Personal Data Protection and Facebook Privacy Infringements in Nigeria

Beryl A. Ehondor
Pan-Atlantic University

Silk Ugwu Ogbu
Pan-Atlantic University

Personal data protection is a fundamental human right. Therefore, privacy infringements by Facebook are breaches of individuals' rights and an issue of global concern. The infringements constitute unethical business conduct, inadvertently exposing victims to socio-economic and security risks. From the lens of Gatekeeping Theory, the paper argues that the social responsibility of governments and media organizations include establishing appropriate standards for practice and use of personal data. The provisions of Nigeria's Data Protection Regulation (NDPR), is criticized as weak and incapable of matching Europe's GDPR standards. This paper proposes bespoke personal data protection strategy and creating a media space that is safe to all.

Keywords: social media, gatekeeping, data protection, privacy infringement, Facebook, media regulation, social responsibility

INTRODUCTION

As contemporary African businesses emerge, an increasing amount of transactions and exchange of information between organisations and individuals are done online. Still, there are unanswered questions on the online data security of individuals in business engagement with the increasing incidence of data infringements. It begs the question on the efforts towards data protection for Africa and Nigerian businesses in particular. The data theft and misuse indicting Facebook have necessitated a re-appraisal of individual and business data protection, plus the role of government as a media-gatekeeping stakeholder. This reassessment of data is even more pertinent because Nigeria, Africa's biggest economy, has business dealings with countries and organisation in all continents of the world, which also leverage communication via social media. This implies an extension of the chain of vulnerability and potential for data infringement, for innocent acquaintances and business transactions; a socio-economic threat.

On the 21st of March 2018, Mark Zuckerberg, Co-founder of Facebook (FB), a social media colossus, broke his silence via a Facebook post concerning recent reports of a data hijacking scandal in the United States of America. He stated, "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again." (CNBC, 2018). Whether the Facebook founder was aware or not of the 'misuse' of subscriber's data is not the focus here, but the fact that it happened and millions of people around the world became vulnerable. That is a breach of TRUST.

Privacy of personal data online is a crucial ongoing conversation in today's world that's largely digital and experiencing a convergence of devices, formats etc. This is also critical due to the ubiquity of the internet and ease of acquiring, sharing, storing and manipulation of data. (Pelteret & Ophoff, 2016). Thus the matter of data privacy has received the focus of media consumers, individuals and organisations, whilst intermittently dominating media and legislative discourse across the world (Pelteret & Ophoff, 2016). Thus continents and countries have begun to look at data protection as a fundamental human right (Manolescu, 2010).

Beyond the recent data theft scandal (CNBC, 2018), the spotlight is on FB, as it is said to have more consumers than any single country's population, with over two billion users worldwide (Verdict, 2017), implying the platform has been trusted by many and has massive latent power due to its numbers. Statistics according to Zephoria Inc. (2018), a digital marketing company, indicate that FB has the highest number of social media users growing by 23% per annum, has users aged between 25-34 as the most common age demographic (i.e. the most active in any economy). The platform also has over 83 million counterfeit profiles, is the biggest online social presence of most companies, plus the application's like buttons are viewed in over 10 million third-party sites (Zephoria Inc., 2018), especially with the advent of the open authentification.

Before the FB-Analytica 2018 data scandal (CNBC, 2018), FB in an expansion move released what it called 'Open-Graph' to the developers and third-party applications. This gave those interested (i.e. third-party applications) the privilege to get personal data of FB users including names, friends details, gender, birthday, location, education, religious & political penchants amongst other info (CNBC, 2018). Facebook's document on Open Authentification, where they made their Application Programming Interface (API)'s open-source also played a contributory role to ease of other people accessing subscribers data (Facebook for Developers, 2018). Open Authentification involves developers setting up an account on FB and tying it to their application so that users can log in via their FB accounts, while the developers, in turn, have direct access to whatever bio-data they'd earlier put in FB and the third-party developers won't have to deal with managing the new users usernames and passwords. Thus data inputted by users on the FB platform in a bid to connect with friends was 'sold' to third parties and used for politics, adverts, rise in distribution of fake news and other forms of profiteering (CNBC, 2018) leading to Mark Zuckerberg being summoned and investigated by the US Congress (The Guardian, 2018) and other nations (The Telegraph, 2018).

The above explains why the conversation on data privacy is a burning issue (Pelteret & Ophoff, 2016), leading to the drive for data protection as a fundamental human right (Manolescu, 2010). This begs the question of gatekeeping on social media, which has metamorphosed (Mai, 2016) with the advent of the internet, the identification of the gated (i.e. the general users of the media who also require protection via gatekeeping) as being a part of the media system and actively empowered for gatekeeping (Böttcher, 2014) as against the traditional models of media gatekeeping, i.e. audience gatekeeping. This also brings to question, the role of the government in gate-keeping the media. This explains why the conversation around data privacy and protection trend on social media because users have a voice, engage in citizen journalism and trigger policy changes in governments.

Following the conversation above, the EU pushed for the Lisbon Treaty in 2009, covering rights to data protection, privacy and transparency (McDermott, 2017) and took it a notch up in April 2016 by signing into law the EU General Data Protection Regulation (GDPR) which replaced earlier data protection regulations. GPPR set a high standard not only for the EU but for other countries, with stiff enforcement for companies around the world who at any point will handle data of EU citizens (Allen & Overy, 2018). Again, the factor of globalisation makes it probable that numerous organisations around the world must at some point access and use personal data of EU citizens as clients or otherwise. Thus GDPR has been put in place as protection for data of EU citizens particularly online and in the prevalence of social media data infringement, specifically Facebook in this instance.

Nigeria is not immune to data infringement on social media (and specifically Facebook) being heavy users of the platform, as it boasts of a whopping 26 million subscribers on FB (TechPoint, 2018), one of the largest in Africa. The Cambridge Analytica data-hijack led to a further investigation which revealed

how the Cambridge Analytica team were paid to influence the outcome of the 2007 presidential election by sharing a video on FB to discredit Mohammadu Buhari, the contender, in favour of Goodluck Jonathan, the incumbent (The Guardian, 2018). The Federal Government went further to set up a committee to investigate the involvement of Cambridge Analytica in the 2007 and 2015 general elections citing them as responsible for use of over 50 million FB profiles to sway elections in many countries (Vanguard, 2018). This contributes a dent to the credibility of the poll results in the 2015 elections. Also bringing to question just how much data has been stolen and how many cases are left untreated due to the absence of firm regulations protecting social media in Nigeria. How secure are personal data of social media platform and Facebook users in Nigeria?

Some literature considers 'the gated' and equally responsible for the security of personal data (Böttcher, 2014). However, with the gated being considered a suitable gate-keeper in a digitised world, there are uncertainties about the literacy and awareness of the happenings on data breaches around the world, use and misuse of FB personal data, plus its implications, particularly in the Nigeria space. But this is supposedly where the government should exercise its duty to protect all citizens and their interests, even virtually, in the light of current-day realities.

In a recent reprimand of Facebook by the United States Federal Trade Commission (FTC), concerning the violation of users' privacy rights, FTC's criticisms are as follows: *"The social network Facebook has accepted the criticisms of the FTC in the sense that it has disappointed users by telling them that they could protect the privacy of their personal information, and then on the other hand regularly sharing and making public this same information."* Mark Zuckerberg responded saying they will ensure that these "mistakes" do not happen again. However, at the moment, users are extremely vulnerable to all sorts of abuse and to violation of their fundamental right to respect for their privacy, meanwhile, public authorities have no real means of enforcement (Ndiandukue, 2012).

The Cambridge-Analytica-Nigeria-election case above is a case-in-point of how data theft via the biggest social media platform in the world, FB, directly impacts the country. Hitherto, the government makes and reinforces media regulations, making them media stakeholders and gatekeepers. But is the Nigerian government sufficiently 'ready' to face this current social cum virtual incidences of data-theft and infringement, also being major gate-keepers of the media?

Here lies the gap this paper attempts to bring to light, a form of social media regulation audit. While FB may have eased filial connections, business growth and taken away the burden of repeated filling of data in some applications during sign-in/ sign-up, the security of the individual's data cannot be negotiated. Every citizen has an unequivocal right to data protection and data privacy (McDermott, 2017) necessary in our digitised era. Data protection is important in today's world, also areas of concern for consumers and organisations is information privacy (Pelteret & Ophoff, 2016). Where does Nigeria stand legislatively in effectively protecting its citizens' personal data and gatekeeping social media?

Thus this conceptual paper attempts to identify current legislation for personal data protection of social media of Nigerians. It furthermore reviews the identified regulation and makes a recommendation for contemporary social media regulation approach and data protection for Nigerian social media users.

LITERATURE / THEORETICAL BACKGROUND

This conceptual paper discusses privacy and data infringement and then rests on two theoretical pillars viz Gatekeeping and Social Responsibility. This is discussed succinctly below in the context of social media and government obligation.

PRIVACY AND DATA INFRINGEMENT ON SOCIAL MEDIA

Data protection is more critical in this internet age than ever and strategies on data protection and/or infringement should be met with policies (Bosher & Yesiloglu, 2018). Policymakers should take into account these emergent issues on social media platforms when considering reform opportunities (Meese

& Hagedorn, 2019). Also, note that proposing legislation is inefficient without strategies for day-to-day implementation.

Individuals data consists of their digital identity and activities. Every internet user associated with a social network or platform has a digital identity. It is made up of everything users publish on their various accounts and allows an inference to be drawn of their personalities and future interests. This implies that upon every login, sending of e-mail and search on a search engine, there is a load of private conversations, IP addresses and addresses of sites visited that are archived and possibly exploited for commercial purposes. Thus, the risks of access to this identity or data by various interest groups become latent woe for the individual and all associated with him, including the state. As a result, there are many types of risk for social network users and the security of the information shared on social networks (Ndiandukue, 2012). These risks include identity theft, advert harassments, cyberbullying, sexual criminalities, financial fraud, terrorism etc.

Social media and platforms and networks are reluctant to assume social responsibility for reasons including financial and strategic interests. This is evidenced by the recent reprimand of Facebook in the US by the Federal Trade Commission (FTC), concerning the violation of users' privacy rights. This inability of governments to implement coercive global legislation led a coalition of experts in privacy protection in 40 countries to publish a statement in 2009. It requires governments to implement and enforce effective legislation on privacy, plus putting pressure on the operators of social media sites to guarantee the security of users. (Ndiandukue, 2012)

GATEKEEPING AND SOCIAL MEDIA

On the question of possible gatekeeping in today's world mediatized by the internet and its dynamic characteristics**,** Singer (2006a) reiterated that the internet defies the entire concept of a 'gate'; as the newspaper editor, broadcast commission, radio producers, publishers and other traditional gatekeepers in the media, have limited control and powers in filtering freely published content by the internet audience. Her findings further suggest that traditional gatekeepers and editors ought to be rethinking their gatekeeping role as they become more experienced in creating content for the Internet (Singer, 2006b), as its ubiquitous nature obliterates the traditional concept of the professional journalist deciding what information people can and cannot see.

Gate-keeping is defined as a selection process where 'gatekeepers' pick and choose which news articles and/or visual images to run in the media. Looking at further definitions of gatekeeping in the media below, the inference is that all information flow requires control and the control of information connotes power with latent capacity for social change. This implies that the force controlling the flow of information within a society inadvertently influences happenings [significantly] in that society and the definitions below corroborate this inference.

> *'Gatekeeping refers broadly to the process of controlling information as it moves through a gate or filter and is associated with exercising different types of power (e.g., selecting news, enforcing the status quo in parliamentary committees, mediating between professional and ethnic groups, brokering expert information)'* - (Barzilai-Nahon, 2017)

> *"Gatekeeping, as a social scientific concept, can be traced to Lewin's (1947) writings on social planning. He observed that the most efficient way to bring about widespread social change is to concentrate on persons in key positions of influence, who function as 'gatekeepers' in the flow of goods and ideas through the society. Lewin viewed the societal impact of gatekeepers as a matter of 'group dynamics,' and hence he saw gatekeeping as a basic problem for sociology. At the same time, however, he conceived of the gatekeeping process itself in individualistic and psychological terms."* (Clayman, 1998)

'A gatekeeping role "filtering out information deemed unworthy from that deemed worthy of dissemination (de Grazia, 1963)." (Beyer, Chanove, & Fox, 1995)

"Gatekeepers are those key technical professionals who are strongly networked to both internal and external sources of critical information." (Katz, 1965)

All of the gatekeeping definitions above share a common theme, it is deliberate yet selective dissemination of information, information channelling to an objective end, by a professional/stakeholder (the gatekeeper), to shield a group of people (the gated). Also, the delineation of obligation and power of the gatekeeper, and for a positive cause too. Furthermore, there is an anticipation of a potentially negative impact against the gated when the gatekeeper or gatekeeping not in effect.

Summarily, the gatekeeper is a power broker whose decisions on what information is going out or otherwise is influenced by broad factors, motives and values. In traditional mass media, the directors and editors in print and motion picture held this office. Institutions, asides media houses, also play gate-keeping roles. For instance, the government, via the Nigeria Broadcasting Corporation (NBC) bans music material that contravenes its codes and doesn't represent the country in a positive light (The Guardian, 2013). So indeed, not only media people are gatekeepers, but the government plays a significant role in gatekeeping the media. Two major research on the identity of the gatekeeper (Agada (1999); Klobas & McGill (1995)) describes the gatekeeper from a pluralistic and neutral standpoint. They originate from within the community in a bottom-up process and represent the needs of members in the community. Their research findings indicated the elements essentially distinguishing gatekeepers from other members of the online community are more often their information skills and not necessarily affiliation with a connection to a certain class or position power.

Gatekeepers primarily preserve culture and ideology, thus Pescosolido et al (1997) call them cultural gatekeepers. *"Cultural gatekeepers, those who determine which images will be available to the public, may be influenced by racial tensions in society. We argue that what these gatekeepers promote influences of future symbolic representations."* The government, especially in a democratic dispensation, is designed to protect and foster the interest of the people, and so are cultural gatekeepers. Looking at how vulnerable citizens have become online being also 'netizens', discerning governments have begun to devise approaches to legally and strategically ensure online data protection and privacy. Thus, this paper taking a cue from contemporary data protection laws enforced internationally takes a cursory look at the Nigerian government social media gatekeeping viz-a-viz its social responsibility.

SOCIAL RESPONSIBILITY AND SOCIAL MEDIA

The evolution of the media is reflective in its functions, now social, and capable of social change. It takes root in man's need to relate and 'Mass Media', communication to many. Today, the media regarded as a social institution, fully integrated into other traditional social institutions such as churches, school, government, and family. Media systems were primarily designed for profit which informs its objectives on content development and broadcast. Thus many media platforms and programs are open-sourced, easily accessible and contain alluring content designed to attract the largest imaginable audience. In today's society, the media is even more integrated with daily living of citizens via the internet (Schrape, 2016) and social media.

Social media is today's biggest example of mass media, meso-media i.e. many-to-many (Schrape, 2016) and refers to the use of web-based and mobile technologies for interactive dialogue barring geography and spatiality and time (Baruah, 2012). The context of media in this paper is streamlined to social media.

Schulz (2004) and Krotz (2007) specified the role of the media in social change, identifying 4 processes whereby media change human communication and interaction:

i. They extend human communication abilities in both time and space
ii. Media substitutes social activities that were previously face-to-face

iii. Media instigates an amalgamation of activities, face-to-face communication combines with mediated communication
iv. Actors in many different sectors have to adapt their behaviour to accommodate the media's valuations, formats and routines

Social media can be succinctly described as applications/platforms that enable virtual interactions interpersonally and within a community, irrespective of geographic location, with dependency on internet connectivity, and use of smart devices. Examples of social media platforms are Facebook, Twitter, Snap-chat, Instagram, YouTube, Blogs, Whatsapp etc. The social in focus of this paper is FB, having over 2 billion users (Zephoria Inc., 2018) across the globe.

Facebook is a social networking website and service where users can post comments, share photographs and links to news or other interesting content on the Web, play games, chat live, and stream live videos (GFCGlobal, 1998). Shared content can be made publicly accessible, or it can be shared only among a select group of friends or family, or with a single person. Facebook as a social media platform that allows one to maintain a friends list and choose privacy settings to tailor who can see content on your profile. It also allows you to upload photos and maintain photo albums that can be shared with your friends. Facebook supports interactive online chat and the ability to comment on your friend's profile pages, sometimes called "walls," to keep in touch, share information or just to say "hi." Facebook's developer network delivers advanced functionality and monetization options. It supports group pages, streaming live videos, live fan pages and business pages that let businesses use Facebook as a vehicle for social media marketing. Facebook Connect allows websites to interact with Facebook and allows Facebook to be used as a universal login authentication service. This integration and social networking on FB involves so much data of users hence the need to enforce the social responsibility of the media.

Social responsibility of the Social media using media functions as identified by Harold Lasswell (1948), Charles Wright (1960) and Dennis McQuail (2005) are characterised below:

a. Surveillance
b. Correlation
c. Transmission
d. Entertainment
e. Mobilization

In essence, the media asides being a watchdog of society and sharing information is also a gatekeeper, determining what information goes out or otherwise. This entrusts social responsibility on the media in its multifacetedness. It is worthy of note that all media are extensions of some human faculty and reflection of society. The 'media' in the context of this context and tasked with the obligation of media functions like Surveillance, Mobilisation, Transmission, etc. In essence, the government via regulations determines media output, channels, stakeholders and platforms.

The government in many countries function as media regulators, media owners (fully or partly) and media gatekeepers. In this sense, they (the government) become 'watch-dogs' of other watchdogs (other media owners and platforms) within its jurisdiction and in the interest of protection of citizens, the economy and national security. To this end, the government makes media regulations, sometimes via sub institutions and parastatals, like the Federal Ministry of Communications and the National Information Technology Development Agency.

FINDINGS

This section shows a textual analysis of findings on Facebook privacy issues, the Nigerian government legislation towards the protection of personal data of its citizens online.

A TIMELINE OF FACEBOOK PRIVACY ISSUES

There are increasing studies on facebook's privacy issues and its implication on countries, organisations, businesses and individuals since its commencement 2006. The issues have been about the use and misuse of users data, tending more to exploitation and scandal, over a decade-long. Below is a chronological timeline of these issues as reported by NBC News (Newcomb, 2018), now represented to ease review herein. Watch out for a pattern throughout the incidences.

TABLE 1
A TIMELINE OF FACEBOOK PRIVACY ISSUES

S/N	DATES	ISSUES	FACEBOOK RESPONSE
1	September 2006	Facebook debuts news feed and about a million users joined FB news feed protest groups arguing the feature was too intrusive	Zuckerberg insisted and the newsfeed stayed on
2	December 2007	Beacon, FB first big brush with advertising privacy issues	FB- founder apologises, give users opt-out choice
3	November 2011	FB settled with the Federal Trade Commission in 2011 over charges that it didn't keep its privacy promise to users by allowing private information to be made public without warning	Facebook agrees to undergo an independent privacy evaluation every other year for the next 20 years; remains liable for a $16,000-per-day penalty for violating each count of the settlement.
4	June 2013	Facebook bug exposes private contact info (in the guise of recommendation)	Facebook fixed the bug, notifies people whose info may have been exposed. FB said it pulled the tool offline and fixed it. The company also said it had notified regulators and pledged to tell affected users
5	July 2014	Mood-manipulation experiment on more than half a million Facebook users to show how emotions could spread on social media	Facebook data scientist apologizes after publishing proceedings in the National Academy of Sciences
6	April 2015	Facebook cuts off apps from taking all the data they want	Developers allowed keep building apps but with 'limited access' to users data. But FB still couldn't keep track of how many developers were using previously downloaded data
7	March 2018	The Cambridge –Analytica data hijack scandal	Founder apologises. FB bans Cambridge Analytica
8	January 2018	Europe's data protection law	Facebook complies, released a set of privacy principles explaining how users can take more control of their data.

9	February 2018	Belgian court tells Facebook to stop tracking people across the entire internet	Appeal the court's ruling, saying it has complied with European data protection laws and gives people the choice to opt-out of data collection on third-party websites and applications
10	March 2018	Revealed that Facebook knew about massive data theft and did nothing	An apology tour and policy changes. Zuckerberg avoided the word "sorry" but did express partial blame for Facebook's role in not doing enough to protect user privacy.

A cursory review of the privacy issues or breaches from Facebook and their response indicates a pattern; repeated breach, excuses, immense profiteering via user data and not taking absolute responsibility for the cause and outcome of all data misuse and privacy breaching. This presupposes that gatekeepers must fashion creative measures to protect its netizens, considering the seriality of these breaches and activities of sinister hackers.

Also observe FB response to National establishments and regulations, as it attempts to comply when brought to book, recognizing the interest of citizens and businesses right to be protected. The timeline of FB privacy issues, the Cambridge Analytica Data hijack and misuse of personal data during the 2015 election raises questions locally as to data protection for Nigerians and reechoes the need for social

The Nigerian Government Social Media Legislative Position; NDPR

This paper has established previously the social responsibility of the government as a media gatekeeper and stakeholder. So in furtherance to data use and protection for Nigeria, the National Information Technology Development Agency Act (NITDA Act) of 2007 empowers the National Information Technology Development Agency (NITDA) to regulate, monitor, evaluate, and verify progress on issues around information technology, on an ongoing basis under the supervision and coordination of the Federal Ministry of Communications. To this end, the National Data Protection Regulation was proposed, in 2019, to tackle privacy concerns and personal data protection (it is yet to be approved by the NITDA board) (NITDA, 2019).

The National Information Technology Development Agency was established in 2001 and is directly under the Federal Ministry of Communication. It operates within confines of the National Information Technology Development Agency Act (NITDA Act) of 2007. The agency's mandate is to regulate, monitor, evaluate, and verify progress on issues around information technology, on an ongoing basis.

To this end, the National Data Protection Regulation was proposed, in 2019, to tackle privacy concerns and personal data protection (it is yet to be approved by the NITDA board) (NITDA, 2019). The objectives of the NITDA Act are as follows;

The objectives of this Regulation are as follows:

a) to safeguard the rights of natural persons to data privacy;
b) to foster safe conduct of transactions involving the exchange of personal data;
c) to prevent manipulation of personal data and
d) to ensure that Nigerian businesses remain competitive in international trade; through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices

The regulation is broken into sections explaining the document and dealing with the subject matter. Filtering through the document, data of individuals is described as 'Personal Data' and implies '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that*

natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others';

The details about personal data above are inclusive of the kind of data necessarily requested and frequently assessed or made public on social media platforms like Facebook e.g. email, gender, photograph, names, location, cultural identity, social preferences etc of the user. Some of the data are very mandatory and avoidance may lead to restrictions in use of the platform, therefore users are compelled to share their personal data.

In the event of a personal data breach Section_2.13.7,8,9 of NITA data protection regulation requires the data controller (Facebook, in this case) to delete the personal data without delay. This request to delete personal data is also at the instance of the data subject (user). This brings to question the role of this government agency, whether the user is enlightened on his 'ascribed' obligation and if Facebook has been notified of this regulation and agrees to be accountable by it. So far, there are no public records of any agreement or regulation from Nigeria for which Facebook can be held accountable.

"2.13.7 Where personal data are transferred to a foreign country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards for data protection in a foreign country. The Data Subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

2.13.8 The Data Subject shall have the right to request the Controller the delete of personal data without delay and the Controller shall delete personal data where one of the following grounds applies:

- *a) the personal data are no longer necessary in relation to the purposes for which they were collected or processed;*
- *b) the Data Subject withdraws consent on which the processing is based;*
- *c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;*
- *d) the personal data have been unlawfully processed; and*
- *e) the personal data have to be erased for compliance with a legal obligation in Nigeria.*

2.13.9 The Controller who has made the personal data public and is obliged to delete the personal data shall take all reasonable steps, to inform Controllers processing the personal data of the Data Subjects request."

Furthermore, section 3.3 of the Nigeria Data Protection Regulation purportedly makes provision for 'Local and International Cooperation'. The proviso that appears like the government is subdued afraid of offending 'some entities' by demanding compliance. Again no emphasis on punitive measures to be meted upon breach of personal data-infringement. This should not be the case considering the market value of Nigerian's patronage and the social responsibility as gatekeepers and 'watchdog'. Facebook is an international platform and their cooperation is required in the protection of personal data of Nigerians. See section 3.3 below:

3.3 Local and International Cooperation
3.3.1 In relation to foreign countries and international organisations, the Agency and relevant authorities shall take appropriate steps to:

- *a) Develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;*

b) *provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;*

c) *Engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;*

d) *Promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries."*

DISCUSSION

The Nigeria Data Protection Regulation from NITDA is not 'enough as is' to facilitate the protection of Nigerian netizens and social media users, especially on Facebook. The NITDA regulation is a good attempt but fails to meet contemporary social media protection realities as it does not make provision or state the obligation of social media platforms in personal data protection. Punitive measures are not stated, demand for compliance is weak and unclear. The proposed regulation also does not make provision or state the obligation of social media platforms in personal data protection. Meanwhile, there are antecedents which reemphasize the need to regulate Facebook data access and usage.

The idea of regulating FB is purely on the grounds of information privacy concerns which include secondary use of information, consumer profiling, price discrimination, identity theft and data breach. (Pelteret & Ophoff, 2016). With more consumers than any single country's population and over two billion users worldwide (Verdict, 2017), Facebook is a prime platform for businesses to leverage on. The platform provides a global audience and marketplace with 70 million businesses signed up actively (Newberry, 2018). Zephoria Inc. (2018) stats indicate that FB has the highest number of social media users growing by 23% per annum, has users across all ages. The platform is the biggest online social presence of most companies, plus the application's like buttons are viewed in over 10 million third-party sites (Zephoria Inc., 2018), and allows content sharability. As the above data shows, tons of personal data of billions of businesses and individuals are stored on FB's database. Nigeria alone accounts for 26 million users on FB (TechPoint, 2018), one of the largest in Africa. This implies that over 26 million individuals and businesses (plus those who transact with them globally) are at potential risk of personal data-infringement via Facebook.

The complexities of this fast-evolving social media sphere and vulnerability of the gated (i.e. individuals, plus businesses and nations by extension) reemphasise the urgent need to implement social media regulations across the globe.

When data protection regulations are implemented by nations, businesses and individuals' data are less vulnerable. Data Protection Regulations are also in the interest of the platform because the public scandal has led to losses in FB stock, growth and revenue (Bloomberg, 2018) and now they must strive to earn public trust again. This brings to the fore the responsibility of the government as stakeholders in gatekeeping the media via legislations.

Regulating FB will also provide control being a fundamental human right to users, (Manolescu, 2010), aid businesses boost & track growth, promote trust for the platform, make data misuse punishable, reinforce respect for the people and nations, plus ensuring the protection of personal data.

The possible downside of regulating Facebook usage in the interest of data protection of citizens is the multiplicity of regulations from different countries demanding compliance largely difficult for FB to sustain.

This may force FB to create a *universal policy* that may or may not favour individual users. For instance, a government may want access to all personal data of its citizens and this counter the wish of the user, entitled to freedom of expression (Mai, 2016) and quiet enjoyment. Individuals still have the right to

their privacy. Meanwhile, Moor (1999) in (Pelteret & Ophoff, 2016) described 'privacy' as an elusive concept, not only because it is difficult to define, but because it is a dynamic one – it is transforming over time and is often influenced by "political and technological features of the society's environment". It is uncertain as to whether government access to citizens personal data will guarantee data protection. This is a challenge in the proposition to regulate Facebook usage with data protection laws

How then can the over 26 million (and counting) Nigerian Facebook users be protected online? This paper proposes the consideration of regional policy on the medium term and/or an adaptation of core elements of the European Union's General Data Protection Regulation (GDPR) to review the current policy document.

Regional and National Data Protection Regulation

This paper entertains the idea of a universal or regional data protection regulation policy. A data regulation policy that is championed by the African Union and adaptable by member states. A regulation that allows the body call to order and exercise punitive measures when social media platforms infringe on citizen data rights. This is, of course, requires a set up to monitor citizen complaints and follow-up with preventive and reactive moves. This idea of a regional data protection regulation is not without its challenges, as some member states may push for and collect private data of its citizens. This may expose the individual to the potential of privacy invasion and harassment from government officials, particularly in democratically unstable countries. The data is exposed to dark hacking and theft where cybersecurity is not tight, making users even more vulnerable to the use and misuse of the data. For now, however, countries are exploring the use of their data protection and regulations with fluctuating success outcomes as this paper's findings indicate.

As indicated earlier in this paper, the Nigerian state via NITDA has proposed an Act, NDPR to cater for social media protection, but gaps where identified in its approach to the obligation of the social media platforms and consequence of personal data infringement. Hence the proposition of this paper for an adoption in-principle of EU GDPR model. EU's General Data Protection Regulation, GDPR, is the latest and prevalent data protection legislation, succeeding the 1995 European Data Protection Directive which predates widespread internet availability. It was approved in 2016 by the EU and signed into law on May 2018.

GDPR is the result of an effort by the European Parliament and other governmental bodies to strengthen data protection for those living in the EU, while also providing greater uniformity to existing data laws. Residents of the EU will gain a greater measure of control over their data (and how it is used), by parties both inside and outside the EU. The legislation applies to any organization that handles, processes, and especially exports EU citizens' data outside the Euro Zone, even if that company is not based in Europe. (Cusick, 2018). Meanwhile, the new regulations will make data protections more uniform across EU member states, allowing for easier compliance from outside nations. It should be noted again that GDPR is not a recommendation, but rather a law that governs the data privacy and protection of the EU citizenry (Pelteret & Ophoff, 2016). It requires wide-scale privacy changes in all regulated organisations, and regulators will gain unprecedented powers to impose fines.

Nevertheless, the GDPR also represents an opportunity to:

- transform the approach to privacy,
- harness the value of individual/corporate data, and
- Ensure the organisation is fit for the digital economy.

Some of the key changes enforced by GDPR are as follows :

i. How personal data is defined
ii. Profiling usage of personal data
iii. The rules governing consent.
iv. The right to be forgotten
v. The right to be informed
vi. Lawful processing

vii. The right to data portability
viii. The right to breach notifications
ix. Transferring data internationally
x. Privacy by design

GDPR has impacted the business world significantly while protecting the EU citizens online, including on Facebook. It represents the single largest shift in the data privacy policy in a generation. As such, it presents a significant challenge for organizations seeking to satisfy compliance mandates. For organisations to satisfy GDPR's provisions, it may require drafting a new set of procedures and closing legal loopholes. Large organizations could see significant implications concerning budgeting, governance, IT, communications, and so on. GDPR also will not have a uniform impact on all organizations or every part of an organization, as the type of data that are handled and other variables can change how and when regulations apply.

With a comprehensive plan, organizational leaders and governments can help ensure they remain compliant with GDPR mandates—while avoiding stiff penalties and reputational harm.

LIMITATIONS AND FUTURE RESEARCH

Discourse analysis was based on documents online from the official website of NITDA. We acknowledge that some changes may have been made, however, this is not available to public notice.

Further research may be conducted on the privacy concerns of the individual and government use of data upon adopting a national general data protection regulation. Nonetheless, Data protection remains a fundamental human right and this paper identifies gate-keeping as a social responsibility of the media while pointing to the government as the stakeholder of the media to gate-keep online data administration via legislations viz data protection regulations, in the national interest.

CONCLUSION

Data protection is a fundamental human right and it should be demanded. Nigeria is currently Africa's biggest economy and continues to grow, therefore associating organisations, institutions and governments should be interested in the data security of the nation, in their best interest, even as online transactions and exchange of information grow exponentially. There is increasing evidence of the breach of data privacy and infringement, providing a basis towards challenging and calling for a review of regulations towards data protection for Africa and Nigerian businesses in particular. The role of government as a media-gatekeeping stakeholder is to set-up and implement effective regulations, however, scholars, international organisations, data advocacy groups, citizens etc are needed as pressure groups to ensure the government meets its obligation to the people.

The break-out of news on the Facebook-Cambridge Analytica scandal exposed the cases of the breach in information privacy and trust. Facebook is largely accountable for these privacy infringements and countries should be concerned about data protection of citizens and netizens. Other countries like Nigeria are making efforts to also protect its citizens' data online, but with little progress. This reassessment of data is even more pertinent because, Nigeria has business dealings with countries and organisation in all continents of the world, which also leverage communication via social media. This implies an extension of the chain of vulnerability and potential for data infringement, for innocent acquaintances and business transactions; a socio-economic threat.

The need for regulating social media cannot be overemphasized as we see a re-defined role for government in gatekeeping the media. The government is as strong as its people, thus the vulnerability of the people is a vulnerability of the government, as seen in the Nigerian election campaign role of Cambridge Analytica (The Guardian, 2018). Also, organizations feed the gross domestic product per capita of the economy- this reinforces the need to protect citizens data protection. This paper thus reechoes gate-keeping as a social responsibility of the media while pointing to the government as the

stakeholder of the media to gate-keep online data administration via legislations viz data protection regulations.

As per regulations, the National Information Technology Development Agency (NITDA), a sub of the Federal Ministry of Communications, is the government body empowered by the NITDA Act of 2007 to cater issues around online personal data protection. NITDA in 2019 proposed the Nigeria Data Protection Regulation with one of its objectives being to 'safeguard the rights of natural persons to data privacy'. The regulation is however inadequate as punitive measures are not stated clearly, demand for compliance is weak and vague. The proposed regulation also does not make provision or state the obligation of social media platforms in personal data protection. The Nigeria Data Protection Regulation from NITDA is thus not enough to facilitate the protection of Nigerian netizens and social media users, especially on Facebook. Hence this paper's advocacy for a bespoke strategic adaptation of the European Union's Data Protection approach in review of Nigeria's National Data Protection Regulation.

The European Union recently launched the largest General Data Protection Regulation in history, which has provided learning points. This paper recommends the EU GDPR and proposes an adaptation, contextualisation to create a model suitable for Nigeria, a framework for Nigeria with slight adjustments to accommodate the nation's unique peculiarities and technological literacy state. The idea of regulating FB is purely on the grounds of information privacy concerns which include secondary use of information, consumer profiling, price discrimination, identity theft and data breach. Using discourse and textual analysis, the paper affirms gate-keeping as a social responsibility of the media, while advocating that the government (in Nigeria) recognises its place as a media stakeholder, and utilise the privilege to sponsor & implement an effective National Data Protection Regulation, in the face of increasing personal data infringement on Facebook and other social media platforms.

REFERENCES

Allen & Overy. (2018, January). *Preparing for the General Data Protection Regulation.* Retrieved August 22, 2018, from http://www.allenovery.com

Baruah, T. D. (2012, May). Effectiveness of Social Media as a tool of communication and its potential for technology enabled connections: A micro-level study. *International Journal of Scientific and Research Publications*, 2(5).

Barzilai-Nahon, K. (2017). Toward a theory of network gatekeeping: A framework for exploring information control. *Journal of the America Society for Information Science and Technology*.

Bloomberg. (2018, July 25). *Facebook's Stock Plummets As User Growth and Revenue Miss Expectations*. Retrieved August 29, 2018, from http://time.com/5349100/facebook-revenue-decline-zuckerberg/

Bosher, H., & Yesiloglu, S. (2018, July 4). An analysis of the fundamental tensions between copyright and social media: the legal implications of sharing images on Instagram. *International Review of Law, Computers & Technology*, 164-186. doi:https://doi.org/10.1080/13600869.2018.1475897

Böttcher, A. V. (2014). *Twitter, News Aggegators & Co: Journalistic Gatekeeping in the Age of Digital Media Culture.* Blekinge Institute of Technology .

Campbell, R., Martin, C. R., & Fabos, B. (2015). *Media & Culture: Mass Communication in a Digital Age.* Boston: Cenveo Publisher Services.

Chavers, R. (2016). *Audience Gatekeeping Via Social Media.* Auburn, Alabama: Auburn University.

Clayman, S. E. (1998). Gatekeeping in action: Editorial conferences and assessments of newsworthiness. *Administrative Science Quarterly*, 63(2), 178–199.

CNBC. (2018, April 10). *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal.* (S. Meredith, Ed.). Retrieved August 22, 2018, from www.cnbc.com

Cusick, J. (2018, March). *The General Data Protection Regulation (GDPR): What Organizations Need to Know*. Retrieved from www.ctcorporation.com

Facebook for Developers. (2018). *App Development.* Retrieved from Facebook for Developers: https://developers.facebook.com/docs/apps/

GFCGlobal. (1998). *What is Facebook?* Retrieved August 23, 2018, from https://edu.gcfglobal.org/en/facebook101/what-is-facebook/1/

Habermas, J. (2006, March 14). Religion in the Public Sphere. *European Journal of Philosophy*, 14(1), 1-25.

Internet Users Statistics for Africa. (2018). Retrieved April 28, 2018, from Internet World Stats: https://www.internetworldstats.com/stats1.htm

Internet World Stats. (2017, December 31). *Internet Users Statistics for Africa.* Retrieved August 22, 2018, from Internet World Stats: https://www.internetworldstats.com/stats1.htm

Katz, E. (1965). *Personal influence: The part played by people in the flow of mass communications.* New York: The Free Press.

Mai, J-E. (2016). Big data privacy: The Datafication of Personal Information. *The Information Society*, 32(3), 192–199.

Manolescu, D. (2010). Data Protection as a Fundamental Right. *Effectius: Effective Justice Solutions*, (5).

Marsoof, A. (2011). Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression. *International Journal of Law and Information Technology*, 19(2), 110-132. doi:doi:10.1093/ijlit/eaq018

McDermott, Y. (2017, January 1). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1).

Meese, J., & Hagedorn, J. (2019). Mundane Content on Social Media: Creation, Circulation, and the Copyright Problem. *Social Media + Society*, 5(2). doi:https://journals.sagepub.com/doi/10.1177/2056305119839190

Ndiandukue, G-H. N. (2012, September 01). Social Networks and Privacy—Threats and Protection. *ISACA Journal Archives*. Retrieved from https://www.isaca.org/resources/isaca-journal/past-issues/2012/social-networks-and-privacy-threats-and-protection

Newberry, C. (2018, January 14). *A Long List of Facebook Statistics That Matter to Social Marketers*. Retrieved August 29, 2018, from https://blog.hootsuite.com/facebook-statistics/

Newcomb, A. (2018, March 24). *A Timeline of Facebook's Privacy Issues-and its responses*. Retrieved April 22, 2019, from NBC News: https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

Nigerian Information Technology Development Agency. (2019). *Nigeria Data Protection Regulation*. Retrieved from Nigerian Information Technology Development Agency: www.nitda.gov.ng

Oyeduntan, O. (2018, June 12). Data Protection in Nigeria: Applicability of the GDPR. *ThisDay Newspaper*. Retrieved August 21, 2018, from https://www.pressreader.com/nigeria/thisday/20180612/281900183914127

Pelteret, M., & Ophoff, J. (2016). A Review of Information Privacy and Its Importance to Consumers and Organisations. *Informing Science: International Journal of an Emerging Transdiscipline*, 19, 277-301.

Schrape, J-F. (2016, January). Social Media, Mass Media and the 'Public Sphere':Differentiation, Complementarity and Co-existence. *RESEARCH CONTRIBUTIONS TO ORGANIZATIONAL SOCIOLOGY AND INNOVATION STUDIES*. Retrieved from http://www.uni-stuttgart.de/soz/oi/publikationen/soi_2016_1_Schrape_Social_Media_Mass_Media_and_the_Public_Sphere.pdf

Schulz, W. (2004). Reconstructing Mediatisation as an Analytical Concept. *European Journal of Communication*, 19(1), 87-101. Retrieved March 30, 2018.

Shoemaker, P. (1991). *Gatekeeping.* Newbury Park, CA: Sage.

Singer, J. B. (2001). The metro wide Web: Changes in newspapers' gatekeeping role online. *Journalism and Mass Communication Quarterly*, 78(1), 65–80.

Singer, J. B. (2006a). The socially responsible existentialist: A normative emphasis for journalists in a new media environment. *Journalism Studies*, 7(1), 2–18. .

Singer, J. B. (2006b). Stepping back from the gate: Online newspaper editors and the coproduction of content in Campaign 2004. *Journalism and Mass Communication Quarterly*, 83(2), 265–280.

Sluss, D. M. (2008). Perceived organizational support as a mediator between relational exchange and organizational identification. *Journal of Vocational Behavior*, 73(3), 457-464.
Smith, A. (2011). Internal social marketing: Lessons from the field of services marketing. In Hastings, G., Angus, K., and Bryant, C. (Eds.), *The Sage Handbook of Social Marketing*. Sage Publications.
TechPoint. (2018, May 23). *Facebook now has 26 million active users in Nigeria*. Lagos, Nigeria. Retrieved August 29, 2018, from https://techpoint.africa/2018/05/23/26-million-nigerians-use-facebook/
The Guardian. (2013, September 10). *Nigeria's film and music industry falls foul of censors*. UK. Retrieved from https://www.theguardian.com/world/2013/sep/10/nigeria-film-music-industry-censors
The Guardian. (2018, March 21). *Cambridge Analytica's ruthless bid to sway the vote in Nigeria*. UK. Retrieved August 22, 2018, from https://www.theguardian.com/uk-news/2018/mar/21/cambridge-analyticas-ruthless-bid-to-sway-the-vote-in-nigeria
The Guardian. (2018, April 5). *Mark Zuckerberg will testify before Senate as well as House*. Retrieved from The Guardian: https://www.theguardian.com/technology/2018/apr/05/facebook-mark-zuckerberg-cambridge-analytica-data-testify-senate
The Telegraph. (2018, April 26). *Mark Zuckerberg faces formal summons from MPs*. Retrieved from The Telegraph: https://www.telegraph.co.uk/technology/2018/04/26/mark-zuckerberg-visit-brussels-face-questions-data-scandal/
Vanguard. (2018, April 1). *Data mining: FG invetsigates Cambridge Analytica*. Nigeria. Retrieved August 22, 2018, from https://www.vanguardngr.com/2018/04/data-mining-fg-invetsigates-cambridge-analytica/
Verdict. (2017, June 28). *Facebook has more users than any single country's population and its still growing*. United Kingdom.
White, D. M. (1950). The "gate keeper": A case study in the selection of news. *Journalism Quarterly*, 27(4), 383–390.
Zephoria Inc. (2018, July 29). *The Top 20 Valuable Facebook Statistics – Updated July 2018*. Sarasota, Florida. Retrieved August 22, 2018, from https://zephoria.com/top-15-valuable-facebook-statistics/