INFORMATIONAL PRIVACY AND SECURITY AMID GROWING ACTIVITIES ON ELECTRONIC PLATFORMS IN NIGERIA: A CASE FOR DATA PROTECTION LAW[1]

Abstract

Data protection is a fundamental approach created to provide security and protection over information that are personal to individuals and are capable of identifying or leading towards the identification of individuals. Informational privacy in this context connotes the protection accorded to individuals in the processing, storage and dissemination of private information. Put differently, it suggests the misuse or unwanted use of private information. This mechanism is extremely crucial to Nigeria in today's growing trends in information and communication technology. Essentially, this paper seeks to re-echo and underpin the importance of adopting a formidable regulation(s) towards the way and manner personal information of people are being processed, stored and disseminated. This is having regards to Nigeria's growing interests in electronic approach to citizen's identity management, education, business and social activities, and governance at all levels. This paper further answers questions on how porous Nigeria has become in the overall management of people's personal information compared to other countries with effective data protection regulations. It also highlights the importance of a data protection regulation to the nation's economy. Furthermore, unprotected use of personal information on internet has prompted another side of reservation about right to privacy. This paper equally looks at how data protection legislation will advance the right to privacy in the use of internet and information technology.

Key words: *Personal Data, Human Right, Privacy, Information Technology.*

1. Introduction

Data protection regulation has emerged quite recently in some developed and developing nations of the globe. This regulation has become very crucial and necessary owing to current dynamics inherent in the use of internet and the attendant consequences that it is posing to individuals in different climes. One of such consequences is substantially hinged on the degree or extent of protection that individuals can still enjoy under the fundamental right to privacy which is considered a universal human right.

Currently, Nigeria's population is about 173.6 million people making her the sixth most populated nation in the world after China, India, USA, Indonesia and Brazil.[2]In addition, the number of internet users on Nigeria's telecoms networks is pegged at 97.21 million in the month of November 2015 according to figures released by the Nigerian Communications Commission (NCC).[3] Recently, the Independent National Electoral Commission (INEC) introduced an electronic element that would help in the conduct of credible, transparent, free and fair elections in Nigeria, known as card reader. For the card reader to make meaning in the electoral process, there has to be an electronic registration of all voters in Nigeria which ultimately involves the collection of vital personal information of individuals and storing same in a data bank. Again, the Nigerian banking sector has been striving towards effectiveness, efficiency, compliance with global best practice and a drastic minimization of any form of financial crimes and money laundering. Consequently, one among other approaches to achieving all the aforementioned objectives was the introduction of the Bank Verification Number (BVN). This approach also involved the compulsory collection, processing and storage of personal information by all banks of their respective customers. There have been many of such exercises by corporate, private and public institutions to collect, process and store personal information of people living, working and utilizing services in Nigeria. This is also true with the social media platforms, hi-tech sophistry of some of the electronic gadgets sold in Nigeria like the mobile phones, televisions etc. To this end, Nigeria's government is clad with the huge task and responsibility of ensuring that her citizens' right to informational privacy and security is adequately protected from breach by unscrupulous persons and

[1]By **Daniel U. NNAM,** Lecturer, Faculty of Law, Enugu State University of Science and Technology, Agbani. Email: danielnnam@gmail.com

[2]www.population.gov.ng/index.php/84-news/latest/106-nigeri... Accessed on 21/15/2015.

[3]www.premiumtimesng.com/news/headlines/192485-nigeria-internet-users-increase-to-97-million-ncc.html Accessed on 21/15/2015.

organizations especially as it relates to the use of internet and other electronic platforms in the conduct of individual affairs, especially when such affairs ought to be private matters.

Worldwide, the surveillance potential of powerful computer systems prompts demands for specific rules governing the collection and handling of personal information. The question is no longer whether information can be obtained, where it has been obtained, how it should be used. A fundamental assumption underlying the answers to these questions is that if the collection of personal information is allowed by law, the fairness, integrity and effectiveness of such collection and use should be protected. In fact, the growing interests by individuals and institutions that manage vast computerised databases have turned the modest records of an insular society into a bazaar of information available to nearly anyone at a price.[4]

2.The Scope and Basis of Data Protection Law

Computers process information, combine it in new patterns and relationships that were previously beyond reach.[5]The wonders of computer networks have made practically possible with less barriers to share information across boundaries. Equally, the availability and attractiveness that come with computer networks such as social networks, search engines, online commerce, e-governance, etc, encourage their users to reveal far more personal information than they otherwise would. This creates powerful opportunities and new tools for acquiring and using information in the hands of decision makers, the curious and mischief-makers alike.[6]

Changes to society and information technology have increased the dangers associated with inadequate controls on processing activities. The use of computer technology and the ability to transfer and publish information all over the world, the processing of sensitive data, the use of close circuit television (CCTV) and the ability to locate an individual carrying a mobile telephone are just some of the issues that could give rise to concerns if not properly regulated.[7]

When pieces of information that are of private interest are endangered by chances of having them on public platforms and further subjecting such information and the individual to vulnerability, manipulations and insecurity, then conflicts arise necessitating the need for a strategic and holistic protection, whether legal, institutional or by any other civil and acceptable means.

Data protection law affects all living being. This is as a result of the various data processing activities by numerous organisations and individuals which involve personal information and consequently require that all such activities should be adequately regulated. Data protection law has its root in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (the Data Protection Convention). That Convention was influenced by the Human Rights Convention; Article 1 which states that its purpose is to secure respect for '…rights and fundamental freedoms and in particular [the] right to privacy, with regard to automatic processing of personal data…'

As a result of the increasing changes to the society occasioned by the overwhelming presence and use of computer technology, particularly advanced digital technologies and electronic mails, there became a need to create confidence in users on their privacy. Taking a lead from the Data Protection Directive and on the basis that confidentiality in communications is guaranteed, particularly by the European Convention for the protection of Human Rights and Fundamental Freedoms, the European Parliament and the Council adopted Directive 97/66/EC of December 15 1997 concerning the processing of personal data and the protection of privacy in telecommunication sector.[8] Shortly afterwards, the

[4] South African Law Reform Commission, 'Privacy and Data Protection' (Discussion Paper 109, Project 124, October 2005) p.4
[5] M McFarland, 'Information Privacy: A case Study and Commentary' (2012) p. 1
[6] ibid, p.2
[7] B David, *'Data Protection Law'* (2nd edition, xpl publishing, St. Albans, 2005) p.1.
[8] B David, *ibid* p. 276.

European Commission thought it necessary to re-visit this form of data protection in the light of further technological developments and the outcome was Directive 2002/58/EC of the European Parliament and the Council of July 12 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications). This Directive repealed and replaced Directive 97/66/EC and Article 19 of the Directive on Privacy and Electronic Communications sector.[9]

Data protection law is essentially concerned with personal data which consists of data relating to a living individual who can be identified from those data or[10] from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.[11]In what arguably remains the most influential English data protection decision, the Court of Appeal in *Durant v. FSA,* [12] gave a definition of personal data: information affecting an individual's privacy; it must be biographical in a significant sense; and it should have the individual as its focus.

A cursory look at the forgoing suggests that data protection law is strategically concerned with sensitive personal data. The sensitivity of such data can be measured on the conceptualization of the degree to which people may feel harmed or hurt about their personal information, if shared or peddled. Sensitive personal data may consist in the racial or ethnic origin of the data subject[13], his political opinions, his religious or other beliefs of a similar nature, his physical or mental health or condition, sexual life, commission or alleged commission by him of any offence or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentences of any court to such proceedings.[14] It is also important to state that the processing of information is a wide connotation that 'embraces the relatively ephemeral operations that will normally be carried out by way of the day-to-day tasks, involving the use of electronic equipment such as the laptop and the modern printing press, in translating information…'[15]

It therefore suffices to state that Data Protection Law is a crucial tool that deepens the protection and privacy of individuals in the face of heightening usage of computer and other related electronic gadgets in the assemblage and processing of personal information or data. It has been devised as a way of ensuring confidentiality and security over personal information. It further seeks to layout appropriate conditions for collecting, storing and processing of any personal information and as well creates permissible extents and limits for sharing such information. It would also punish or sanction any breach of this informational or data privacy of individuals and would ensure commensurate compensation to the victim of such breach.

3.The Symbiosis of Right to Privacy and Data Protection

Privacy is a valuable aspect of personality. In the same vein, data or information protection forms an element of safeguarding a person's right to privacy. But then, it may be one of those concepts that are better described than defined. However, there have been some attempts at explaining the purport of privacy. Privacy is seen as right to be left alone.[16] It is 'the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information'. Significantly, there is no hazard in the absence of a single line definition of privacy. An appropriate usage is dependent on the contextual circumstance. An idea of the key issues in the right of privacy can be found in the classification of the four torts which had then emerged from

[9]*Ibid,* p.277

[10]s.1 of Data Protection Act (DPA) 1998, this is the extant data protection legislation in United Kingdom.

[11] P Carey, *Data Protection Handbook* (2nd edition, the law society, 2008) p.22. Also see s.1 of Data Protection Act (DPA) 1998. Data Controller is a person who either (alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.

[12] [2003] EWCA Civ 1746

[13] Data subject is the person who is the subject of the personal data

[14]Borrowing a leaf from United Kingdom's Data Protection Act 1998, s.2.

[15]*Campbell v Mirror Group Newspapers* [2002] EWHC 299.

[16]*Olmstead v United States* 277 US 438, 478 per Brandeis J.

the American protection of privacy.[17] These four torts are: publicity which places plaintiff in false light; appropriation of the plaintiffs name or likeness; intrusion upon plaintiff's seclusion or solitude; and public disclosure of private facts about the plaintiff. These torts have found different manifestations in different countries, albeit, they remain the signposts for the protection of the right to privacy.

Bringing it down to Nigeria, s.37 of the 1999 Constitution (as amended) provides that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' Accordingly, this is the foundation of right to privacy available to be enjoyed by every Nigerian citizen. But as the society evolves into a more complex organism, there is an attendant need to create legal protection against occurrences that may contradict or breach the essence of the initial constitutional provision which is inherently rigid to quick changes as issues crop up. Therefore, the creation of primary or secondary statutes are considered a more effective and proactive step to arresting certain related occasions and challenges that require regulation and remedies, hence, the need for a data protection law in Nigeria.

The right to privacy appears to be one right that has not received much legal attention in Nigeria but that is not to state that its relevance is minute or inconsequential. Nigerians and other persons legitimately dealing with Nigeria deserve to be protected regarding their privacy. The globe is consistently advancing by the tick of time and it keeps the law proactively vigilant and ready to contend with consequential matters. A combination of appropriate laws could effectively and satisfactorily correct or compensate a wrong committed against a person's right to privacy. Outside the Nigerian constitutional provision, a data protection law could safely afford one an alternative route to seeking relief against an infraction of the right to privacy especially as this right involves informational privacy or data privacy. The law could pose as a more peculiar jurisprudence for that kind of circumstance.

Elsewhere, data protection law has aided the courts in resolving cases related to privacy rights. This is seen in *Venables and Thompson v MGN*[18]where the courts expanded the law of confidentiality to protect the claimants from a threat to their lives, which in the court's wisdom were under the threat because of the proposed disclosure of information relating to their identities and whereabouts. Further, in *Peck v United Kingdom*[19], the European court held that the disclosure of local authority CCTV footage to the media showing the applicant in a state of distress constituted a serious interference with the applicant's right to respect for private life. In the court's view, the disclosure of private, intimate information could only be justified only by overriding requirement in the public interest and in the present case the disclosure was not accompanied by sufficient safeguards and thus constituted a disproportionate and unjustified interference with the applicant's private life.

4.Informational Privacy and Related Infractions

According to a study carried out by the International Working Party on Telecommunications, the likely threat that may arise by posting a user's profile in a social networking environment is the rise of identity theft. It stated thus;

> Millions of young people have made themselves vulnerable to identity theft as well as putting their future academic and professional prospects at risk by recklessly posting personal information on the internet, Britain's privacy watchdog warns in a report published today… Now in a far-reaching study of the internet behaviour of young people, the Information Commissioner's Office (ICO) says that 4.5 million web users aged between 14 and 21 could be vulnerable to identity fraud because of the

[17] E S Nwauche, 'The Right to Privacy in Nigeria' (CALS Review of Nigeria Law Practice (2007) Vol.1(1)) p.65

[18] [2001] 2 WLR 1038

[19] [2003] 36 EHRR 719

> carefree way they give information on the internet, especially when visiting social networking sites.[20]

On identity theft, someone pretends to be someone else by assuming that person's identity in order to access resources or obtain credit and other benefits in that person's name. This can equally extend to the 'identity thief' using such stolen information to commit other crimes and eventually the victim is being chased for responsibility to such crimes. On this note, a credit checking firm has revealed that fraudsters exchanged 12 million pieces of personal information online in the first quarter of 2012, an increase of 300% since 2010.[21]Consequently, victims of identity theft have ranged from refusal of loans or credit cards, debts being run up in their names to being chased by debt collectors for money they do not owe.[22] These are very embarrassing inconvenience to the affected individuals. In the United Kingdom, for instance, the Information Commissioner (ICO) relayed a case where a subscriber to a social network cancels his account but the social network still retains the personal data relating to that person. In 2008, Bebo, a social network site was reported to have retained personal data of a subscriber whose account had been cancelled.[23]

In 2010, Facebook introduced a new tool for users to share information about the things on the web that they liked. But Facebook users who had clicked on the 'LIKE' button for some products began seeing their name and photo used to promote their product. A class-action lawsuit was launched. Nick Begus became part of the class-action after his friends saw his name being used to promote a 55-gallon barrel of personal lubricant he had 'Liked' as a joke. His sarcastic comment was, 'for Valentine's Day and every day for the rest of your life'. This eventually became part of an advertisement for Amazon, where the barrel was for sale. Currently, Facebook's European privacy practices are to be investigated by the Irish data protection watchdog, after a three-year legal fight by Austrian privacy campaigner Max Schrems.[24] Facebook has been sued in a class action suit led by Max Schrems. This action focuses on the way Facebook collects and forwards data in breach of the safe harbour[25] agreement between Unied Kingdom and United States of America. The legal action also claims privacy laws are breached in the way the networking giant monitors use the site's 'LIKE' buttons. It has been brought against Facebook's European headquarters in Dublin, which registers all accounts outside the US and Canada.

In another development, the US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and email, according top secret documents revealed by former contractor Edward Snowden. The files show that the National Security Agency and its UK counterpart GCHQ have broadly compromised the guarantees that internet companies have given consumers to reassure them that their communications, online banking and medical records would be indecipherable to criminals or governments. In addition, the agencies have adopted covert measures to ensure control over setting of international encryption standards, the use of supercomputers to break encryption with 'brute force' and collaboration with technology companies and internet service providers themselves. Through these covert partnerships, the agencies have inserted secret vulnerabilities known as backdoors or trapdoors into commercial encryption software.[26]

---

[20] R Verkaik, 'New front in the battle against identity theft' *The Independent*, November 23, 2007.

[21] W Ashford 'Online Identity Theft is up 300% on 2010, warns Experian' (17 July 2012) http://www.computerweekly.com/news/2240159690/online-identity-theft-is-up-300-on2010-warns-Experian Accessed on 27/15/2015

[22] ibid

[23] A written correspondence by the ICO dated September 30, 2008.

[24]www.theguardian.com/technology/2015/oct/20/max-schrems-facebook-privacy-ireland-investigation Accessed 27/15/2015.

[25] The safe harbour agreement is a 15-year old agreement which provides that European citizens' data transferred between the European Union and United States of America as being adequately protected, allowing US companies to self-certify their data protection practices.

[26]Revealed: How US and UK spy agencies defeat internet privacy and security-www.theguardian.com/world/2013/sept/05/nsa-gchq-encrypti.... 27/5/2015

Samsung was the cause of recent fuss over so-called 'smart' TVs invading people's privacy after a Samsung customer checked the privacy policy of a new gogglebox[27] that supports voice commands to change channels. 'if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party,' the policy warned. This raised the spectre of the TV in your living room listening to private conversations. Samsung moved to clarify that the TV transmits only samples of spoken commands back to the firm that develops the speech recognition technology, ostensibly to improve the accuracy of the system. The storm that ensued when this was blown into the open shows just how little people are aware of the information such smart devices are reporting back to their producers. It also reveals how such technology could easily by hackers and turned into a real spy in the living room.[28]

Laptops, smartphones and memory sticks are devices that could reveal personal data if not properly secured and handled. Cyber-criminals could take advantage of these kinds of laxity and weaknesses on the part of the data controllers and processors. The 'Geotagging' functionality of these smartphones using the built-in GPS is capable of spotting the user's exact location into the file of photos taken using the smartphone's camera. Geotagging is the process of embedding location information into photos. Consequently, if these photos end up on the internet, criminals can use the geotag to track someone's movement or find out one's residence.[29]

There are incidents of mobile telecommunication networks sending unsolicited and inconveniencing text messages to network subscribers and many of such similar direct marketing messages from unknown sources through the mobile networks. The big question is, how did those marketers get the phone numbers without the owners' consent? These acts could be regarded as the unauthorized use of personal information thereby invading people's privacy and personal data breach.

5. Conclusion

On the basis of all the issues discussed above, the need for an effective data protection and privacy law cannot be overemphasized. There is a profound worrisome gap that raises concern on how Nigerian Citizens' personal data are being processed both locally and internationally and by extension affects national security and the economy adversely. Appallingly, Nigeria has two Data Protection related bills (one dated 2008 and the other 2010); yet neither has been passed into law. Owing to the absence of a regulatory framework for processing personal data, public and private institutions in Nigeria resort to third parties in foreign countries for these services because due diligence cannot be obtained in Nigeria and contractual clauses are not favourable to Nigerians. Furthermore, Nigerians are susceptible to surveillance and monitoring by other countries and large organisations. This is possible with Nigerians' use of smartphones, laptops, iPads and other tablets, smartwatches, smart televisions, Point of Sale (POS) terminals, CCTVs, etc. With a properly designed and effective data protection and privacy law, other developed countries will be willing to indulge in profitable activities that would require processing of people's private information across the globe and as well add value to Nigeria's socio-economic fabric. As a result, Nigeria will be recognized as a country with the requisite regulatory framework for adequate protection on personal information and privacy. Also, a data protection and privacy law will set out permissible modalities and strict compliance measures for electronic, IT software and Apps developers/designers, even other controllers. This category of persons and organizations will be compelled to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. With the availability of this legal tool, Nigerian citizens can now be educated properly on their rights under the law and how to lay complaints and make claims against

[27]www.v3.co.uk/news/2394850/top-10-technology-privacy-risks-prying-phones-spying-cars-and-snooping-homes/page/3

[28] F FAkinsuyi, 'Data Protection and Privacy Laws Nigeria: A Trillion Dollar Opportunity!!' http://ssrn.com Accessed on 27/15/2015

[29]Privacy in the Age of the Smartphone' (Privacy Rights Clearinghouse, 2012) http://www.privacyrights.org Accessed on 27/15/2015.

any person or organization that has acted in breach of the law to invade or misuse their personal information and privacy.

Finally, an independent regulatory commission must be set up to compliment the workability of the law. Such commission needs to ensure strict compliance and enforcement of the law by issuing notices to affected parties and claiming compensation on behalf of data subjects for any damage suffered from the party in breach. Of course, obstruction of commission's work should be regarded as a very serious breach of the law and may constitute a serious offence. In United Kingdom, for instance, the Information Commissioner's Office has the power to issue financial penalties to organisations that breach Data Protection and Privacy legislation. The ICO has succeeded in slamming fines thus[30]:

i. On the 18th December, 2015, Bloomsbury Patient Network was fined after it advertently revealed the identities of HIV patients through an email error.
ii. On the 25th Nov, 2015, Telecom Protection Service Ltd has been fined £80,000 for making unsolicited marketing calls to sell cold call blocking devices. The Bournemouth based company was telephoning people to sell a call-blocking service and device to stop unsolicited calls, the same type of calls the company itself was making.
iii. UKMS Money Services Limited, a PPL claims company that sent more than 1.3 million spam texts has been fined £80,000. It used mobile phone numbers it had bought from list brokers to encourage people to make a claim for PPL compensation. A total of 1,442 people complained to the ICO and the 7,726 spam text reporting service during UKMS's nine-week direct marketing campaign between April and June 2015.
iv. On 10th November, 2015, Oxygen Limited, a South Wales based lead generation company has been fined £120,000 for making unsolicited automated marketing calls. Oxygen Ltd made over one million calls playing a recorded message claiming to be a 'government awareness call' and offering to write off debt.
v. On 20th October, 2015, an online pharmacy, Pharmacy 2U, sold details of more than 20,000 customers to marketing companies has been fined £130,000. The pharmacy offered the customer names and addresses for sale through an online marketing list company. The ICO investigation found that the pharmacy had not informed its customers that it intended to sell their details and that the customers had not given their consent for their personal data to be sold on. This was in breach of the UK Data Protection Act.
vi. In July 2014, the ICO fined Thomas Cook subsidiary, Think W3 Limited £150,000 after a hacker stole more than 1.1million customers' personal details including credit and debit card numbers due to poor data security measures on its website.
vii. UK branch of Zurich Insurance fined £2.3m for failing to have adequate systems and controls in place to prevent the loss of customers' confidential information.
viii. Prudential Insurance fined £50,000 over a mix-up over the administration of two customers' accounts led monies meant for an individual's retirement fund, ending up in the wrong account.
ix. Bank of Scotland fined £75,000 after customers' account details were repeatedly faxed to the wrong recipients. The information included payslips, bank statements, account details and mortgage applications, along with customers' names, addresses and contact details.
x. Ministry of Justice fined £140,000 for failing to keep personal data securely, after spreadsheets showing prisoners' details were emailed to members of the public in error.[31]

The ICO has achieved over 163 enforcements and penalties[32] over data protection breaches and over £2.17m in monetary penalties issued during 2013-2014.[33]

Emphatically and very strongly too, Nigerian legislature must note that in a revived interest to pursue a safe haven for personal information belonging to Nigerians, it needs to give consideration to other competing interests such as the administering of national social programmes, maintaining law and order, and protecting the rights, freedoms and interests of others, including the commercial interests of industry sectors such as banking, insurance, direct marketing, healthcare, pharmaceuticals and travel services. The task of balancing these opposing interests is a delicate one.

[30]www.ico.org.uk/action-weve-taken/enforcement Accessed 27/15/2015. See F FAkinsuyi, *ibid* at 7
[31]*ibid.*
[32]www.ico.org.uk/action-weve-taken/enforcement Accessed on 27/12/2015.
[33]www.itgovernance.co.uk/dpa-penalties.aspx Accessed on 27/12/2015.