemporary society, is the evolution of such genres as citizen journalism. This genre has broadened the definition of a journalist to be potentially anyone with “a laptop and a wireless connection”, although it has also blurred the distinction between source and receiver (Whitehouse, 2010: 321), and become a source of concern in terms of privacy breaches and other unethical activities. Goode (2009) identifies citizen journalism practices as photo and video sharing, posting of eyewitness commentary on current issues, current affairs blogging, re-posting, and comments on posts by other users or other inputs in the news process of other news outlets, without being creators of content.

Postman (1993) had written his book, *Technopoly: the surrender of culture to technology, to warn about what he described as the* alarming rate at which we adopt technology without considering its side effects. There are indeed concerns about the absence of control, and the misuse of the freedom available on social media which leaves participants in social media interactions, some of whom are considered as citizen journalists, uncensored. While there is no advocacy for the gagging of journalistic expressions and initiatives in any form, the rate at which fake news permeate the social mediascape has activated variable responses. The government of Nigeria, according to a Wall Street Journal Report quoted by *Punch* (https://punchng.com/fake-news-could-be-nigerias-biggest-threat-to-credible-elections-report/, accessed 29/05/19),

described Nigeria as the 'capital of fake news' and considered the phenomenon as major threat to the 2019 general election in the country. Part of the report, as quoted by the Punch notes that:

> *Fake news has upended elections across the globe but found particularly fertile ground in Africa, where 54 countries, more than 1,000 languages and chronically underfunded local media, complicate efforts to combat the spread of rumours and misinformation*.

The report also quoted Peter Cunliffe-Jones, an executive director at Africa Check, one of Facebook's three third-party fact-checking partners with focus on news from, and about Nigeria, as warning that fake news "has the potential to do a huge amount of social harm, harm to individuals and harm to society". Hassan Idayat, the director of the Centre for Democracy and Development (CDD), West Africa, as reported by Premium Times (https://www.premiumtimesng.com/ news/headlines/311532-analysis-how-nigerian-politicians-supporters-use-fake-news-as-campaign-strategy.html, accessed 29/05/19) blamed the proliferation of social media for the quick spread of fake news in the build up to the 2019 general elections, lamenting that it was "promoting animosity along religious, ethnic and regional divides". Premium Times quoted her as saying that,

> *False information in Nigeria spreads through various channels, but social media provides the cheapest and quickest ways to access millions. Through Whatsapp and Facebook, people share propaganda videos, made-up quotes, and fabricated articles made to look like they are from the likes of the BBC or Al-Jazeera*

A study of the 2019 Presidential elections in Nigeria, found that social media was dominated by hate speech, with supporters of the two presidential candidates then President Goodluck Jonathan, and the contender, General Muhammadu Buhari, being more inclined to disseminate such hate messages (ACSPN, 2018: 215). Social media has therefore, become the fertile ground for sowing and harvesting of fake news. Wardle and Derakhshan (2017) defined fake news as 'the complex phenomenon of information pollution, or information disorder'. This tends to be amplified by the penchant for politicians to assign the term to any news that does not favour them. Fake news is misinformation, and not restricted to the legacy media, indeed it is spread more by the new media.

Alzamora and Andrade (2019) identified seven types of fake news/misinformation contexts common to discourse on the concept: of false connection (subtitles that do not correspond to the content), false context, context manipulation, satire or parody (without explicit intentionality), misleading content (misuse of data), deceiving content (use of false sources), and made-up content (with the intention of manipulating public opinion and harming). Allcott and Gentzkow (2017) on their part define fake news as news that are verifiable and intentionally fake, and able to deceive readers. The authors clearly linked the increase in the engagement in online social networks, associated with the decline of confidence in traditional news media, to the rapid growth of the spread of fake news. Such news are spread as their purveyors access the vast data of online users and exploit the social media illiteracy of many on such database. Omatseye (2011) does not regard social media as the magic wand many claim it to be, pointing to its effective use by criminally minded (individuals) youths as a great disservice to society. One of the grey areas in social media use is that the free market self-regulation of social networks fundamentally impinges on their capacity to guarantee the type of privacy individuals may desire or deserve (Spinelli, 2010: 67).

The consequences and dilemmas deriving from the uses and misuses of social networking, has thrown up these vulnerabilities. Yusuf (n.d.) chronicles a number of incidents to buttress these in Nigeria, starting with the account of Cynthia Osukogu, a postgraduate student of Nassarawa State University who through Facebook contacts to whom she disclosed personal details and got murdered following a bait. Temitope Joshua, General Overseer of The Synagogue Church of All Nations, Lagos drew attention to an account by the name - TB Joshua Ministry can Change the World with over 40,000 followers and through which people were supposed to be sending prayer requests TB Joshua who was till then not aware of the scam. Facebook posts purportedly by Pastor Enoch Adejare Adeboye of The Redeemed Christian Church of God had asked people to wear clothes with red colour on a particular day while another post asked Christians to hold a prayer vigil on a designated date to protect them and family from evil. The photograph of Governor Adams Oshiomole of Edo State was doctored to a compromising sexual posture, in an attempt to tarnish his image as he campaigned for a second term in office.

Beyond these, in 2015 Apostle Johnson Suleman and his wife of Omega Fire Ministries, Auchi, Edo State, Nigeria, Pastor Matthew Asimolowo of Kingsway International Christian Centre, United Kingdom, Dr Paul Enenche, Dunamis International Gospel Church, Abuja, Reverend Joshua Talena of Shepherd House International Church, Abuja have had to alert of the operation of multiple dubious Facebook accounts purportedly operated by them but actually the products of fraudsters who use them to solicit for donations. It is common to have nude photographs posted on Facebook, some of them as instruments of blackmail or attempts to get even in soured relationships. The duplication of profiles and proliferation of pages for unscrupulous activities is acknowledged as common occurrence with Facebook warning in August 2012 that “83 per cent of its users are fake.” Yusuf (n.d.). Omionawale, Ani and Oni, M (2013) assert that the Nigerian Twitter space is witnessing a rise in nude photo postings, with the revelation that young ladies resort to this practice for self-promotion and to break into trending issues. They acknowledge the trend of posting not just nude photos, but gory photos. There are therefore, concerns about the threat to privacy that participants on social media interactions face despite the various opportunities the platforms offer them.

Through social networks, a variety of personal information are disclosed using the web pages which users are assigned following registration. Privacy options are available to users who can limit their information to a circle of friends although the sense of security offered in the process may be misleading, since these sites are businesses and information on them are on servers. Tierney, Spiro, Bregler and Subramanian (n.d.) assert that social networking has compromised traditional notions of privacy, especially in visual media” although Cryptagram is designed to protect photo privacy. Breaches also occur in professionalism (Lee and Bacon, 2010: 533). Three areas identified by Chew, Balfanz and Laurie (n.d: 3.) where privacy can be compromised by social networking sites include 'activity stream' where the expectations of users about the events that get fed into their activity stream and the audience within that stream may not be met by the network; 'unwelcome linkage' through which sensitive information about an individual may have been shared; and 'merging social graphs' which enable information supposedly exclusive to particular networks could overlap with those in other networks and reveal information traceable to a particular person.

Within the context of Web 2.0 settings, there has been significant changes to the environments of information privacy. Web 2.0 involving blogging and social networking sites has spawned interactive personalized web computing which enable users to self-publish. Blogging as “equivalent of digital diaries”, allow a great deal of “self-expression” and have gained in

popularity, rising from 50 in 1999 to 50 million almost a decade ago (Mooradian, 2009, 167-168). Gross and Acquisti (2005) highlight the blurring of boundaries of privacy by the logics of social networking with users either being ignorant, uncaring or just being realistic in embracing the wider implications of online habits and practices. According to them, there is the possibility of stalking - with a potential adversary able to know with information on profiles, the likely location of the user most of the day, building a digital dossier with sensitive personal details on views and orientations, and a fragile privacy protection following from Facebook users, for instance, being able to use personal information from the network on those in supposedly secure campus environments with some form of privacy protection.

With the transformative capacities of smartphones making them to virtually regulate lives, there are inbuilt realities about their configuration which contradict the logic of privacy. For instance and as Adewumi (2015) notes, from research evidence, all it takes to cut anonymity including the GPS coordinates, are obtainable from smartphones. Other features which reveal identity are geographical location, the serial number of the smartphone, date, and time - all of which are referred to as metadata. According to Graham Cluley (see Adewumi, 2015) metadata can be collected in the routine processes of receiving or making calls, location when call was made or how long the call was made. Through geotagging which on Facebook (also Instagram and Twitter) is automatically opted into in the instant messaging service except when the feature is disabled, it is possible to show exact locations. He revealed the possibility of a thief being traced with a stolen smartphone. Patterns of data from a phone can be used to match "stress, depression and loneliness" using an app developed at Dartmouth College. An increase in the number of online platforms used, raises a user's prospects of being hacked. Findings on the use of social media sites by 802 teens are revelatory in relation to issues of privacy and confidentiality. Madden *et al* (2013) state that such teenagers are disclosing more about themselves now than previously, more of them are using Twitter, the average teen user of Facebook has 300 friends and 79 Twitter friends, they are losing interest in Facebook because of increasing adult presence on the network, 60% of teenagers on Facebook "keep their profiles private", take steps to manage their reputation, networks and information they don't want to be in the public domain, are not particularly concerned about the access of third parties to their data. The example of Facebook, shows that as a network increase in size there tends to be greater variety, "information sharing, and personal information management", and teens tend to report positive rather than negative experiences of themselves.

Other findings by Madden (2012: 4-11) show that the action of individuals tend to contradict their affirmation that privacy is important to them; while two-thirds of adults maintain online profiles most of them limit access to their friends, privacy settings are chosen by both young and old for their profiles, and women tend more than men to keep private profiles. The management of privacy controls, presents difficulty for half of social media users with the most educated among them having the most difficulty, and the pruning of profiles through deleting contacts, photo tags and comments is on the increase. Women and the young are most fond of deleting friends, young adults are most fond of deleting comments and photo tags as part of reputation management mechanism. The social media presence of most users of social networks is on Facebook, where such presence is managed through one account. A tenth of profile owners express regrets over their posts. Users also manage the posts of others.

Studies in other settings show the evolution of social media as popular culture unbounded by demographics. In the United Arab Emirates, Nair (2011) reported, based on a study, that the average resident spends at least three hours daily on social media sites with 90% of respondents

updating their Facebook profile regularly and 16% of that number affirming that they are "perpetually connected to their accounts", suggesting that "the nation is overrun by internet drones" - a reflection of an acknowledged addiction to social media. The same pattern is reported in Israel where Karniel and Lavie-Dinur (2012: 288) note that not less than 85.3% of Israeli internet users are on Facebook compared to the United States where 60.4% of internet users are on Facebook. Out of 282.7 million Internet users in Europe by December 2008 those who visited social networking sites were 200 million (Kaupins and Park, 2010: 84). Despite this reach, there are concerns about the blurring of personal and professional time of workers by social media as a collateral consequence. In Mexico, Marisol Macias Castaneda, a newsroom manager with Nuevo Laredo newspaper was for instance decapitated in a border city with a handwritten sign by her side indicating that she was killed because of her social networking site postings (Stevenson, 2011).

The risks of disclosures on social media as amplified by Normand Landry (see Dusseault, 2013:3) include absence or loss of anonymity, disclosure of otherwise confidential information, possibility of attacks on personality, cyber-bullying, identity theft, sexual or psychological violence. Wortham (2011) emphasizes that the retention of anonymity has become more challenging with increased interconnectedness of the Web population. Given the logics of social networking, Dusseault (2013: 29) highlights the need for digital literacy which require a capacity for privacy management as a core skill. Digital literacy skills enable the individual to "make wise, informed and ethical online decisions" and are located within the "larger digital economy strategy." On their part, the social media networks are also coming up with steps to curtail the use of their networks as platforms for the spread of fake news. In the second to the last week of May 2019, Facebook, according to Bright removed "a network of hundreds of pages, groups and Instagram accounts it labelled as producing "coordinated inauthentic behaviour", an euphemism for fake news, toward Africa" (https://techcrunch.com/ 2019/05/20/facebook-account-purge-africa-fake-news/, accessed 29/05/19). According to the report, those behind the networks that promoted the 'inauthentic behaviour' used fake accounts to run pages, presented themselves as locals, including local news organisations and published information about politicians they claimed were 'leaked'. "The Page administrators and account owners frequently posted about political news, including topics like elections in various countries, candidate views and criticism of political opponents", according to Bright, adding that the activity took place on over 65 Facebook accounts, 161 Pages, 23 Groups, 12 events and four Instagram accounts. One of the pages had a total of 2.8 million accounts, while some 5,500 accounts joined at least one of the Groups. There are similar moves by other networks, including an agreement to have a code of conduct to tackle the menace more vigorously, including closer scrutiny of advertising on accounts and websites where fake news appears, through fact checkers, according to Punch newspaper (https://punchng.com/facebook-google-to-tackle-spread-of-fake-news/, accessed 30/05/19).

The submission of Karklins (2011) supports the argument that digital literacy is key to resolving the paradox of use and expectation:

> *We live in a world where the quality of information we receive largely determines our choices and ensuing actions, including our capacity to enjoy fundamental freedoms and the ability for self-determination and development. Driven by technological improvements in telecommunications, there is also a proliferation of media and other information providers through which vast amounts of information and knowledge are accessed and shared by citizens.*

Adding to and emanating from this phenomenon is the challenge to assess the relevance and the reliability of the information without any obstacles to citizens' making full use of their rights to freedom of expression and the right to information.

A Nigeria Response

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, represents a comprehensive response to the core issues of the erosion of privacy, among other security imperatives, within the latitude enabled by social media. Civil society, media bodies and coalitions, and advocates for freedom of expression, have maintained a sensitivity to attempts at legislation. The 'Frivolous Petitions and Other Matters Connected Therewith Bill' labelled the "anti-social media bill" was, for instance, aborted on the strength of the resistance to its enactment into law (Owens-Ibie, 2016: 242-276). The shutdown by the National Broadcasting Commission (NBC) of Daar Communications, owners of African Independent Television (AIT) and Ray Power on June 6, 2019, and its subsequent negotiated re-opening, also provided an example of a continuing attempt to explore and agree a consensus for appropriate responses to the challenges of media expressions. In the latter case, the citing of the use of information sourced from social media on *Kaakaki* AIT's breakfast programme which has a segment on postings on various platforms, was in contention.

Although various laws in the annals of the media, directly or indirectly address issues bordering on fake news and hate speech, the capacities of such laws to fundamentally reshape the virtual public sphere, remains an issue. The Copyright Act, Seditious Offences Ordinance of 1909, 1916 Criminal Code, as revised, Obscene and Harmful Publications Act of 1961, and institutional frames like those of the Nigeria Broadcasting Code, Code of Ethics for Journalists in Nigeria (see *Reporting Elections*…, 2018),, and the Nigerian Media Code of Election Coverage (2018), are part of the evolving frame, with the earlier laws mainly targeting traditional media. Although institutional mechanisms relying on law and policies to sanction offenders are recording variable levels of effectiveness, such response is significant, although it appears that technology and the competencies of users of such technology could be indicative of dilemmas, which are more global than local.

Conclusion

Within the digital environment, privacy becomes more complicated, or a paradox. This has prompted calls for what Debatin refers to as "privacy literacy" defined as "an informed concern for their privacy and effective strategies to protect it", by patrons of social networking sites (see Gauthier, 2012, p. 158). The same literacy capabilities are needed to tackle the menace of fake news and hate speech, since defamation is a possible consequence of inappropriate comments online. Despite the debates around privacy, hate speech and fake news, or in response to the phenomenon, social networking sites have evolved periodic updating of privacy policies and strategies for dealing with fake news, to accommodate the logics of a continuously unveiling communication context. The evolution of privacy policies have witnessed transitions with obvious sensitivity to the concern of users who have choices. Social media users understand they have choices and insist on making those choices, as demonstrated in the swift condemnation of the controversial Facebook's 'News Feed' of September 5, 2006 (Boyd, 2008: 13-14, 18).

It is important for users to engage with the logic that the individual's information footprint, through their activity online or those of others, is larger than they imagine, given the possibility of drawing inferences from such information. Other realities of significance, are that: anonymity

does not exist on the Internet; anyone can use information on an individual against them; un-encrypted information over any network can be accessed by a third party; sources lose control over information disseminated on a network; information across networks can be misinterpreted; duplication of information occurs on the Internet which never loses information in it; information can be retrieved from the Internet; there is no guarantee of identity on the Internet as impersonation is always possible; and avoiding the Internet by for instance being offline, does not guarantee privacy.

Fundamental therefore, to the resolution of the existing paradox, is the issue of digital literacy, for which there does not currently appear to be a comprehensive framework so that the choices made by users in the digital ecosystem is properly contextualised. Although typical of the transitional character of the development process, it suggests that beyond frameworks relating to security considerations, there is a need to provide legal and policy safeguards on protecting privacy rights and confidentiality given the logics which compromises both, within digital realities. In Nigeria, this poses a challenge to the education system and the need for its de-bureaucratisation, in order to cope with the demands of technology and its pace of evolution. The flexibilities intrinsic to digital cultures require a matching by similar dynamism in the redevelopment of curricula at all levels. That UNESCO's effort to mainstreaming the media and information literacy curriculum, was still at the level of pilot-testing by May 2019, suggests the need for pace, not just for the formal, but also the informal sectors. When the appropriate level of awareness and ownership is achieved by the rising population of social media users, the implication of actions would align more with the promises of the law, and policies driven by the need for appropriate conduct, self-regulation and the benefits of media and digital literacy. There is already a growing coalescing of collaborations by global and local interests to drive this initiative.

References

13 types of social media platforms and counting (n.d.). Retrieved from http://decidedlysocial.com/13-types-of-social-media-platforms-and-counting/

28 Internet acronyms every parent should know (2014, December 9). Retrieved from http://www.vanguardngr.com/2014/12/28-internet-acronyms-every-parent-know/

Acquisti, A., and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *PET, 2006.*

Adewumi, B. (2015, February 10). The biggest myth about phone privacy: How selfies can put your identity at risk. Retrieved from Http://www.tribune.com.ng/component/k2/item/29081-the-biggest-myth-about-phone-privacy-how-selfies-can-put-your-identity-at-risk

Allcott, Hunt., and Gentzkow, Matthew. (2017). "Social Media and fake news in the 2016 election," Cambridge, Mass.: National Bureau of Economic Research, NBER Working Paper No. 23089, January 2017, revised April 2017a.

Alzamora, Geane, Carvalho., and Andrade, Luciana. (2019). The transmedia dynamics of fake news by the pragmatic conception of truth. *Agenda in Communication Research. V.13 - Nº 1 Jan./abr. 2019*

Association of Communication Scholars & Professionals of Nigeria (ACSPN) (2018). *Understanding Nigerian media and elections through research: Analysis of the 2015 presidential election campaign messages.* Ontario: Canada University Press.

Baden, R., Bender, A., Spring,N., Bhattacharjee,B., and Starin. D. (2009). Persona: an online social network with user-defined privacy. *SIGCOMM, 2009*.

Banks, L., and Wu, S. F.(2009). All friends are not created equal: An interaction intensity based Approach to privacy in Online Social Networks. *CSE, 2009*.

BBC World Service. (2017). Fake internet content a high concern, but appetite for regulation Weakens: BBC World Service Poll. https://www.bbc.co.uk/mediacentre/latestnews/2017/bbc-world-service-poll, accessed 30/05/19.

Berger, Guy. (2018). "Foreword" In Ireton, Cherilyn and Posetti, Julie (eds) Journalism, 'Fake news' and disinformation. Paris:: United Nations Educational, Scientific and Cultural Organization

Bosslet, G.T. and Warren, C. (n.d.). Commentary: The good, the bad, and the ugly of social media 2011 by the Society for Academic Emergency Medicine doi: 10.1111/j.1553-2712.2011.01197.x PII. Retrieved from http://www.researchgate.net/publication/51806347_Commentary_The_Good_the_Bad_and_the_Ugly_of_Social_Media

Boyd, D. (2008). Facebook's Privacy Train wreck Exposure, Invasion, and Social Convergence. *Convergence: The International Journal of Research into New Media Technologies* London: Sage Publications. Vol 14(1): 1320

Boyd, D. M., Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer- Mediated Communication, 13(1), 11*.

Bright, Jake. (2018). *Facebook's latest account purge exposes Africa's misinformation problem.* Https://techcrunch.com/2019/ 05/20/facebook-account-purge-africa-fake-news/, accessed 29/05/19.

Brookshire, Bethany. (2017). "On social media, privacy is no longer a personal choice". Https://www.sciencenews.org/blog/ scicurious/social-media-privacy-no-longer-personal-choice, accessed 06/05/19.

Butt, Sidra A. (n.d). Facebook Cambridge Analytica Scandal Retrieved from https://moodle.taltech.ee/pluginfile.php/352023/mod_resource/content/1/Facebook%20Cambridge%20Analytica%20Scandal.pdf

Chew, M., Balfanz, D. and Laurie, B. (n.d.). (Under)mining privacy in social networks. Retrieved from http://w2spconf.com/2008/papers/s3p2.pdf

CIO Council, Privacy best practices for social media. July 2013. Retrieved from https://cio.gov/wp-content/uploads/downloads/ 2013/07/ Privacy-Best-Practices-for-Social-Media.pdf .

Communications Council best practice guide. Social media Code of Conduct (n.d.). Retrieved from http://www.communicationscouncil.org.au/downloads_tcc/2012/CC_Social%20Media%20Code%20of%20Conduct_FINAL.pdf

Cybercrimes (Prohibition, Prevention, etc.) Act 2015

Determann, L. (2012). Social media privacy: A dozen myths and facts *Stanford Technology Law Review* STAN. TECH. L. REV. 7 Retrieved from http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf.

Dusseault, P. (2013). Privacy and social media in the age of big data: Report of the Standing Committee on Access to Information, Privacy and Ethics April. 41st Parliament, First Session http://www.parl.gc.ca . Retrieved from http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf

Eckles, D., Ahern, S., Good, N.S., King, S., Naaman, M., and Nair, R. (2007). 'Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* ACM, pp.357366.

Fang, L., and LeFevre, K. (2010). Privacy wizards for social networking sites. *WWW, 2010*.

Fuchs, C. (2011). "Towards an alternative concept of privacy". *Journal of Information, Communication & Ethics in Society*. Vol. 9 No. 4, 2011 pp. 220-237.

Funke, P.N. and Wolfson, T. (2014). "Class In-Formation: The intersection of old and new media in contemporary urban social movements". *Social Movement Studies: Journal of Social, Cultural and Political Protest*, 13:3, 349-364, DOI: 10.1080/14742837.2013.831755 To link to this article: http://dx.doi.org/10.1080/14742837.2013.831755. Retrieved from http://www.researchgate.net/publication/262580826_ Class_In-Formation_The_Intersection_of_Old_and_New_ Media_in_Contemporary_Urban_Social_Movements

Garcia, David. (2017). Leaking privacy and shadow profiles in online social networks. *Sci. Adv. 2017;3: e1701172, pp 1-6*

Gauthier, C.C. (2012). Can privacy and social networking co-exist? *Journal of Mass Media Ethics:Exploring Questions of Media Morality*, 27:2, 157-159.

Goode, L. (2009). Social news, citizen journalism and democracy. *New Media Society* http://www.sagepub.co.uk/ journalsPermissions.navVol 11(8): 12871305

Gormley, K. (1992), "One hundred years of privacy", *Wisconsin Law Review, Vol. 1992, pp. 1335-441.*

Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social networks (The Facebook case) Pre-proceedings version. ACM Workshop on Privacy in the Electronic Society (WPES). Retrieved from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Hessler, R.M. and Freerks, K. (2014). Privacy ethics in the age of disclosure: Sweden and America compared. *The American Sociologist*, Vol. 26, No. 2, Part II: Sociology, Law, and Ethics (Summer, 1995), pp. 35-53 Published by: Springer Stable URL: http://www.jstor.org/stable/27698725 . Accessed: 14/09/2014 18:26.

Ige, R. and Omorogbe P. (2014, May 20). Social media making people anti-social. Retrieved from http://www.tribune.com.ng/ quicklinkss/features/item/5634-social-media-making-people-anti-social

Ireton, Cherilyn., and Posetti, Julie . (2018). "Introduction" In Ireton, Cherilyn and Posetti, Julie (eds) *Journalism, 'fake news' and disinformation.* France: United Nations Educational, Scientific and Cultural Organization

Ito, M., Bittanti, H.H.M., Boyd, D., Herr-Stephenson, B., Lange, P. G., Pascoe, C.J., and Robinson, L. with Baumer, S., Cody, R., Mahendran, D., Martínez, K., Perkel, D., Sims, C. and Tripp, L. (2008). "Living and Learning with New Media: Summary of Findings from the Digital Youth Project". The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning. November. Retrieved from https://www.macfound.org/media/article_pdfs/DML_ETHNOG_2PGR.PDF

Kaupins, Gundars., and Park, Susan. (2011). Legal and ethical implications of corporate social networks. *Employee Responsibilities and Rights Journal June 2011. DOI: 10.1007/s10672-010-9149-8*

Karklins, Janis. (2011) "Foreword". In Alton Grizzle and Carolyn Wilson (eds) *Media andInformation Literacy Curriculum for Teachers*. France: United Nations Educational, Scientific and Cultural Organization.

Karniel, Yuval., and Lavie-Dimur, Amit. (2012). Privacy in new media in Israel: How social networks are helping to shape the perception of privacy in Israeli society. *Journal of Information, Communication and Ethics in Society, Vol. 10 Issue: 4, pp.288-304, https://doi.org/10.1108/14779961211285908*

Kavanagh, Jenifer., and Rich, Michael D. (2018). *Truth Decay: An initial exploration of the Diminishing Role of Facts and Analysis in American Public Life.* Santa Monica, Calif: RAND Corporation.

Krishnamurthy,B., and Wills,C.E. (2009). On the leakage of personally identifiable information via online social networks. *WOSN, 2009.*

Lehavot, K. Ben-Zeev, D. and Neville, R.E. (2012). Ethical considerations and social media: A case of suicidal postings on Facebook, *Journal of Dual Diagnosis*, 8:4, 341-346, DOI: 10.1080/15504263.2012.718928. . Retrieved from http://www.tandfonline.com/doi/abs/10.1080/15504263.2012.718928 .

Lewis, K., Kaufman, J., and Christakis, N. (2008). The taste for privacy: An analysis ofcollege student privacy settings in an online social network. *Computer-Mediated Communication, 14(1), 2008.*

Liu, Yabing., Gummadi, Krishna P., Krishnamurthy, Balachander., and Mislove, Alan. (2011). **"Analyzing Facebook privacy settings: User expectations vs. reality"** In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, 2 to 4 November 2011, pp. 6170.*

Madden, M. (2012, February 24). Privacy management on social media sites (Most users choose restricted privacy settings while profile "pruning" and unfriending people is on the rise). Pew Research Center's Internet & American Life Project. Retrieved from http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx.

Madden, M., Lenhart, A. Cortesi, S., Gasser, U., Duggan, M., Smith, A. and Beaton, M. (2013, May 21). Teens, social media, and privacy. Retrieved from http://pewinternet.org/Reports/2013/ Teens-Social-Media-And-Privacy.aspx

Mill, J.S. (1965) in Mill, J.S. (Ed.), *Principles of political economy, Vol. 2.* London: University of Toronto Press.

Monte, C.D. (2012, March 23). The 7 Different types of social media platforms. Retrieved from http://www.iblogmarketing.com/ 2012/03/23/the-7-different-types-of-social-media-platforms/

Moor, James H. (1997). Towards a theory of privacy in the information age. *Computer and Society, September 1997, pp 27-32.Computers and Society, September 1997*

Mooradian, N. (2009), July 14). The importance of privacy revisited. Springer Science+Business Media B.V. Ethics. Inf Technol 11:163174 DOI 10.1007/s10676-009-9201-2. Retrieved from http://connection.ebscohost.com/c/articles/44096863/importance-privacy-revisited

Moreno, M.A., Goniu, N, Moreno, P.S. and Diekema, D. (2013). "Ethics of social media research: common concerns and practical considerations." *Cyberpsychology, Behavior, and Social Networking Volume 16, Number 9.* Mary Ann Liebert, Inc. DOI: 10.1089/cyber.2012.0334. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/23679571

Nair, P. (2011, September 19). Internet socialising a national pastime? Retrieved from http://www.khaleejtimes.com/ darticlen.asp?xfile=data/theuae/2011/September/theuae_September416.xml&section=theuae

Norris, P. (2000). *A Virtuous circle: Political communications in post-industrial societies.* Cambridge University Press, NY; Fall 2000.

Nyst, Carly. (2018). Two sides of the same coin the right to privacy and freedom of expression, https://privacyinternational.org/ blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression, accessed 30/05/19

Oladipupo, I. (2013). How social media can ruin your brand, September 3. Retrieved from http://www.punchng.com/i-punch/how-social-media-can-ruin-your-brand/

Omatseye, S. (2011, February 21). The alternate society. Retrieved from http://thenationonlineng.net/web3/columnist/monday/ sam-omatseye/28622.html

Owens-Ibie, N. (2016). Social media, the public sphere and the marginalisation of a new minority in Nigeria, *Research for Development* (The Journal of the Nigerian Institute for Social and Economic Research), Vol 26, Nos 1 & 2, 242-276

Postman, N. (1993). *Technopoly: The surrender of culture to technology.* New York: Vintage Books.

Rehr, David K. (2017) How Is Social Media Being Used In Advocacy? Retrieved fromhttp://www.huffingtonpost.com/ entry/how-is-social-media-being-used-in-advocacy_us_589a7b12e4b0985224db5bac.

Reporting Elections and Democratic Accountability: A resource manual (2018). Lagos: International Press Centre

Schoeman, F.D. (1984b), "Privacy: philosophical dimensions of the literature", in Schoeman, F.D. (Ed.), Philosophical Dimensions of Privacy. Cambridge, MA: Cambridge University Press, pp. 1-33.

Scott, J.T., Maryman, J. (2016). Using social media as a tool to complement advocacy efforts. *Global Journal of Community Psychology Practice, 7(1S), pages 1-22.*Retrieved 25/05/19, from (http://www.gjcpp.org/).

Solove, D. (2004). *"The digital person", Technology and privacy in the information age*. New York, NY: New York University Press.

---------- (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Spinell, Christopher F. (2010). Social media: No 'friend' of personal privacy. *The Elon Journal of Undergraduate Research in Communications Vol. 1, No. 2 Fall 2010*

Stevenson, M. (2011). Woman decapitated in Mexico for web posting. September 24. Retrieved from http://news.yahoo.com/ woman-decapitated-mexico-posting-012958564.html

Stutzman, F., and Kramer-Duffield, J.(2010). Friends only: Examining a privacy-enhancing behavior in Facebook. *CHI, 2010.*

Srinivasan, S. (n.d). Social media security: Protecting privacy. Retrieved from http://csrc.nist.gov/organizations/fissea/2012-conference/presentations/fissea-conference-2012_srinivasan.pdf

Tavani, H.T. (2008). "Informational privacy: concepts, theories, and controversies", in Himma, K.E. and Tavani, H.T. (Eds), *The Handbook of Information and Computer Ethics*. Hoboken, NJ: Wiley. pp. 131-64.

The: Nigerian media code of election coverage (Revised Edition 2018). Lagos: International Press Centre

Tierney, M., Spiro, I., Bregler, C., and Subramanian, L. (2013). "Cryptagram: Photo privacy for online social media" In Proceedings of the First ACM Conference on Online Social Networks, COSN '13, pages 7588, New York, USA

Wardle, C., and Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. *Council of Europe Report.*

Westin, A. (1967). *Privacy and freedom.* New York, NY: Altheneum.

Whitehouse, G. (2010). Newsgathering and privacy: Expanding ethics codes to reflect change in the digital media age, *Journal of Mass Media Ethics: Exploring Questions of Media Morality*, 25:4, 310-327, DOI: 10.1080/08900523.2010.512827. Retrieved from http://dx.doi.org/10.1080/08900523 .2010.512827.

Yusuf, A. (n.d.). The ugly face of Facebook. Retrieved from Http://www.tellng.com/index.php?option=com_k2&view=item&id=1789:the-ugly-face-of-facebook