SOCIAL MEDIA AND BREACH OF PERSONAL DATA PRIVACY: AN ANALYSIS

by Abraham Omoufoma Aigba

Introduction

In recent times, data privacy and security have attracted much-needed attention culminating in the formulation of national laws and regulations aimed at protecting and promoting data privacy of persons (data subjects). This protection is closely linked with the data subject's right to privacy guaranteed under most domestic and international legal instruments.

However, the more the efforts exerted by various governments with a view to safeguarding data subjects' right to data privacy, the more advancement in technology seems to clog all efforts in that regard. Particularly, the role of social media platforms as a vehicle for breach of data privacy right is becoming increasingly significant.

In a world where people are constantly connected through the internet by social media platforms which hold and process a wide range of personal data, the breach of personal data of data subjects on these platforms is predictable, particularly in developing countries like Nigeria, where there is little or no awareness of the need for data protection and the attendant consequences of data breach.

This article will appraise some common actions on social media platforms[1], such as adding a data subject(s) to a 'group(s)'[2] without the consent of the data subject(s) first sought and obtained; or the common practice of sending a data subject's contact details to friends or acquaintances without prior consent of the data subject.

Where any of the above instances is the case or there is any form of processing of personal data on social media platforms without the express consent of the data subject, this article argues that there is a breach of personal data under the Nigerian Data Protection Regulation[3] and/or an infringement of the right to privacy under the 1999 Constitution of the Federal Republic of Nigeria (as amended).[4]

The Scenarios

Scenario I

Mr **M** vies for the NBA presidency and has campaign managers and coordinators across the country. They enlist the help of local NBA branches, fora and groups or even hacked the database to get the personal details[5] of eligible lawyers. Using the details obtained, the names of lawyers are added to campaign groups on WhatsApp, Telegram, Facebook, *et al* with a view to selling a candidate vying for elective office, without the consent of the lawyers.

[1] For example, WhatsApp, Facebook, Telegram, etc.
[2] In particular, this work explores and argues against indiscriminate additions to political groups created to advance the candidacy of one or more candidate in various professional elections such as the NBA election
[3] Herein NDPR
[4] The Constitution
[5] Such as phone numbers, social media accounts, etc.

Scenario II

P, who wants to establish contact with R, has just met Q a friend of R's. Q is nice and warm and decides to oblige P with R's phone number and email address.[6]

Analysis under the Nigeria Data Protection Regulation (NDPR)[7]

Arising from Scenario I is the issue of whether the personal data of the data subjects[8] so added to the various platforms has been breached. The features of the various social media platforms under discourse are such that to add data subjects to groups, one has to obtain basic information such as the phone number or email address of the data subject[9]. This basic information is what the NDPR refers to as personal data[10]. It would therefore mean that the personal data was obtained without the consent of the data subjects contrary to the provisions of the NDPR which provide that personal data shall only be processed with the consent of a data subject. It is immaterial that you did no more than add the data subject.

Under the provisions of the NDPR, *'processing'* means *"any operation or set of operations which is performed on personal data or on sets of personal data…"* Hence, storing the names and/or phone numbers through whatever means and actions taken to add the data subjects to the group(s) are all *"processing"* within the contemplation of the NDPR. It should be noted that actions that amount to processing are inexhaustible and this explains the use of *'such as'* in the NDPR. Therefore, the processing in Scenario 1 above was done without the consent of the data subjects. In the absence of a contract, legal obligation or consideration of the vital interest of the data subject, such processing of personal data without the consent of the data subject is wrong and offends the provisions of the NDPR.

The effect of the foregoing is that these campaign coordinators, being data controllers/administrators/processors as contemplated under the NDPR, may be liable to enforcement actions[11] which may ground a civil claim for damages and/or penal sanction under the NDPR and the National Information Technology Development Agency Act, 2007. In addition, the local branches, fora, etc. from whence the personal data[12] are obtained, may likewise be liable for data breach as aforesaid.

The foregoing analysis applies *mutatis mutandis* to Scenario II save that processing thereunder is of a different nature. Although, given the indifference and seeming lack

---

[6] Both scenarios are case studies which can be modified and extrapolated

[7] It should be noted that the right to data privacy under the NDPR is not exclusive of the fundamental right to privacy guaranteed under Section 37 of the 1999 Constitution of Nigeria as amended.

[8] Data Subject means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

[9] Names, phone number, usernames, etc.

[10] Under the NDPR, "Personal Data" means 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 identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others

[11] It is of course a different kettle where the data subjects join the group/s using group invites.

[12] Themselves having lawfully obtained the personal data from the data subject

of awareness in Nigeria on the subject of discourse, it may be regarded as preposterous for a data subject to commence an action for breach of his/her data privacy right on this ground. Nonetheless, same runs contrary to the provision of the NDPR.

Commendably, some of these social media platforms now have features requiring the consent of the data subject before he/she is added to any group. However, more needs to be done as the fact that a data subject was unaware or did not activate the features restricting unauthorised data processing on his/her account, is not enough to exonerate the data controller/administrator in the event of a data breach.

Conclusion

The danger posed by random additions to group is multifaceted. It may lead to serious security breach, personal data coming into possession of persons a data subject would ordinarily be opposed to, unsolicited texts, Ads, etc., all to a data subject's chagrin.

Whilst it may be argued that protection of personal data as well as the privacy of persons is still in its infancy in Nigeria, Nigerians are, however, becoming more and more aware of their right to protection of their personal data.

The Courts are also tilting towards treating unauthorised disclosure of personal details like phone numbers to third parties for commercial purposes as breach of privacy. The cases of **Godfrey Eneye v MTN Nig. Communications Ltd**[13] and **Ezugwu Anene v. Airtel Nigeria Ltd**[14] are prime examples.

It is therefore hoped that the courts will, as time goes on, appropriately accord data subjects the full protection afforded by the NDPR and the Constitution with respect to the protection of their right to data privacy, taking into consideration the peculiarities of each case.

[13] (Unreported) CA/A/689/2013
[14] (Unreported) FCT/HC/CV/545/2015