REGULATING ONLINE ACTIVITIES: NIGERIA TWITTER BAN IN PERSPECTIVE*

Abstract

The importance and deployment of Information Communication and Technology (ICT) in Socio-Economic reforms, in nation building, need not be overemphasized. The effective working of any advanced nation depends on some ICT-based platforms, hence the need for an adequate legal framework governing affairs on these spheres. In Nigeria, for instance, the government has been benefitting immensely from effectively deploying ICT to run its day to day affairs. From the introduction of BVN (Bank Verification Number), the TSA (Single Treasury Account) to the introduction of the NIN (National Identity Number), either for data capturing or revenue mobilization, has been made more effective. Having said that, the negative effects of ICT, in a growing economy like Nigeria, has become worrisome. There is need for the government of the day to live up to its responsibilities by not just churning out laws, but implementable laws devoid of breach on civil liberties. Free speech commands the same rights, both online and offline, but adequate screening and editorial measures, which such rights, hitherto, enjoyed, has been jettisoned leading to a deluge of unguarded, inciting, and inflammatory statements on different online platforms. This work aims at reviewing some legal frameworks, both within and outside Nigeria, and determining the effectiveness of these laws in policing the on-goings in the cyber-space. An analysis will also be conducted by this work, in order for the government of the day to understudy how foreign laws bothering on specific online activities were implemented and using decided cases as a case study, formulating best ways of effectively implementing our local ICT laws while bearing citizen`s civil liberties in mind.

Keywords: Online Defamation, ISP Liability, Electronic Contracts, Wrap Agreements, Fundamental Human Rights

1. Introduction

For reference purposes, it may be ideal to briefly trace a historical background of the growth of ICT in Nigeria. Until mid-2001, the Nigerian ICT sector was not robust as the National Telecommunications Carrier, NITEL, failed in its responsibilities of providing advanced telecommunications equipment to usher in the growth of internet services trending worldwide as at that time[1]. As part of the government`s privatization reforms, the telecommunications industry was unbundled, and thereafter, privatized, leading to an exponential growth and advancement in the nation`s ICT sector. Prior to this privatization, NITEL, being the government`s sole provider of telecommunications service, was bedevilled with lack of infrastructure, corruption and obsolete equipment, to mention but a few challenges[2]. As part of the NCC`s mandate to introduce competition in the telecommunications sector, other players in the industry were granted access into the market and an aspect of competitiveness was introduced in a sector that was prior to the NCC Act, a government monopoly[3]. Section 4 of the Nigerian Communications Act, 2004, mandates the Nigerian Communications Commission to promote fair competition in the communications industry and protection of communications services and providers from the misuse of market power of anti-competitive and unfair practices by other service or facilities providers.[4]

With huge investments in telecommunications infrastructure by these Telco's in Nigeria, there has been great improvement and growth in the ICT sector in Nigeria[5]. In 2011, GLO became the first telecommunication company to build an S800, 000,000 (Eight Hundred Million Dollar) High Capacity Fibre-Optic cable known as GLO-1, spanning from the United Kingdom to Nigeria[6]. With such advanced telecommunication infrastructure and huge investments by these telecommunication companies, there was the dire need to have

***By Chidi EZEAMA**, Lecturer in the Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Email: chidiezeama@gmail.com. Phone: +2348109001356; and

*__Nneka Obiamaka UMEJIAKU, PhD,__ Senior Lecturer and Head, Department of Commercial and Property Law, Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria. E-mail: nnekaumejiaku@gmail.com. Tel: +2348033809219

[1] F.C Chidozie, L.P Odunayo, A.O Olutosin: 'Deregulation of the Nigerian Telecommunications Sector: Interrogating the Nexus Between Imperialism and Development', *Academic Journal of Interdisciplinary Studies* Rome Italy Vol. 4 No. 1 (2015)

[2] F.C Chidozie, L.P Odunayo, A.O Olutosin, ibid.

[3] The Telecommunications Sector was fully deregulated in 2001 by the Nigerian Government and Private sector participation was introduced in the Industry which hitherto the Deregulation enjoyed Government Monopoly

[4] S.4(d) Nigeria Communications Act, 2004

[5] Deloitte ' Nigeria Telecommunications Industry: Looking Back and Looking Forward' Inside Tax available at <www.deloitte.com>

[6] J. Olaoluwa : 'Then and Now: Nigeria`s Telecommunications History'; Nairametrics on <www.nairametrics.com> accessed on Jne 8, 2021 at 5:43am

adequate legal framework, which will promote healthy competition, fairness and equity in the market and quality of service to the consumers.

The Telecommunications market in Nigeria, today, can be said to have metamorphosed from a strictly government-regulated sector, to a semi-self-regulated sector, showing growth and maturity in the market[7]. Hitherto, major arbitrations handled by the Nigerian Communications Commission were based on dominant behaviour, exhibited by early entrants into the market.[8] Over the years, the commission, through regulations,[9] had promoted healthy competitive practices in the market.

2. The Role of Telecommunication Companies in Nigeria`s ICT Sector

An article, titled 'Law on the Wings of Digital,[10]' by A&E Law Partnership, classifying the roles of several players on the internet and their responsibilities, would be relevant in this present discuss on the current twitter ban in Nigeria and who is to be held accountable for inciting comments on the platform. Behind the screen of every laptop connected to the internet are many channels, protocols, servers and sites which disseminate all types of information encoded and decoded. If there is a web of connectivity of activities that are behind the curtain for messages to be transmitted online, the question arises, would the laws of strict liability be applied in cases of legal breach in the process or are there specific laws guiding each and every transaction that occurs online? Some have likened the internet like a big library where people access knowledge from, others sources, like A&E Law partnership have envisaged the internet to be like a landlord and tenant relationship where people pay and subscribe for cyber-airtime and are given opportunity by an Internet Service Provider to sell, market, and advertise, their product or service.[11] To further understand the above position some major players on the internet will be categorized into some different heads.

1. Network Operators: These are telecommunication companies, like MTN Nigeria, Globacom, whose role is to provide internet access. As explained earlier, GLO1 cable was a major infrastructure that improved internet services in Nigeria. Such infrastructure can only be provided by multinational companies, who invest heavily on infrastructure and make their profits by providing a platform for other smaller players in the sector[12].
2. Network Infrastructure Provider: While telecommunication companies invest huge resources in acquiring infrastructure, there are other companies whose role it is to maintain and service these items of telecommunication infrastructure[13]. In Nigeria, IHS Ltd., a network infrastructure provider, in June 2016, acquired from Heilos Towers 1,211 tower sites, or in telecommunications parlance, base stations, taking full control of all the infrastructure on such sites.[14]
3. Internet Access Providers: While Big Multinationals, like GLO, invest in bulk purchase of 3-5G networks, smaller companies, like Multilink Limited, Smile Communications Limited, buy access from big multinationals and make their profit through customers subscribing to their networks. The web created by these business relationships occasions some legal controversies as to who is to be held responsible should a subscriber slander, for instance, an aggrieved third party user on an internet access provider`s platform. Some decisions, from advanced jurisdictions, would be reviewed by this work to clear the air.
4. Internet Service Providers: Companies like Gmail, Yahoo, and Chrome are all classified as Internet Service Providers on whose platforms subscribers gain access to the internet.[15]
5. Social Networks: These are virtual online communities that provide platforms for sharing ideas, concepts and opinions and give room for interaction. Since these communities envisage high subscriber traffic, there is need for adequate regulation, as studies have shown that cases of cyber-bullying, account cloning, hate speeches and racist comments are prevalent on such platforms.

With the above classification, this work will now review some decided English and US authorities on the tort of Defamation, analysing how the courts determines issues of liability of tortious actions, occurring

[7] F.C Chidozie, L.P Odunayo, A.O Olutosin, ibid.
[8] NCC Guidelines on Co-Location and Infrastructure Sharing,
[9] ibid
[10] A&E Law Partnership, 'Law on the Wings of Digital' Intermediary Liability of Companies in the Internet' <www.andelaw.com >accessed on 8th June, 2021.
[11] Ibid.
[12] ibid
[13] ibid
[14] HIS Towers Closes the first African Mobile Infrastructure Consolidation Transaction with HTN Towers. <www.ihstowers.com> accessed on June 8th 2021 at 3:36Pm
[15] ibid

online. These decisions would guide the Nigerian courts in ruling on matters bothering on the above topics, more so now that there is brewing controversy on the ban of twitter in Nigeria and its legal implications.

3. Defamation Categorized Into Libel and Slander under the Nigerian Law of Torts

In simple terms, libel is defamation in a permanent form which occurs most times in written form, while slander is a malicious verbal statement made against a person in order to malign or undermine the character of a person, so that a right thinking man in the society would be swayed by such statement. The challenge of categorizing a verbal, recorded, defamatory statement under the tort of libel or slander has spanned over the years as an integral element of proving libel, that is, it, being in a permanent form. Questions may arise, then concerning where to classify more recent technologies, like Whats App voice notes, which falls neither here nor there, hence the need for legislations on ICT to draw a clear line between what amounts to either libel or slander, while using a technology device to record a derogatory statement undermining the character of a person.

Publication, an Integral Element in Proving Defamation

In this era of social media and ICT advancement, the need to underscore the importance of publication of a defamatory material becomes necessary. However, publication may not be the only criterion for determining if a statement amounts to defamation. Tracing and pin-pointing the source of the defamatory statement is also important, since several channels, protocols, servers and platforms all form part of the process when a message is disseminated on the internet. It remains immaterial if a defamatory statement was published unintentionally. What the court looks at is the ripple effect of such statement on the character of the party who is alleging to have been defamed. At best, the courts seek to ensure that the widespread publicity given to such defamatory statement is retracted by the same source. Sometimes, while awarding damages, the monetary aspect of compensation is secondary, as the courts first looks at the publicity given to the defamatory statement and how it has negatively affected the plaintiff`s character. In the case of *Christian Onyenwe & Anor v Chief Godwin Anaejionu*[16], the courts while determining if a libellous statement that defamed the character of the plaintiffs to the chairman Aboh Mbaise and 12 other recipients was justified, it was held as follows: 'The defaming statement about the claimant in this suit, in the exact words of the text being ' a notorious political tout, a man that has no means of livelihood, a criminal and an instigator, a trouble shooter, and an irresponsible person given to instigating trouble where blood shed would result''. The afore-mentioned recipients were held by the courts to amount to sufficient publication of the defamatory statement.

4. Defamation on the Internet: How Do the Courts Determine Issues Bothering on Liability?

Having laid to rest the factors which the courts looks at to determine if a tort of defamation against a party in a suit attained the requisite level of publicity, another important aspect of this work would be focusing on online defamation and what would amount to sufficient publicity to ground an action. Taking into cognizance the borderless nature of the cyber space, what level of publicity is required to ground an action if such defamatory statement is published on an online platform. If A is alleging that he was defamed on Facebook, a worldwide platform, how does A, if based in another jurisdiction, determine the court that will assume jurisdiction to pursue his claims, or even after securing a judgement in his favour, how does he enforce the court`s judgement, if based in a different jurisdiction with 'B', the source of the defamatory material? Knotty issues that the advent of ICT has brought about as regards defamation over the internet will be discussed here. Notwithstanding the scale of immediacy associated with disseminating information on line, virtually the same principles apply to rules guiding defamation outside of the internet. Intermediaries play a vital role while trying to determine what amounts to defamation on the internet. The speed at which an original information can be doctored to amount to defamation makes issues bothering on (Internet Service Provider) ISP liability necessary while discussing the above head. If our laws distinguish between Libel and defamation, then there is need to review the above mentioned context in an internet era. Knotty issues have caused the courts in their judicial activism while deciding matters focusing on ICT, to make pronouncements which may not ordinarily fall within the ambits of what Libel or slander is in our conventional laws means. If slander, in normal parlance, means verbal denigrating statements made against a person, which are untrue before the hearing of others and Libel means putting such statements in a permanent form and making it public (e.g. Newspaper Publication), how then can our present day judicial system interpret such, when for instance a voice note over a Whatsapp message is alleged to be defamatory. Would it fall under slander or would the courts put into consideration the permanency of a voice note and call it Libel? To answer the above, we would discuss the liability of an Internet Service Provider.

[16] CA/OW/338M/2012

Internet Service Provider`s Liability

Under the general laws of defamation, broadcasting houses, and newspaper companies whose platform are used to re-publish or re-broadcast defamatory materials/statements, ordinarily would be held liable or joined as defendants in a suit for defamation, unless they can convince the courts of their neither knowing nor having any reason to know that such published material was defamatory in nature. Does the above general rule apply to Internet Service Providers or platforms like Yahoo, Facebook, Twitter, and Whats App whose platforms are most times used to re-distribute or re-disseminate defamatory statements or generally on ISP liability who owe the public a duty of care in policing their sites/platforms to ensure that content published therein is fair, and of good conscience. Several jurisdictions would be reviewed in this section of this work, to determine, to what extent, an ISP can be held liable for a defamatory material published on its platform. Much of the cases would be US-based cases as there is a dearth of decided cases on this subject in our Nigerian Legal system, hence referral to foreign judgements and cases law. While there has been a longstanding argument on the need limit the evidential burden placed on ISP`s in online defamation cases, several jurisdictions (UK and US) tried to distinguish between what a carrier of defamatory material is, in defamation matters and the Publisher of a defamatory material. This clarification will help Nigerian courts in deciding on matters bothering on online defamation.

Who is a Carrier or a Publisher of a Defamatory Material?

In the case of *Cubby Inc. v Compuserve Inc*,[17] there was a distinction by the courts in what amounts to publishing defamatory content by a website and being a mere distributor of a defamatory content on line. The facts of this case are as follows: Compuserve, operated a bulletin board online, where an independent company and, in this case (Cameron Communications Inc.), managed its journalism forum. Cameron then entered into an independent contract with DFA for the provision of a periodical newsletter called 'Rumorsville,' which included gossip. Since DFA was a third party with no legal relations with CompuServe, the bulletin board by DFA did not pass through the editorial board or any form of auditory checks by CompuServe to review the content posted online. The plaintiffs objected to the content on the site as defamatory against them and sued Compuserve. It was held by the courts that CompuServe, in this case, were mere distributors of the online content as their contract did not mandate them to review content posted on the site by Publishers, hence their being exculpated from any form of liability. The general common law rule exculpated newspaper vendors and libraries from being joined as parties in a suit for defamation even though the defamatory material is displayed on their platform. A newspaper vendor on the streets cannot be held liable for a defamatory statement in the front page of a Sun Newspaper on his stand. The most the person alleging such defamation could do is to secure a court order to remove from the market any of such defamatory material found within the vendor`s stand. This same rule applies on online platform or a website where other online users could publish their adverts, events, soft sale gossip, etc. They act as a medium for dissemination of information; hence from the ruling of the court, compuserve can be likened to an e-vendors or e-library and will not be held accountable as the source or author of such defamatory material.

The court held: 'CompuServe has no more editorial control over such a publication than does a public library, book store or a newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so' From the above court`s decision, it can be deduced that the amount of control a website owner wields over the inputs in his website determines the extent of liability in a defamation charge. The principle is that the higher the control the more propensity of being held liable for a charge of defamation and vice-versa. While advanced jurisdictions can boast of a wealth of decided cases on this subject (ISP liability), Nigeria, between the years 2015-2021, reeled out a couple of legislations[18] and in 2021 an ICT framework partially implemented. It is necessary, at this point to review some advanced jurisdictions, like United States of America and United Kingdom/EU laws, on this subject. These laws would serve as a guidance for Nigerian courts which are yet to have much judicial precedence on matters ancillary to the sub-head.

ISP Liability in the United States of America

In the controversial case of *Stratton Oakmont Inc. v Prodigy Services Company*[19] , a New York Court digressed from its earlier decision in Cubby` case which offered some form of protection for ISP`s by distinguishing between a distributor and a publisher. While the defendants in this case relied on the earlier court`s decision in Cubby`s case, an invitation to treat, placed on their online platform suggested otherwise, as they advertised their site as '*family oriented computer network*' and *claimed to exercise editorial control*

[17] 776 F. Supp. 135 (S,D.N.Y 1991)
[18] Cyber Crime Prohibition and Prevention Act 2015
[19] 23 Media L. Rep. 1974; 1995 wl 323710

over the site. Such claims placed the burden of monitoring the content placed on the site on them, hence their being bound by any tort or liability on aggrieved third parties.

With these two conflicting decisions of the United States courts, there was need to settle the dust of controversy raised, hence an Act of the United States Parliament termed the Communication`s Decency Act of 1996[20] which came about to settle the above controversy.

Highlights of the United States Communications Decency Act Of 1996[21]

It was indeed a herculean task for the Courts in the United States to distinguish between who is a publisher and who is a mere distributor in matters bothering on ISP liability hence the coming about of the this Act. A major milestone recorded by this Act. Is enshrined in its S.230[22] which recognizes protection for ISP`s who take proactive steps in ensuring that their sites are free form obnoxious and offensive content. ISP`s were also offered protection from liability if while ensuring that their sites are free from content termed offensive under the Act, *they through technical means, restrict access to such material*. The Communications Decency Act 1996 digressed from the initial court`s opinion in Stratton`s case. The position before the advent of the Act, resulted in ISP`s exempting themselves from conducting any form of due diligence on their platforms even when it bothers on matters like copyright or distribution of obscene materials online. The passage of this Act encouraged ISP`s to police what is published on their platforms, while enjoying protection of the Act resulting from aggrieved third party suits. The attitude by ISP`s since Stratton`s case, has been one of shielding themselves from liability of what goes on in their site or platform which is contrary to S.230 which offers a double- barrelled protection for both the users and their ISP provider. This assurance of the protection offered by the above section 230 re-assures ISP`s of the Act`s protection and encourages them to carry out self-regulatory roles in monitoring content and taking down obscene, obnoxious and injurious materials, thereby, playing a quasi-editorial role.

ISP Liability in France: 3 Strikes and Your`E Out Rule

Another strategy to be emulated was devised by the French government to ensure that internet users stay within the ambits of the laws on Copyright, while conducting their affairs. The law known as *Hadopi (Haute Autorite Pour la Diffussion des (Euvres et laprotection des droits sur internet),*[23] which terminates the internet access of individuals that violate, repeatedly, their copyright laws. At the third violation of their copyright laws online, the law mandates the government or the ISP, as the case maybe to take down the violating online content.

5. Justifying or Criticizing the Current Twitter Ban in Nigeria

Regulatory steps,[24] taken by the Nigerian government, in ensuring that its cyber-space is devoid of obnoxious practices would, sometimes, result in their wielding the big stick. Such bans on some platforms have been witnessed in countries like Iran[25], North Korea[26], France[27] and most recently Nigeria[28]. This part of this work would critically analyse the reason behind these bans and either justify or recommend better ways of regulating internet content within a cyber-space, while bearing the civil liberties of citizens in mind. The borderless nature of the cyber-space, sometimes, makes it impracticable for national laws governing jurisdictions to apply on activities on the cyber-space. Rules on privacy, defamation, taxation, broadcasting and internet laws have all encountered such difficulty, while trying to implement local laws on these above-mentioned heads. To paint a vivid picture on the difficulty faced while trying to apply local legislations on rules governing ICT in some certain aspects, an American decision in the case of *Piedes Negras Broadcasting Co. v. Commissioner*[29] will be understudied. Piedes Negrass, a Mexican suburb, which shares a boundary with Texas City, USA, operates a studio and a transmitting station and most of their listeners are

[20] The Communications Decency Act 1996 (CDA)
[21] CDA 1996 ibid.
[22] S.230 CDA 1996
[23] Haute Autorite Pour la Diffussion des (Euvres et la protection des droits sur internet 2009 Repealed in 2013
[24] NITDA (NDPR) Regulations
[25] Since 2010 Iran through government bans has clamped down on the internet within its jurisdiction the most recent being the 2019 ban amid violent street protests against increase in gasoline prices. Sourced from <www.rferl.org >accessed on 15th June,2021 at 2:33pm
[26] Asides from telephone communications there is no access to the world wide web and internet access to an ordinary citizen in North Korea <www.amnesty.org >accessed on 15th June,2021 at 2:33pm
[27] Hadopi Ibid.
[28] Nigeria`s Government suspension of twitter activities in the country, Punch Newspapers editorial available at <www.punchng.com >15th June 2021
[29] 43 B.T.A 297 US Tax Board of Appeals

residents of the United States of America, whereas the Radio Station was situate in Mexico. Most of their paid adverts were from residents of Piedes negrass and in a bid to make payment easier for US residents, they entered into a contract with the plaintiffs in Eagle Pass Texas to collect advert fees, on their behalf, from the United States resident's neighbours, who were also regular listeners of their radio programmes.

The United States Tax Office decided to tax the radio station based in Mexico because of the enormous profits made through paid adverts from their listeners in Texas. The matter was brought before a United States Tax Board to determine if the Radio station which was based in Mexico should be bound by United States Tax laws, bearing in mind the borderless nature of disseminating radio waves and signals. Controversies such as these have bedevilled the courts in recent times as a result of the borderless nature of the internet. While deciding on this matter, the petitioner relied on the previous decisions of the United State Tax Board on similar matters citing *East Coast Oil Co. S.A.*[30] It was held in this instant case that though the above named oil corporation was a Mexican corporation; that received its payment for oil at its office within the United States, the courts held that the source of the oil was not from the United States of America. Since the source of income from the oil emanated from outside the United States, hence Mexico had the rights to the payments collected from the US office, created as a result of convenience. Other cases cited and relied on by the petitioner were *Briskey Co*[31], *N.v Koninklijke Hollandische Lloyd*,[32] *Helvering v. Stein*,[33] *Nicholas Roerich*[34]. The respondent, in their submission, argued that Piedes Negrass Broadcast Corporation, having an outlet or an outpost in Eagle Pass Texas, means doing business within the jurisdiction of the United States of America. The courts while deciding if the office in Eagle Pass Texas was an office as recognized by the laws of the United States, considered the reason for the existence of that office and it was unravelled by the board; Piedes Negrass Broadcast Corp. claimed that the office was solely for receipt and sorting of mails from their US customers and that the office space was a free donation from a Hotel, which enjoyed their patronage as a result of traffic from guests who visit because of the Mexican radio station. The board, while deciding if that space constituted an office took into consideration the rent free nature of the space as no consideration was offered, the space cannot be termed an office under the United States Laws. It was also decided by the Tax board, that the collection of payment for broadcasting/advertising was not such activity as to indicate that their source of income was from within the United States. Based on the strength of the above, the United States Tax Board ruled in favour of the Mexican Broadcasting Corp. (Piedes Negras), on the grounds that a small outpost for receipt of mails and correspondence within the United States does not amount to doing business within the USA and hence not bound by the US Tax laws.

With the above decision of the US Tax Board as a guide, this paper will attempt to either justify or criticize the recent twitter ban in Nigeria. The above US decision was purely a revenue and a Tax matter, whereas the Nigeria Twitter ban bothers around breach of privacy policy on an online platform being instrumental in disseminating inciting and inflammatory statements which have the capability of compromising the corporate existence of Nigeria[35]. Under the Nigerian criminal law system, such alleged statements disseminated on twitter platform if proven, can amount to treasonable statements. The question now will be, who is liable? Is it the ISP (Internet Service Provider), the publisher or the user of the platform? To tackle the above issues raised, we will first review the twitter privacy and terms of usage and decipher if indeed their regulation No.4, as claimed by their management, was flouted by a user.

Was there a Binding Contract between the Nigerian President and Twitter?

At this juncture, it might be ideal to review the fundamentals of what forms an electronic contract to decipher if there exists a binding contract between any twitter account holder and its management. Online contracts simply mean where humans transact with artificial intelligence, acting as representatives of companies, making such transactions valid or voidable subject to certain rules governing basic laws of contract[36]. To enlighten more on this subject, this article will conduct a review of different modes whereby internet users may enter into online contracts knowingly or unknowingly.

[30] 31B.T A 558 affd. 85 Fed (2d) 322
[31] 29 B.T A.987
[32] 34 B.T.A 830
[33] 115 Fed. (2d) 468
[34] 38 B.T A567 affd.
[35] Nigeria`s Twitter Ban ibid.
[36] C. Ezeama 'Electronic Contracts are traditional paper contracts still relevant?' LLM Dissertation Robert Gordon University, Aberdeen Scotland. Archives 2011

Click Wrap and Shrink Wrap Agreements

Tech-companies have gone a step further to ensure that basic elements of contract law are included in online transactions in order to keep all parties abreast of their duties and liabilities while concluding online transactions. These types of contract agreements online are most times, neglected by users while concluding online transactions[37].

Click Wrap Agreements

These types of online agreements offer the user an opportunity to engage in a somewhat negotiated agreement with the electronic device or platform before accepting or declining an offer. Usually, a box at the bottom of the terms of usage or service which contains some other information or terms which parties are bound to adhere to, is included as a way of concluding the negotiations. Sometimes, a dialogue box asks the user to either click yes or no in order to complete the transaction. This introduces the fundamental aspect of a contract called the meeting of minds or in Latin, 'consensus ad idem'. Hence, clicking 'yes' means that there was a negotiated agreement before the contract was concluded[38]. In the recent case of *Spencer Meyer Vs. Uber Technologies Inc. And Ors*.[39] , which bothers on a mandatory arbitration clause contained in the Uber platform which every user must have to assent to before entering into a valid contract with Uber company. The plaintiff, in 2014, downloaded onto his smartphone a software application offered by the defendant company, Uber Technologies. After using the software overtime, the plaintiff brought an action before the courts claiming that, against the company`s policy which he agreed to online, the drivers of uber rides, who are third party agents in this agreement, determined the charge of their services as against the company whom he entered into an agreement with. However, the CEO of Uber Travis Kalanick, in his defence, claimed that the company`s uber application allowed third party drivers to fix prices. Uber also claimed that there was an arbitration clause as contained in their terms of service, which was a condition precedent to any client entering into a contract agreement with the company. It was held, that arbitration in this matter cannot be compelled. For an agreement to be assented to, via a click wrap agreement online, the feature must be reasonably conspicuous notice of such agreement in existence, and the user must unambiguously manifest his assent at the point of registration. Any wrap agreements, short of these two-limbed approaches, will be seen by the courts as not sufficient notice to either of the parties entering into the agreement. Clauses like 'Terms of service', as stipulated in the highlighted part of this page, form the basis of transaction with the user, followed by 'YES I AGREE', amount to sufficient notice and unambiguous acceptance of such contract. From the above case, we would review the Uber technologies Software engineer`s testimony in court as what forms the basis of their e-contract on their platform. With an android phone, the first screen a user arrives at after downloading the application is

1. CLICKING THE BUTTON MARKED REGISTER, which includes fields where the user would supply his basic information.
2. After completing this page and clicking next, the user advances to a second screen for payment, where card details of the user are entered. After such process the user clicks the PAYMENT button,
3. However, there is another box on the payment Screen Marked 'REGISTER,' on the same screen as the payment screen.
4. Still below the credit card input field is yet another box referring the user to a hyperlink, which when clicked, the terms of service and the privacy policy of Uber tech-service is displayed.

According to the plaintiff, he claimed he did not see such hyperlink which contained the terms of service of the contract. It was held by the courts that such terms must be conspicuous and unambiguous, leading tech companies to develop sites which make the registration incomplete without the user reading the terms and conditions of the service rendered. The element of doubt introduced in this case by the plaintiff, claiming ignorance of the terms of service, swayed the courts to rule in his favour as to the mandatories and conspicuousness of the terms of service on the company`s registration platform. With this basic information on online contracts, this paper will now look at twitter`s website to first determine what type of contract its users enter into with the management; and what their regulations or rules are, as contained in their privacy policy.

The first issue to consider is whether Mr. President registered twitter on a *twitter.com* platform or a ***twitter.co.uk*** platform as these are governed by different rules guiding online transactions in the United States of America and the United Kingdom/EU[40]. Though the users may be domiciled in any part of the

[37] Ibid.
[38] Ibid.
[39] 2nd Circuit Court of Appeals, No. 16-2750 (2017), 868 F.3d 66
[40] Twitter Privacy Policy (Website restricted within Jurisdiction as at the time of Publication)

world but most terms of usage agreements state that 'should any dispute arise in this transaction, the laws governing United States or the United Kingdom, as the case maybe would govern this transaction[41]'. The above distinction bothers on privacy safeguards of internet users in different jurisdictions, since United Kingdom Privacy laws offers more data protection measures to internet users within its jurisdiction as against other jurisdictions[42].

An Analysis of Regulation Number 4 of Twitter Rules

This rule states that 'ABUSE /HARRASMENT: You may not engage in the targeted harassment of someone, or incite other people to do so. This includes wishing or hoping that someone experiences physical harm'[43]. On the basis of this sole regulation, the tweet of President of Nigeria was taken down and his account blocked. This section, while trying to justify or criticize the twitter`s management decision to take down the aforementioned account, would consider the applicable laws governing the transactions between the account user and the company. Depending on what platform an account was registered on, either the laws of Silicon Valley, California State in the United States or the laws of United Kingdom and Ireland/EU laws would govern the transaction taking into consideration the domicile of business of the tech company. If the company alleges and proves that an utterance was an inciting statement capable of causing physical harm or threat to persons violating the laws where they are domiciled, then taking a user account down would be a justifiable[44] act by the company. This justification is based on the prior reviewed, decided authority in the case of Piedes Negrass Broadcasting Corp. vs. Commissioner,[45] where it was held that the domicile of a business is where its operational equipment are situate and in this case United States. The second limb of this brewing controversy is the Powers of the Nigerian Government to regulate the activities of an online platform which operates within its jurisdiction taking into account the borderless nature of the internet. According to a statement by the Minister of Information in Nigeria, 'that the persistent use of Twitter for activities capable of compromising the nation`s corporate existence, hence the ban by government'. To further elucidate on the above, a review of existing laws governing the cyber-space in Nigeria would be reviewed. While it is fact that the NCC Act and the NBC Act are specific legislations that tackle the above legal controversy, other subsidiary legislations like the NITDA NDPR (Regulations) and the Cyber-Security Policy Framework 2021, will be reviewed in other to recommend the international best practices needed to check the excesses of online broadcasting platforms.

The National Broadcasting Commssion Act Cap N11 LFN 2004

This Act empowers the NBC, by virtue of its S.23[46], to make regulations subject to the approval of the Honourable Minister. According to a publication by AELEX[47], referencing Chapter 2 of the NBC Code 6th Edition which derives it authority from S.23 of its establishing Act, the code, makes provision for mandatory registration of all intending web/online broadcasting services with the commission. All web/online broadcasting providers would also face sanctions which include but not limited to, takedowns order or blocking of its channels or a shutdown order. A recent newspaper advertorial dated 10th June, 2021, setting in motion its S.(1)(b)(i) NBC Act, 2004, calling on all OBS providers and social media platforms to obtain service licence which, hitherto, now was unregulated.[48] There has been this brewing controversy which this advertorial seems to have laid to rest, regarding the strength a subsidiary legislation has over an enabling law. Digital Broadcasters like DSTV, until now, have hinged on this argument as a defence to evade sanctions by NBC. Their argument is hinged on a Supreme Court decision in *Famfa Oil v. NNPC*[49] on the powers by the president to grant an OML (Oil Mining licence) and if such powers overrides the dictates of the constitution. It was held by the courts that ' By virtue of S. 44 of the Constitution of the Federal Republic of Nigeria 1999, no moveable property or interest shall be taken possession of compulsorily and no right over or interest in any such property shall be acquired except in a manner as prescribed by the Constitution'. The Courts held that an attempt by the Minister of Petroleum to participate in OML 127 without complying with the 1st paragraph of S.35 contravenes the provisions of S44 of the CFRN 1999. The Constitution being the grund norm overrides any regulation by the Federal Ministry of Oil and Gas which strips the constitution

[41] Ibid.
[42] *Max Schrems v Facebook and ors*. CJEU 2000/520/EC
[43] Regulation Number 4 Twitter Rules available on< www.twitter.com >(Site restricted within jurisdiction), accessed outside jurisdiction on 11th June, 2021, at 3:29pm
[44] S.230 US Communications Decency Act, 1996
[45] ibid
[46] NBC Act CAP N11 L.F.N 2004
[47]<www.aelex.com >
[48]OBS providers and social media platforms to obtain service licence which hitherto now was unregulated <www.proshareng.com >accessed on 11th June, 2021 @ 10:38pm
[49] (2012) 12NWLR prt. 148

of its powers over the management and granting of oil licences in Nigeria. Linking this above argument to our present discuss, Digital Broadcasting Operators in Nigeria, while contending with Chapter 2 of NBC code 6th edition, mandating them to register all web/online digital broadcasting platforms, opined that the Nigerian Copyrights Act[50] offers them sufficient intellectual property rights protection. DBO`s, in their argument, opined that a (regulation, rules or codes of practice NBC code 6th edition), which derives its authority from a substantive law (NBC Act 2004) which creates it, cannot, on its own, override the provisions of another substantive law (Nigeria Copyrights Act) without first undergoing an amendment, citing the legal authority of NNPC vs. FAMFA OIL Ltd[51]. However, this argument which, hitherto, now offered some form of reasonable protection has been overtaken by this recent Newspaper advertorial dated 10th June, 2021, setting S.(1)(b)(i) NBC Act, into motion which mandates all social media platforms in operation within Nigeria to from henceforth obtain service licence and clearance for the Government of Nigeria .

On the strength of the above, it can be said that the National Broadcasting Commission with the mandates of regulating DBO`s; which twitter falls under can, after all make regulations and rules to ensure that the cyber space in Nigeria is devoid of obnoxious, unscrupulous and inflammatory content. Adequate checks like issuance of licences, approvals, approvals in principle and enforcements needs to be regular to ensure quality standards.

Does the Twitter Ban Infringe on the Fundamental Rights of its Users within Jurisdiction?

The Universal Declaration of Human Rights[52] enunciates certain laid down rights which every person is entitled to. However, these rights become non-absolute when matters bothering on national security or protecting the sovereignty of a nation become an issue. This begs the question national security and civil liberty rights of individuals, which overrides the other? In answering this rhetoric, this article will cite some United States precedents and statues, pre and post 9/11 legislations to underscore the necessity of whittling down some civil liberties rights while ensuring that peace and security of citizens in a nation is guaranteed. The Patriot`s Act of 2001[53], which amended some provisions of existing US laws like The Foreign Intelligence Surveillance Act FISA (1978) [54], and The Electronic Communications Privacy Act (1986),[55] reduced restrictions placed on law enforcement agents to wiretap telephone, email information of private individuals. The Patriot Act, 2001, gives law enforcement agents access to wiretap and trace telephone calls and emails of US citizens in the course of discharging their duties. In the United States, Security agents, prior to the advent of the Patriot`s Act, were mandated to secure court warrants before compelling telephone companies to release phone or email information of private individuals; but the Patriot`s Act gives telephone service providers the right to disclose private customer information if they reasonably believe that an emergency, which involves immediate death, danger or serious bodily or physical harm to any person, requires such disclosure without delay. See *Hepting v. AT&T*[56] where a class action case was instituted against AT&T, for disclosing private phone information and records to the office of the NSA. In *American Civil Liberties Union v. NSA*[57] , the plaintiffs challenged the spying programme of the NSA (National Security Agency) of the United States, where a district court declared the programme unconstitutional. The 6th Circuit which is their appellate court for some states including Michigan and Kentucky, overturned the decision of the district court on the ground that ACLU did not show sufficient evidence of how the programme affected them and the NSA also invoked the State Secret Privilege rule which gives the government the privilege not to disclose some information that border on National security. The case of United States V Reynolds critically examines the meaning of State Secret Privileges, which simply gives the government the right to withhold vital information from the public based on security reasons.

However, in *Al Haramain Islamic Foundation v. Bush Surveillance Programme* [58], the government did not enjoy the State Secret Privilege because the plaintiffs provided enough evidence to show that they were subjected to warrantless electronic surveillance.

[50] Nigeria Copyrights Act CAP 28 LFN 2004
[51] ibid
[52] UDHR 1948
[53] US Patriots Act 2001 (Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)
[54] Foreign Intelligence Surveillance Act 1978
[55] Electronic Communications Privacy Act, 1986
[56] 439F Supp. 2d 974
[57] 493 F3d 644
[58] District of Oregon Case No. 06-274-K1

In most cases where the government enjoys its state privilege of not disclosing information that bother on national security, it is very difficult for private individuals to provide evidence of government`s surveillance Programmes to prove that their private rights were infringed upon.

To prove that the government made a warrantless intrusion into a private person`s account in the United states, as claimed by the plaintiff in the above case, the plaintiff must prove that such intrusion was outside the government`s (targeting procedures). A targeting procedure aims to prevent abuses, such as monitoring that is baseless and or discriminatory, or surveillance that targets people based on their free-expression rights. (s. 702 FISA) From the above, if twitter can disprove the Nigerian government`s claims that their activities in Nigeria would be undermining the corporate existence of the nation, then they can challenge the ban in our Nigerian courts, but most times, matters bothering on National Security which forms the basis of the ban, are not made public. Disproving government`s stands on the ban by the company would be a herculean task.

6. Conclusion and Recommendations

The sole reason for the twitter ban in Nigeria was hinged on activities on twitter platform which was alleged to have the capacity of undermining Nigeria`s corporate existence. Having established that these activities bother around the cyber-security of the nation, and the rhetoric of national security of a nation and fundamental rights of its citizens; which overrides the other? It is recommended that

1. A prototype of the United States Patroit`s Act should be enacted in Nigeria taking into consideration the current security challenges facing the nation. The Nation through a Cyber-security Policy Framework 2021, has taken the first giant step towards a roadmap in securing the nation`s cyber-space. However, most of the short-or medium term plan in this policy document[59] are more of inter-agency collaboration, trainings, and making of policies and regulations as against the force of law that is required while dealing with matters bothering on imminent national security threats. The seriousness by United States Congress in passing the Patriots Act into law, after the deadly twin tower attacks in America, underscores the importance of National security over personal civil liberties safeguards. Nigerian Citizens should be able to trade a little bit of their privacy and civil liberties rights for National Security intrusion as desperate times demand desperate measures. Bureaucratic bottlenecks like securing court warrants, court orders for wire-tapping (surveillance) by security agents may be dispensed with if there is reasonable apprehension of danger occurring. A text message reading '*meet me with the bombs at the airpor*t' shouldn`t pass through the routine safeguards of Fundamental rights liberties as enshrined in our Constitution, NDPR regulations [60] or the Anti-terrorism laws[61] which require securing the necessary warrants and court orders in order for security agents to be pre-emptive in their efforts to avert the loss of lives and properties'. In urgent circumstances, reasonable intrusion can be allowed but can later be challenged in court if proved unreasonable.
2. A peace-meal approach towards wielding government sanctions on ISP`s and internet intermediaries should be adopted, rather than an outright ban which adversely affects a young thriving tech-economy. The French Model of 'three-strikes, you're out' approach[62] should be adopted where adequate warnings must have been issued to either defaulting subscribers or ISP platforms before utilising other penal strategies like fines, sanctions and bans.
3. An aggressive educating of the youth on the adverse effects of publishing online materials and information capable of inciting the public, promote ethnic and cultural division and hate among the citizenry should be encouraged. Introducing internet ethics, as a curriculum in the junior secondary, would go a long way in re-orientation of the youth on internet usage and ethics.
4. Cross-border collaboration and partnership, which is one of the strategies adopted by the recent Cyber-Security Policy Framework 2021[63] by the Office of the National Security Adviser, should be adequately utilized.

[59] National Cyber-Security Policy Framework Document 2021
[60] NITDA (NDPR) Regulations 2019
[61] Terrorism (Prevention) Amendment Act, 2013
[62] ibid
[63] National Cyber-Security Policy Framework Document 2021 ibid